EKSTRAKT – BIND I – PROCESSKRIFTER

I sagen for

Østre Landsret, 16. afdeling

BS-36799/2018-OLR

Foreningen imod Ulovlig Logning
Birkegade 15, 5. tv.
2200 København N
advokat Julie Bak-Larsen i henhold til proceduretilladelse
(”Sagsøger”)

mod

Justitsminister Nick Hækkerup
Justitsministeriet
Slotholmsgade 10
1216 København K
advokat Rass Holdgaard
("Sagsøgte")

Sagen hovedforhandles den 5. maj 2021, kl. 9.30-15, og den 6. maj 2021, kl. 9.30-12.

INDHOLDSFORTEGNELSE

Bird & Bird

Bird & Bird
Advokatpartnerselskab
Sundkrogsgade 21
2100 København Ø
Tlf +45 72 24 12 12
Fax +45 72 24 12 13
twobirds.com

TIDSPLAN

I sag BS-36799/2018-OLR

Foreningen imod Ulovlig Logning
CVR-nr.: 39 30 93 86
Birkegade 15, 5. tv.
2200 København N
v./ advokat Martin Von Haller)
("Sagsøger")

Mod

Justitsminister Nick Hækkerup
Justitsministeriet
Slotholmsgade 10
1216 København K
v./advokat Rass Holdgaard
("Sagsøgte")

Sagen er berammet til hovedforhandling i Østre Landsret, retssal 16, Bredgade 59, 1260 København den 5. maj 2021 kl. 9.30 – 15.00 og den 6. maj 2021 kl. 09.30 – 12.00.

Den 5. maj 2021:

09.30 - 09.40	Nedlæggelse af parternes påstande, introduktion af parterne.
09.40 - 10.45	Forelæggelse, inkl. Sagsøgtes eventuelle supplerende bemærkninger
10.45 - 11.00	Formiddagspause
11.00 - 12.00	Forelæggelse (forsat)
12.00 - 13.00	Frokost
13.00 - 14.10	Procedure, Sagsøger
14.10 - 14.20	Eftermiddagspause
14.20 - 15.00	Procedure, Sagsøger (forsat)

Den 6. maj 2021:

09.30 - 10.45	Procedure, Sagsøgte
10.45 - 11.00	Formiddagspause
11.00 - 11.30	Procedure, Sagsøgte (forsat)
11.30 - 12.00	Replik, duplik

Sagens oplysninger

Den 19. april 2021

Østre Landsret, sagsnr. BS-36799/2018-OLR

Foreningen imod Ulovlig Logning mod Justitsministeriet, Departementet

Sagens parter og andre sagsdeltagere:

Sagsøger Foreningen imod Ulovlig Logning
Foreningen imod Ulovlig Logning er momsregistreret

(advokat Martin Von Haller Grønbæk)

SagsøgteJustitsministeriet, Departementet
Justitsministeriet, Departementet er ikke momsregistreret

(advokat Rass Markert Holdgaard)

Sagstype: Almindelig civil sag

Sagsemne: EU, Menneskerettigheder, Retspleje og civilproces, Statsforfatningsret

Kort beskrivelse af sagen: Sagen handler om sagsøgtes opretholdelse af logningsbekendtgørelsen (bkg. nr. 988 af 28. september 2006). Opretholdelsen er i strid med EU-retten og menneskerettighederne. Sagsøgte skal tilpligtes at anerkende, at logningsbekendtgørelsen er ugyldig.

Sagen er modtaget hos Østre Landsret den 1. juni 2018

Hvis sagen er henvist/appelleret
Oprindelig ret:
Oprindeligt sagsnr.:
Oprindelig afgørelses dato:
Sagen videreført til:

Status
Optaget til afgørelse:
Afsigelsedato:

Tidspunkt, hvor sagen blev registreret som optaget til afgørelse:
Afsigelsestidspunkt:

Værdien af parternes påstande:

Sagsøger Foreningen imod Ulovlig Logning: 0,00 kr.
Retsafgift: 2.500,00 kr.

Sagsøgte Justitsministeriet, Departementet:
Retsafgift: 0,00 kr.

Retsmøder:

Forberedende møde: 17. august 2020 kl. 10:00 - 11:00 i Retssal 14

Forberedende møde pr. telefon: 23. november 2020 kl. 10:00 - 10:30

Votering: 4. maj 2021 kl. 09:30 - 15:00

Hovedforhandling: 5. maj 2021 kl. 09:30 - 15:00 i Retssal 16

Hovedforhandling: 6. maj 2021 kl. 09:30 - 12:00 i Retssal 16

Votering: 6. maj 2021 kl. 13:00 - 15:30

Votering: 10. maj 2021 kl. 09:30 - 15:00

Votering: 12. maj 2021 kl. 09:30 - 15:00

Votering: 1. juni 2021 kl. 09:30 - 15:00

Votering: 2. juni 2021 kl. 09:30 - 15:00

Skønsmand:

Påstandsoversigt, 19. april 2021

Østre Landsret, sagsnr. BS-36799/2018-OLR

Foreningen imod Ulovlig Logning mod Justitsministeriet, Departementet

Påstande

Sagsøger, Foreningen imod Ulovlig Logning, har under denne sag den 25. marts 2021 nedlagt følgende påstand:

Justitsministeriet, Departementet skal til Foreningen imod Ulovlig Logning betale 0,00 kr.

Sagsøger nedlægger følgende sideordnede anerkendelsespåstande:

1) bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik er ugyldig;

2) Sagsøgte har ikke sikret, at den ugyldige retstilstand fra bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger blev bragt til ophør hurtigst muligt.

Tidligere påstande

Sagsøger, Foreningen imod Ulovlig Logning, har under denne sag den 1. juni 2018 nedlagt følgende påstand:

Sagsøgte skal anerkende, at bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik er ugyldig.

KØBENHAVNS BYRET
RETSBOG

Den 28. september 2018 holdt Københavns Byret møde i retsbygningen.

Dommer Michael Toftager behandlede sagen.

Sag BS-19085/2018-KBH

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsminister Søren Pape Poulsen, Justitsministeriet
(advokat Rass Markert Holdgaard)

Foreningen imod Ulovlig Logning har i stævningen anmodet om, at sagen henvises til behandling ved landsret som første instans.

Justitsminister Søren Pape Poulsen, Justitsministeriet, har tilsluttet sig anmodningen herom.

Retten afsagde

KENDELSE

Efter retsplejelovens § 226, stk. 1, kan byretten efter anmodning fra en part henvise en sag til behandling ved landsret, hvis sagen er af principiel karakter og har generel betydning for retsanvendelsen og retsudviklingen eller væsentlig samfundsmæssig rækkevidde i øvrigt.

Efter parternes oplysninger omfatter sagen blandt andet spørgsmål om fortolkning af EU-lovgivning og principielle og ikke afgjorte EU-retlige spørgsmål.

Sagen er således efter de foreliggende oplysninger af principiel karakter og har generel betydning for retsanvendelsen og retsudviklingen.

Betingelserne i retsplejelovens § 226, stk. 1, foreligger således opfyldt.

Den fremsatte begæring opfylder de tidsmæssige krav, jf. § 226, stk. 3.

Betingelserne for at henvise sagen til behandling ved landsret som første instans er derfor opfyldt, hvorfor

THI BESTEMMES:

Sagen henvises til Østre Landsret.

Sagen herefter sluttet her ved retten.

ØSTRE LANDSRET
RETSBOG

Den 26. februar 2019* holdt Østre Landsret møde i retsbygningen i København.

Landsdommerne Benedikte Holberg, Rosenløv og Anne-Mette Lyhne Jensen (kst.) behandlede sagen.

Sag BS-36799/2018-OLR
(14. afdeling)

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsministeriet
(advokat Rass Holdgaard)

Der er indleveret breve af 5. december 2018 og 29. januar 2019 fra sagsøgte samt breve af 19. december 2018 og 15. februar 2019 fra sagsøgeren.

Sagsøgte, Justitsministeriet, har i brevet af 5. december 2018 anmodet om, at behandlingen af sagen udsættes med henblik på at afvente EU-Domstolens afgørelse i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres), jf. retsplejelovens § 345, og har til støtte herfor anført bl.a. følgende:

> "Som nævnt i svarskriftet … angår sag C-520/18 bl.a. spørgsmålet om, hvorvidt en domstol, med henblik på at undgå retsusikkerhed og muliggøre, at data, der forinden er blevet indsamlet og lagret, stadig kan anvendes til de formål, der er omhandlet i loven, midlertidigt kan opretholde virkningerne af regler om indsamling og lagring af data, uanset at disse måtte være i strid med bestemmelserne i artikel 15, stk. 1, i direktiv 2002/58/EF.

Dette spørgsmål er efter Justitsministeriets opfattelse centralt for bedømmelsen af sagsøgernes påstand i denne sag. Det skyldes, at i det omfang EU-Domstolen måtte erkende, at en domstol kan opretholde en lagring som ovenfor nævnt, er det så meget desto mere nærliggende at antage, at en udøvende myndighed må kunne afvente, at den nationale lovgiver foretager en ændring af de gældende regler om indsamling og lagring af data, uagtet at de gældende regler måtte være uforenelige med EU-retten. Som det fremgår af svarskriftet …, gør Justitsministeriet bl.a. gældende, at den nugældende danske logningsbekendtgørelse kan opretholdes midlertidigt som følge af de ekstraordinære retlige og faktiske vanskeligheder, som en målretning af logningsforpligtelsen medfører, og de væsentlige samfundsmæssige skadevirkninger, som en øjeblikkelig tilsidesættelse ville medføre.

Hertil kommer, at den belgiske forfatningsdomstol i forelæggelseskendelsen ud over spørgsmålet om en eventuel midlertidig opretholdelse af lovgivningen også stiller mere grundlæggende spørgsmål om rækkevidden af Tele2-dommen, herunder hvorvidt det kan tillægges betydning, at logningsforpligtelsen ikke kun har til formål at bidrage til efterforskning, afsløring og retsforfølgning af grov kriminalitet.

Den belgiske forfatningsdomstol spørger nærmere bestemt, om det kan tillægges betydning, at den pågældende logningsforpligtelse sikrer den nationale sikkerhed, forsvar af territoriet, den offentlige sikkerhed, efterforskning, afsløring og retsforfølgning af andre grunde end grov kriminalitet eller forebyggelse af ulovlig brug af elektroniske kommunikationssystemer eller gennemførelse af et andet formål i henhold til artikel 23, stk. 1, i forordning (EU) 2016/679 (databeskyttelsesforordningen).

Herudover spørger forfatningsdomstolen, om det kan tillægges betydning, at logningsforpligtelsen har til formål at opfylde de positive forpligtelser, der påhviler myndigheden i henhold til chartrets artikel 4 og 8, der består i at fastsætte en retlig ramme, der muliggør en effektiv strafferetlig efterforskning af og en effektiv retshåndhævelse over for seksuelt misbrug af mindreårige.

De danske regler om pligt til lagring af trafik- og lokaliseringsdata bygger bl.a. på Brydensholt-udvalgets forslag fra betænkning 1377/1999 om børnepornografi og IT-efterforskning og er således også begrundet i bl.a. hensynet til at sikre effektiv retshåndhævelse over for seksuelt misbrug af mindreårige. Hertil kommer, at det fremgår af afsnit 3.1.2 i de almindelige bemærkninger i lovforslag nr. L 35 af 13. december 2001, hvor retsplejelovens § 786, stk. 4, blev indført, at terrorangrebet den 11. september 2001 gav grundlag for nu at foreslå reguleringen. Den danske logningsforpligtelse varetager således også et hensyn til at sikre den nationale sikkerhed og afsløring og retsforfølgning af bl.a. terrorisme.

Det er på den baggrund Justitsministeriets opfattelse, at også en besvarelse af de øvrige spørgsmål i forelæggelseskendelsen i C-520/18 kan få indfly-

delse på udfaldet af denne sag. Uanset om EU-Domstolen besvarer spørgsmålene bekræftende eller benægtende, må det forventes, at dommen vil yde væsentlige fortolkningsbidrag til, i hvilket omfang en logningsforpligtelse kan begrænses uden samtidig at prisgive de hensyn, der er nævnt i de præjudicielle spørgsmål. Sådanne fortolkningsbidrag vil i det mindste bidrage til at præcisere, hvilke dele af de danske logningsregler der kan opretholdes i lyset af Tele2-dommen. Også af denne grund er det Justitsministeriets opfattelse, at sagen bør udsættes med henblik på afventning af dommen i sag C-520/18.

Samlet set er det Justitsministeriets forventning, at en afgørelse fra EU-Domstolen i sagen vil kunne få indflydelse på udfaldet af denne sag. For at undgå, at landsretten afsiger en dom, der er i uoverensstemmelse med EU-Domstolens dom, bør denne sag derfor udsættes, indtil EU-Domstolen afsiger dom i sag C-520/18, jf. retsplejelovens § 345."

Sagsøgeren, Foreningen imod Ulovlig Logning, har i brevet af 19. december 2018 protesteret mod, at sagen udsættes, indtil der afsiges dom i EU-Domstolens sag C-520/18, og har til støtte herfor anført bl.a. følgende:

"2. DER ER IKKE TALE OM EN PÅKRÆVET UDSÆTTELSE
2.1 Der er ikke tale om en sag, der vil få indflydelse på sagens udfald
Sagsøger finder det ikke *nødvendigt* og *påkrævet* at udsætte nærværende sag med henblik på at afvente EU-Domstolens afgørelse i sag C-520/18, da sagen ikke vedrører nye forhold, som EU-Domstolen ikke allerede har taget stilling til i (C-293/12) Digital Rights Ireland og Tele2/Watson-sagen (C-203/15). Udfaldet i sag C-520/18 kan derfor ikke forventes at få indflydelse på denne sags udfald, da EU-Domstolen på sin tredje behandling af samme forhold ikke kan forventes at ændre en praksis, der allerede er stadfæstet ved to tidligere meget klare afgørelser.

Således blev EU-Domstolen i Tele2/Watson-sagen adspurgt, om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7 og 8 samt artikel 52, stk. 1, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning som den i hovedsagen omhandlede, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

I den belgiske sag C-520/18 er det tilsvarende blevet spurgt, om artikel 15, stk. 1, i direktiv 2002/58/EF, sammenholdt med den ret til sikkerhed, der er sikret ved artikel 6 i Den Europæiske Unions charter om grundlæggende rettigheder, og retten til respekt for personoplysninger, som er sikret ved artikel 7, 8 og artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, fortolkes således, at bestemmelsen er til hinder for en national lovgivning – såsom den omhandlede, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester

til at lagre trafik- og lokaliseringsdata som omhandlet i direktiv 2002/58/EF der genereres og behandles af dem inden for rammerne af udbuddet af disse tjenester – som ikke kun har efterforskning, afsløring og retsforfølgning af grov kriminalitet som formål, men ligeledes sikring af den nationale sikkerhed, forsvar af territoriet, den offentlige sikkerhed, efterforskning, afsløring og retsforfølgning af andre grunde end grov kriminalitet eller forebyggelse af ulovlig brug af elektroniske kommunikationssystemer eller gennemførelse af et andet formål i henhold til artikel 23, stk. 1, i forordning (EU) 2016/679 (2), og som endvidere er undergivet præcise garantier i denne lovgivning vedrørende lagring af data og adgangen dertil.

Som det fremgår af ovenstående, angår begge spørgsmål, om EU-retten er til hinder for nationale logningsregler, der fastsætter en generel og vilkårlig logningsforpligtelse. Spørgsmålet i den belgiske sag har EU-Domstolen derfor allerede svaret på i Tele2/Watson-sagen, i.e. EU-retten er utvivlsomt til hinder for et sådant logningskrav.

Sagsøger mener derfor ikke, at dette spørgsmål vil få indflydelse for nærværende sag, dels fordi spørgsmålet allerede er blevet besvaret af EU-Domstolen, dels fordi C-520/18 ikke handler om de danske logningsreglers forenelighed med EU-retten.

Det tredje præjudicielle spørgsmål, som den belgiske forfatningsdomstol stiller i sag C-520/18, omhandler hvorvidt en belgisk lov i strid med EU-retten midlertidigt kan opretholdes med henblik på at undgå retsusikkerhed og muliggøre, at data, der allerede er indsamlet og lagret, forsat kan anvendes. Det gøres i den forbindelse gældende af sagsøger, at et spørgsmål om hvor længe en retsstridig lov midlertidigt kan opretholdes også allerede er blevet behandlet både af EU-Domstolen og Højesteret, og derfor heller ikke af den grund vil få indflydelse på nærværende sag.

Højesteret har som nævnt i både stævning og svarskrift netop taget stilling til dette forhold i U.2017.1243H (Pereda-sagen). I dommen blev det fastlagt, at de danske myndigheder havde tilsidesat EU-retten ved ikke at have ændret ferieloven tilstrækkelig hurtigt. Ifølge Højesteret burde myndighederne senest have ændret reglerne med virkning fra den 1. januar 2011 med henblik på at bringe loven i overensstemmelse med den retstilstand, der blevet fastslået i EU-Domstolens afgørelse i Pereda-sagen, der blev afsagt den 10. september 2009. Dommens konsekvenser for de danske regler stod klart i september 2010, og på trods heraf blev reglerne først ændret i april 2012, dvs. først 2,5 år efter EU-Domstolens afgørelse og 1,5 år efter det stod klart, at de danske regler var i strid med EU-retten.

Højesteret henviste i sin begrundelse til praksis fra EU-Domstolen, hvor det bl.a. fremgår af Brasserie du pêcheur-dommens præmis 57 og Larsy-dommens præmis 44, at en overtrædelse af EU-retten under alle omstændigheder er åbenbar, "*når den har varet ved, til trods for at der er afsagt dom i en præjudiciel sag, hvoraf det fremgår, at den omtvistede adfærd har karakter af en*

overtrædelse…" I begrundelsen anføres det endvidere, at "*Efter at der er afsagt en dom i anledning af en præjudiciel forelæggelse, hvoraf følger, at en national lovgivning er uforenelig med fællesskabsretten, påhviler det den pågældende medlemsstats myndigheder at træffe de almindelige eller særlige foranstaltninger, der er egnet til at sikre overholdelsen af fællesskabsretten på deres område, jf. EU-Domstolens dom af 21. juni 2007 i de forenede sager C-231/06-C-233/06 (Jonkman), præmis 38. Myndighederne skal ifølge den nævnte præmis navnlig påse, at national ret så hurtigt som muligt bringes i overensstemmelse med fællesskabsretten, og at borgernes rettigheder i henhold til fællesskabsretten gennemføres fuldt ud*."

Det er således sagsøgers vurdering, at EU-Domstolens svar på det tredje spørgsmål heller ikke kan forventes at have indflydelse på denne sags udfald, da det allerede nu er klar praksis både fra EU-domstolen og Højesteret omkring, hvordan "hurtigst muligt" skal fortolkes.

2.2 Sagerne er ikke tilstrækkeligt forbundne
Det gøres endvidere gældende, at sagerne ikke er så nært forbundne, at retten bør fravige udgangspunktet om, at sager fremmes hurtigst muligt.
…

Retspraksis viser således, at der skal være en særdeles tæt forbindelse til den sag, der søges udsættelse for, herunder på en måde, hvorved et delspørgsmål bliver fuldtud afgjort i den anden sag. I den konkrete situation er der tale om, at sagsøgte søger sagen udsat på et *muligt fortolkningsbidrag*, der med *en begrænset sandsynlighed* kan have relevans for nærværende sag som et fortolkningsbidrag til en retstilstand, der allerede er klart afgjort af Højesteret og EU-Domstolen.

Sagsøger mener derfor ikke, at der er tale om et så nær sammenhæng, der kan danne grundlag for den høje standard, som Rpl. § 345 kræver for at finde en udsættelse *påkrævet.*

3. UDSÆTTELSEN VIL VÆRE UFORHOLDSMÆSSIG LANG
Udgangspunktet efter Rpl. § 345 er, at retten skal fremme sagen hurtigst muligt, *medmindre* en udsættelse er påkrævet.

De præjudicielle spørgsmål i sag C-520/18 er først blevet indgivet den 2. august 2018, og sagen forventes derfor ikke at blive afgjort før om flere år. En udsættelse af denne sag vil således resultere i, at sagsøgte kan fortsætte med en passiv henlæggelse af sagen og en fortsat krænkelse af borgernes grundlæggende rettigheder i strid med en klar retstilstand og dermed de facto ikke overholde sin forpligtelse til at efterleve gældende ret.

Princippet om, at sager skal fremmes hurtigst muligt følger endvidere af EMRK art. 6 og EU Chartret art. 47, der fastslår, at enhver har ret til en retfærdig rettergang inden *en rimelig frist*. Ved vurderingen af, om en sag skal udsættes, har nationale domstole således endvidere en pligt til at sikre, at udsættelsen ikke vil være uforholdsmæssig lang set i lyset af, om det reelt

er påkrævet at udsætte sagen i en meget lang periode med henblik på at afvente udfaldet i en anden verserende sag.

4. UDSÆTTELSESANMODNINGEN ER SAMLET SET ET UFORHOLDSMÆSSIGT OG IRRELLEVANT PROCESINSTRUMENT
Sagsøger mener, at sagsøgte forsøger at udnytte muligheden i Rpl. § 345 til at udskyde nærværende sag så længe det overhovedet er muligt, da sagsøgte tydeligvis ikke kan acceptere EU-Domstolens tidligere afgørelser, og som følge heraf vil bede EU-Domstolen om for tredje gang at genoverveje logningsreglernes lovlighed samt "*visse af de udtalelser, som Domstolen afgav i Tele2-dommen*", jf. Justitsministeriets orientering til Folketingets Europaudvalg og Folketingets Retsudvalg ("Justitsministeriets orientering") s. 3.

Sagsøgte har endvidere både i sin replik og i sit Notat til Folketingets Retsudvalg … henvist til sine udfordringer med at indføre logningsforpligtelser, der ikke udgør generel og udifferentieret logning, herunder eksempelvis ved at indsnævre forpligtelsen geografisk, tidsmæssigt, til særlige personer eller anden segmentering. Sagsøgte har i den forbindelse i sin replik henvist til, at EU-Domstolen i Tele2/Watson ikke har givet tilstrækkelige anvisninger til medlemsstaterne.

Sagsøger gør selvfølgelig gældende, at det ikke er domstolenes kompetence at anvise ny lovgivning, men at træffe afgørelse om en foreliggende konkret retsakts gyldighed. Det har EU-Domstolen gjort i Tele2/Watson og Digital Rights Ireland. Det er nu op til den udøvende magt at efterleve praksis og op til Folketinget at vedtage ny lovlig lovgivning. Sagsøgte medgiver, at det ikke er en nem opgave for Sagsøgte at foreslå nye gyldige logningsregler, der kan træde i stedet for den ulovlige logningsbekendtgørelse. Det er dog ikke det, denne sag omhandler, selvom sagsøgte forsøger at inddrage sådanne administrative hensyn.

Rpl. § 345 udgør en undtagelse til udgangspunktet om, at sagen skal fremmes hurtigst muligt. Sagsøgtes udsættelsesanmodning skal af ovenstående grunde afvises, herunder også som et uforholdsmæssigt og irrelevant procesinstrument, der på ingen måde er påkrævet eller relevant for den konkrete sag."

Justitsministeriet har i brev af 29. januar 2019 til støtte for sin anmodning om udsættelse af sagen supplerende anført bl.a. følgende:

"… Domskonklusionen i Tele2-dommen er … udtrykkeligt begrænset til lovgivning, *"der med henblik på bekæmpelse af kriminalitet"* fastsætter en generel og udifferentieret lagring af trafik- og lokaliseringsdata. Hverken Tele2-dommens konklusion eller dens præmisser behandler spørgsmålet om, hvorvidt andre hensyn, f.eks. hensynet til den nationale sikkerhed, kan begrunde logning i videre omfang.

> Hertil kommer, at Tele2-dommen ikke angår spørgsmålet om, hvorvidt medlemsstaterne midlertidigt kan opretholde gældende regler om logning af hensyn til bl.a. retssikkerheden i afventning af et nyt regelsæt. Selvom det følger af Jonkmann-dommen, at medlemsstaternes myndigheder i tilfælde af afsigelse af en dom i anledning af en præjudiciel forelæggelse, hvoraf følger, at en national lovgivning er uforenelig med EU-retten, skal påse, at national ret så hurtigt som muligt bringes i overensstemmelse med EU-retten, har denne dom ikke afklaret, hvilken betydning det i den forbindelse skal have, at der er særlige retssikkerhedsmæssige problemer forbundet med en tilsidesættelse af gældende regler. Dette tema, som det tredje forelagte spørgsmål i sag C-520/18 angår, har væsentlig betydning for udfaldet af denne sag.
>
> Justitsministeriet fastholder, at en afklaring af de spørgsmål, der er forelagt i sag C-520/18, vil kunne få indflydelse på udfaldet af denne retssag."

Justitsministeriet har i brevet endvidere gjort gældende, at hvis sagsøgeren har ret i, at den belgiske forfatningsdomstols spørgsmål kan besvares uden vanskeligheder på baggrund af eksisterende retspraksis, må EU-Domstolen forventes at afgøre sagen hurtigt ved afsigelse af en begrundet kendelse efter proceduren i procesreglementets artikel 99, og at en berostillelse i denne sag i så fald vil være tilsvarende kortvarig.

Justitsministeriet anfører afslutningsvis, at hvis landsretten beslutter ikke at udsætte nærværende sag, må det give anledning til at overveje, om landsretten selv bør forelægge præjudicielle spørgsmål for EU-Domstolen, hvilket Justitsministeriet vil forholde sig til, når landsretten har truffet afgørelse om eventuel udsættelse.

Foreningen imod Ulovlig Logning har i brev af 15. februar 2019 fastholdt, at sagen ikke bør udsættes, da der ikke er tale om en påkrævet udsættelse, og har til støtte herfor yderligere anført bl.a. følgende:

> "1. SPØRGSMÅLENE STILLET I SAG C-520/18 ER ALLEREDE BESVARET I TELE 2-DOMMEN
> …
> EU-Domstolen behandler forholdet i præmis 64-81, hvor det fastlægges, at direktiv 2002/58 af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (eDatabeskyttelsesdirektivet) også finder anvendelse på lovgivning, der har til formål at beskytte den nationale sikkerhed , forsvaret og den offentlige sikkerhed, inklusiv nationale regler der pålægger teleudbydere en logningsforpligtelse (se præmis 72-74 sammenholdt med præmis 81).
>
> EU-Domstolen anfører specifikt i præmis 73, at eDatabeskyttelsesdirektivets artikel 15 (der hjemler medlemsstaternes mulighed for at indskrænke

rækkevidden af de rettigheder og forpligtelser, der følger af direktivet, herunder kommunikationshemmeligheden), ville blive frataget enhver effektiv virkning, hvis nationale logningsregler ikke var omfattet af direktivets anvendelsesområde, og at det udtrykkeligt fremgår af direktivet, at logningsregler der har til formål at beskytte den nationale sikkerhed netop kan vedtages inden for rammerne af eDatabeskyttelsesdirektivet.

Herefter opstiller EU-Domstolen i præmis 113-125 de betingelser en medlemsstat skal iagttage ved vedtagelsen af nationale logningsregler, herunder 1) at formålet med logningen skal være begrænset til grov kriminalitet, 2) at lovgivningen kun må pålægge teleudbydere målrettet logning af trafikdata og lokaliseringsdata, 3) at logningen skal være begrænset til det strengt nødvendige, 4) at nationale myndigheder, som har fået adgang til de loggede oplysninger, skal underrette de berørte personer herom, 4) at teleudbydere skal sikre effektiv beskyttelse og sikkerhed af de loggede oplysninger og 5) at oplysningerne ikke må overføres til lande uden for EU.

Der er således ingen tvivl om, at disse betingelser også finder anvendelse for nationale logningsregler, der har til formål at beskytte den nationale sikkerhed.

Det er derfor ikke korrekt, at Tele2-dommen ikke behandler spørgsmålet om, hvorvidt hensynet til den nationale sikkerhed kan begrunde logning i videre omfang. EU-Domstolen opsætter helt konkrete rammer for logningsreglerne, hvori ligger, at en mere indgribende logning pr. definition vil være i strid med EU-retten. Hvis EU-Domstolen havde været af den opfattelse, at en videre logning af hensyn til den nationale sikkerhed var en mulighed, havde EU-Domstolen taget stilling til dette i Tele2-dommen, da sagen netop vedrører lovgivning, der bl.a. har til formål at beskytte den nationale sikkerhed.

2. DET TILKOMMER IKKE EU-DOMSTOLEN AT TAGE KONKRET STILLING TIL HVORDAN NY LOVGIVNING SKAL INDRETTES

Det er korrekt, at Tele2-dommen ikke angår spørgsmålet om, hvor længe lovgivning i strid med EU-retten må opretholdes, og heller ikke indeholder konkrete anvisninger på, hvordan nationale logningsregler i stedet skal indrettes.

Det er imidlertid ikke EU-Domstolens opgave at vejlede medlemsstaterne i, hvordan lovgivning konkret skal indrettes, når denne er erklæret i strid med EU-retten. Dette tilkommer medlemsstaterne. Der kan på nuværende tidspunkt ikke herske nogen tvivl om, at sagsøgte ikke har handlet "hurtigst muligt", som påkrævet efter Jonkmann-dommen, uanset at sagsøgte måtte mene, at der er tale om retssikkerhedsmæssige problemer forbundet med en tilsidesættelse af logningsreglerne. Dette understreges af, at flere andre medlemsstater enten har suspenderet eller vedtaget ny lovgivning på området. Sagsøgte har derimod ikke foretaget sig noget mærkbart for at efterkomme EU-Domstolens afgørelse, udover at holde en række møder."

Foreningen imod Ulovlig Logning har i brevet endelig anført, at foreningen ikke er enig i, at der blot vil være tale om en kortvarig berostillelse af sagen, uanset om EU-Domstolen træffer afgørelse ved begrundet kendelse eller ej, ligesom foreningen ikke er enig i, at der er behov for at inddrage EU-Domstolen i den foreliggende sag.

EU-Domstolens sag C-520/18

Den belgiske Cour Constitutionelle (Forfatningsdomstolen) har den 2. august 2018 indgivet anmodning om præjudiciel afgørelse til EU-Domstolen, jf. C-520/2018 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres), og har i den forbindelse anmodet EU-Domstolen om at besvare følgende præjudicielle spørgsmål:

> "Skal artikel 15, stk. 1, i direktiv 2002/58/EF, sammenholdt med den ret til sikkerhed, der er sikret ved artikel 6 i Den Europæiske Unions charter om grundlæggende rettigheder, og retten til respekt for personoplysninger, som er sikret ved artikel 7, 8 og artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, fortolkes således, at bestemmelsen er til hinder for en national lovgivning – såsom den omhandlede, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata som omhandlet i direktiv 2002/58/EF, der genereres og behandles af dem inden for rammerne af udbuddet af disse tjenester – som ikke kun har efterforskning, afsløring og retsforfølgning af grov kriminalitet som formål, men ligeledes sikring af den nationale sikkerhed, forsvar af territoriet, den offentlige sikkerhed, efterforskning, afsløring og retsforfølgning af andre grunde end grov kriminalitet eller forebyggelse af ulovlig brug af elektroniske kommunikationssystemer eller gennemførelse af et andet formål i henhold til artikel 23, stk. 1, i forordning (EU) 2016/679, og som endvidere er undergivet præcise garantier i denne lovgivning vedrørende lagring af data og adgangen dertil?
>
> Skal artikel 15, stk. 1, i direktiv 2002/58/EF, sammenholdt med artikel 4, 7, 8, 11 og artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder fortolkes således, at bestemmelsen er til hinder for en national lovgivning – såsom den omhandlede, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata som omhandlet i direktiv 2002/58/EF, der genereres og behandles af dem inden for rammerne af udbuddet af disse tjenester – såfremt denne lovgivning bl.a. har til formål at opfylde de positive forpligtelser, der påhviler myndigheden i henhold til chartrets artikel 4 og 8, der består i at fastsætte en retlig ramme, der muliggør en effektiv strafferetlig efterforskning af og en effektiv retshåndhævelse over for seksuelt misbrug af mindreårige, og som rent faktisk gør det muligt at identificere gerningsmanden bag overtrædelsen, selv i tilfælde, hvor der gøres brug af elektroniske kommunikationsmidler?

> Såfremt Cour constitutionnelle (forfatningsdomstol) på grundlag af besvarelserne af det første og det andet præjudicielle spørgsmål konkluderer, at den anfægtede lov er i strid med en eller flere af de forpligtelser, der følger af de i disse spørgsmål nævnte bestemmelser, kan Cour constitutionnelle (forfatningsdomstol) da midlertidigt opretholde virkningerne af lov af 29. maj 2016 om indsamling og lagring af data i den elektroniske kommunikationssektor med henblik på at undgå retsusikkerhed og muliggøre, at data, der forinden er blevet indsamlet og lagret, stadig kan anvendes til de formål, der er omhandlet i loven?"

Landsretten afsagde

KENDELSE

Da besvarelsen af de præjudicielle spørgsmål i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres) må antages at have betydning for afgørelsen af den foreliggende sag, finder landsretten det påkrævet at udsætte behandlingen heraf for at afvente EU-Domstolens afgørelse, jf. retsplejelovens § 345. Sagsøgtes anmodning om udsættelse tages derfor til følge.

THI BESTEMMES:

Behandlingen af sagen udsættes med henblik på at afvente udfaldet af EU-Domstolens afgørelse i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres).

Sagen udsat herpå indtil videre til den 1. september 2019.

* I medfør af retsplejelovens § 221, stk. 1, berigtigede Østre Landsrets 14. afdelings retsbog dateret den 26. februar 2018, således at retsbogen dateres den 26. februar 2019.

Publiceret til portalen d. 14-03-2019 kl. 15:58
Modtagere: Advokat (L) Martin Von Haller Grønbæk, Advokat (H) Rass Markert Holdgaard, Sagsøger Foreningen imod Ulovlig Logning, Sagsøgte Justitsministeriet, Departementet

ØSTRE LANDSRET
RETSBOG

Den 30. september 2019 holdt Østre Landsret møde i retsbygningen i København.

Landsdommerne Benedikte Holberg, Rosenløv og Stine Fink-Hansen (kst.) behandlede sagen.

Sag BS-36799/2018-OLR
(14. afdeling)

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsministeriet
(advokat Rass Holdgaard)

Der er siden retsbog af 26. februar 2019 indleveret meddelelse af 30. august 2019 fra sagsøgte og breve af 30. august 2019 og 12. september 2019 fra sagsøgeren.

Sagsøgte, Justitisministeriet, har anmodet om, at sagen, der ved landsrettens kendelse af 26. februar 2019 blev udsat foreløbig til den 1. september 2019 på EU-Domstolens afgørelse i sag C-520/18, yderligere udsættes til den 1. marts 2020. Det er oplyst i anmodningen, at mundtlig forhandling i den pågældende sag skulle foretages den 9. og 10. september 2019.

Sagsøgeren, Foreningen imod Ulovlig Logning, har ved brev af 30. august 2019 anført følgende:

”…

I forbindelse med, at kendelse om foreløbig udsættelse af sagen udløber den 1. september 2019, anmoder jeg hermed på vegne af min klient, Foreningen Imod Ulovlig Logning, at Retten genovervejer sin kendelse om at udsætte sagen med henblik på at afvente udfaldet af EU-Domstolens afgørelse i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres).

Retten anmodes om at revurdere sin kendelse om at udsætte sagen henset til de nye oplysninger, der er kommet frem i medierne henover sommeren 2019 og som har udviklet sig til en regulær teleskandale, der kan have helt uoverskuelige konsekvenser for retssikkerheden og har skabt øget mistilid til det danske retssystem.

Der er således nu, om muligt, et endnu større behov for at få afgjort, hvorvidt Justitsministeriet ikke bare har behandlet de registrerede data ukorrekt, men måske slet ikke har haft lovligt grundlag til at få de pågældende data registreret og opbevaret i første omgang.

Teleskandalens baggrund
Den 13. juni 2019 meddelte Rigspolitiet og Rigsadvokaten, at fejl i itsystemer har ført til, at teleoplysninger brugt som bevismateriale i flere retssager har været mangelfulde og fejlbehæftede … Dette har betydet, at mangelfulde teleoplysninger og fejlagtige data om den sigtedes geografiske placering kan være blevet brugt som bevismateriale i flere end 10.000 sager, og at domstolene i disse sager dermed kan være blevet præsenteret for mangelfuld og/eller misvisende bevismateriale, som domstolene har truffet afgørelse på grundlag af. Rigspolitiet har været opmærksom på problemet siden februar 2019 og rettede angiveligt fejlen 8. marts, men valgte at udskyde offentliggørelse til efter folketingsvalget 5. juni 2019 …

Skandalen har siden sagen kom frem været massivt dækket i medierne, ligesom det har skabt bekymring hos flere, deriblandt forsvarsadvokater, folketingspolitikere og selv sagsøgte i nærværende sag, justitsminister Nick Hækkerup.

Tirsdag den 2. juli 2019 bad justitsministeren om en samlet redegørelse for alle relevante forhold i sagen og krævede, at uvildige eksperter inddrages i Rigspolitiets gennemgang af sagerne, herunder at eksperterne med en landsdommer i spidsen kontrollerer og styrer gennemgangen af straffesager omfattet af sagen …

For så vidt angår den tidsmæssige afgrænsning af sagen, spurgte Folketingets Retsudvalg den 17. juli 2019 ind til omfanget af skandalen,

som Rigspolitiet havde sat til 10.700 berørte sager fra 2012-2019 … I et brev til Folketingets Retsudvalg af 14. august … erkendte sagsøgte, at den tidsmæssige afgrænsning af sagen var større end først antaget, og at det dermed forventelig vil berøre endnu flere sager, også fra før 2012.

Fredag den 16. august 2019 oplyste Rigspolitiet til Justitsministeriet, at der ved en gennemgang af visse berørte straffesager er identificeret fejl i forbindelse med konverteringen af geografiske koordinater for telemasters placering, og søndag den 18. august 2019 blev det oplyst, at der ligeledes er identificeret fejl i den rådata, som politiet modtager fra teleselskaberne vedrørende teleoplysninger. Omfanget af, årsagen til og betydningen af disse fejl er endnu ikke afdækket. Der henvises til justitsministerens orientering til Folketingets Retsudvalg herom i …

Fremkomsten af disse oplysninger har betydet, at Rigsadvokaten har valgt midlertidig at suspendere brugen af teledata i straffesager indtil den 18. oktober 2019 …, og at flere varetægtsfængslede er blevet løsladt …, ligesom igangværende og kommende hovedforhandlinger, som anklagemyndigheden vurderer ikke vil kunne gennemføres uden anvendelsen af teleoplysninger må udsættes. Dette betyder også, at flere varetægtsfængslinger er blevet forlænget. Dommerformanden, Mikael Sjöberg, har i den forbindelse udtalt, at det er helt uoverskueligt, hvor stor betydning sagen vil få for det danske retssystem, jf. …

Justitsminister Nick Hækkerup har som følge af de nye oplysninger fra 16. og 18. august bedt om, at de nye oplysninger indgår i den samlede redegørelse, og har samtidig forlænget fristen for redegørelsen til udgangen af september 2019 …

Anmodning om revurdering af kendelse om udsættelse
I lyset af de seneste måneders begivenheder anmoder sagsøger om, at Retten i sin vurdering af, om sagen fortsat skal udsættes, tager i betragtning, at der er tale om et forhold af særlig samfundsmæssig relevans og af særlig indgribende karakter. Såfremt sagen fortsat udsættes, vil der fortsat ske en potentiel ulovlig registrering og opbevaring af teledata. Den samfundsmæssige betydning og risici forbundet hermed er aktualiseret og eksemplificeret ved den relevante teleskandale.

Sagsøger finder ikke, at den nuværende udsættelse af nærværende sag er påkrævet eller nødvendig, eller kan få indflydelse på sagen i

> en sådan grad, at det proportionelt kan undtage rettens altovervejende udgangspunkt om, at sagen skal behandles så hurtigt som muligt, særligt under hensyntagen til den alvorlige krænkelse af den danske befolknings rettigheder, som den forsatte logningsforpligtelse medfører.
>
> Sagsøger skal derfor anmode om, at Retten beslutter, at sagen ikke længere skal udsættes.
> …"

Ved brev af 12. september 2019 har sagsøgeren yderligere anført følgende:

> "…
> … der [er] intet grundlag for at forvente, at Domstolen har nået at træffe afgørelse i sag C-520/18 før den 1. marts 2020, idet generaladvokaten endnu ikke har fremsat forslag til afgørelse, og at det forsat er uvist, hvornår dette vil ske. Det bemærkes i den forbindelse, at der i Tele2/Watson-sagen (C-203/15 og C-698/15) af generaladvokaten blev fremsat forslag til afgørelse den 19. juli 2016, hvorefter Domstolen traf afgørelse i sagen den 21. december 2016, dvs. først 5 måneder senere, på trods af, at sagen var undergivet den fremskyndede procedure i henhold til artikel 105, stk. 1 i Domstolens procesreglement.
> …"

Landsretten afsagde

KENDELSE

Ved kendelse af 26. februar 2019 udsatte landsretten behandlingen af sagen med henblik på at afvente EU-Domstolens besvarelse af præjudicielle spørgsmål i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres), jf. retsplejelovens § 345. Landsretten finder det fortsat påkrævet, at sagen udsættes herpå. Det af sagsøgeren anførte kan på nuværende tidspunkt ikke føre til et andet resultat.

Sagsøgtes anmodning om fortsat udsættelse tages derfor til følge.

THI BESTEMMES:

Behandlingen af sagen udsættes fortsat med henblik på at afvente udfaldet af EU-Domstolens afgørelse i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres).

Sagen udsættes herpå indtil videre til den 1. marts 2020.

Retten hævet.

Publiceret til portalen d. 30-09-2019 kl. 14:27
Modtagere: Advokat (H) Rass Markert Holdgaard, Sagsøgte
Justitsministeriet, Departementet, Advokat (L) Martin Von Haller Grønbæk,
Sagsøger Foreningen imod Ulovlig Logning

ØSTRE LANDSRET
RETSBOG

Den 10. marts 2020 holdt Østre Landsret møde i retsbygningen i København.

Landsdommerne Benedikte Holberg, Rosenløv og Stine Fink Hansen (kst.) behandlede sagen.

Sag BS-36799/2018-OLR
(14. afdeling)

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsministeriet
(advokat Rass Holdgaard)

Der er siden retsbog af 30. september 2019 indleveret meddelelse af 4. marts 2020 fra sagsøgte og meddelelse af s.d. fra sagsøgeren.

Sagsøgte, Justitsministeriet, har ved meddelelse af 4. marts 2020 anmodet om, at sagen, der ved landsrettens kendelse af 30. september 2019 blev udsat foreløbig til den 1. marts 2020 på EU-Domstolens afgørelse i sag C-520/18, yderligere udsættes til den 1. juni 2020. Det er oplyst i anmodningen, at der siden seneste udsættelse er afgivet forslag til afgørelse fra Generaladvokaten i sagen ved EU-Domstolen, men at der fortsat ikke er afsagt dom. Det er forventningen, at Domstolen vil afsige dom i sagen i løbet af sommerhalvåret 2020.

Sagsøgeren, Foreningen imod Ulovlig Logning, har ved meddelelse af 4. marts 2020 anført følgende:

> "…
> Det er forsat uvist, hvornår der helt præcist vil falde dom i EU-Domstolens sag C-520/18…, og Retten anmodes derfor om at revurdere sin ken-

delse om at udsætte sagen af de grunde, der allerede er anført i vores tidligere breve til Retten. Herudover bemærkes, at det siden Retten sidste gang besluttede at lade sagen udsætte på trods af teleskandalen er kommet frem, at teleselskaber også registrerer og deler indholdet af borgernes sms-beskeder, at Rigspolitiet har vidst dette og at det er holdt hemmeligt for borgere, forsvarsadvokater og domstolene.

Som tidligere anført vil en yderligere udsættelse af sagen medføre en forsat ulovlig registrering og opbevaring af teledata. Sagsøger finder ikke, at den nuværende udsættelse af nærværende sag er påkrævet eller nødvendig, eller kan få indflydelse på sagen i en sådan grad, at det proportionelt kan undtage rettens altovervejende udgangspunkt om, at sagen skal behandles så hurtigt som muligt, særligt under hensyntagen til den alvorlige krænkelse af den danske befolknings rettigheder, som den forsatte logningsforpligtelse medfører.

Sagsøger skal derfor anmode om, at Retten beslutter, at sagen ikke længere udsættes."

Landsretten afsagde

KENDELSE

Ved kendelse af 26. februar 2019 udsatte landsretten behandlingen af sagen med henblik på at afvente EU-Domstolens besvarelse af præjudicielle spørgsmål i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres), jf. retsplejelovens § 345, foreløbigt til den 1. september 2019. Ved kendelse af 30. september 2019 tog landsretten en anmodning om fortsat udsættelse til følge frem til foreløbigt den 1. marts 2020.

Landsretten finder det fortsat påkrævet, at sagen udsættes på EU-Domstolens besvarelse af præjudicielle spørgsmål i den nævnte sag, og det af sagsøgeren anførte kan på nuværende tidspunkt, hvor EU-Domstolens dom må forventes at foreligge inden for overskuelig fremtid, ikke føre til et andet resultat. Sagsøgtes anmodning om fortsat udsættelse tages derfor til følge.

THI BESTEMMES:

Behandlingen af sagen udsættes fortsat med henblik på at afvente udfaldet af EU-Domstolens afgørelse i sag C-520/18 (Ordre des barreaux francophones et germanophone m.fl. mod Conseil des ministres).

Sagen udsættes herpå indtil videre til den 1. juni 2020.

Retten hævet.

Publiceret til portalen d. 10-03-2020 kl. 13:41
Modtagere: Sagsøger Foreningen imod Ulovlig Logning, Advokat (H) Rass Markert Holdgaard, Advokat (L) Martin Von Haller Grønbæk, Sagsøgte Justitsministeriet, Departementet

ØSTRE LANDSRET
RETSBOG

Den 17. august 2020 kl. 10.00 holdt Østre Landsret forberedende retsmøde for lukkede døre i retsbygningen i København.

Landsdommer Benedikte Holberg behandlede sagen.

Sag BS-36799/2018-OLR
(14. afdeling)

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsministeriet
(advokat Rass Markert Holdgaard)

I retsmødet var sagsøgeren repræsenteret af advokat Julie Bak-Larsen og sagsøgte af advokat Rass Markert Holdgaard og advokat Peter Ahlberg.

Advokat Peter Ahlberg meddelte, at EU-Domstolens dom efter det nu oplyste formentlig ikke kan forventes at foreligge før ultimo 2020 eller primo 2021.

Der var efter drøftelse enighed om at forhåndsberamme sagen og om, at der bør afsættes 1 ½ retsdag til hovedforhandlingen.

Sagen blev berammet til foretagelse **den 5. oktober 2021, kl. 9.30-15, og den 6. oktober 2021, kl. 9.30-12**, i landsrettens 16.afdeling, hvortil sagen vil blive omregistreret 4 uger før hovedforhandlingen. Den fortsatte forberedelse varetages indtil da af 14. afdeling.

Den videre forberedelse af sagen

Når EU-Domstolens dom foreligger, udsætter landsretten sagen på replik og derefter på duplik, idet begge parter herunder skal fremkomme med bemærkninger til betydningen af dommen for sagens videre forløb.

Der afholdes forberedende retsmøde med fremmøde i landsrettens 14. afdeling **den 3. maj 2021, kl. 10-11**, til drøftelse af eventuelle udestående spørgsmål.

Endelig tidsplan
Parterne skal senest **den 1. september 2021** indlevere endelig tidsplan til landsretten.

Berammelsesafgift
Sagsøgeren skal betale 2.000 kr. i afgift for hovedforhandlingen (berammelsesafgift). Afgiften skal indbetales via minretssag.dk senest **den 5. juli 2021**. Afgiften for hovedforhandlingen bortfalder/tilbagebetales, hvis landsretten senest 6 uger før hovedforhandlingen modtager meddelelse om, at sagen er bortfaldet.

Påstandsdokumenter
Parterne skal senest **den 28. september 2021** indlevere påstandsdokument til landsretten. Påstandsdokumentet skal udformes således, at det umiddelbart kan indgå i en dom.

Overskridelse af fristen kan få udeblivelsesvirkning, jf. retsplejelovens § 360, stk. 5, jf. § 357, stk. 1.

Ekstrakt
Sagsøgeren skal senest 14 dage før hovedforhandlingen forelægge et ekstraktudkast for sagsøgte og efter anmodning medtage yderligere materiale fra sagen.

Sagsøgeren skal herefter senest **den 28. september 2021** indlevere ekstrakt til landsretten. Inden samme frist skal sagsøgeren indlevere 3 eksemplarer af ekstrakten i papirform.

Overskridelse af fristen for indlevering af ekstrakt til landsretten kan få udeblivelsesvirkning, jf. retsplejelovens § 360, stk. 6, jf. § 357, stk. 3.

Juridiske materialesamlinger samt opgørelse over afholdte udgifter og udlæg
Eventuelle juridiske materialesamlinger bør – gerne som en fælles materialesamling – indleveres til landsretten, herunder tillige i papirform i 3 eksemplarer, senest en uge inden hovedforhandlingen.

Parterne anmodes endvidere om senest ved hovedforhandlingen at indlevere en specificeret opgørelse over afholdte udgifter og udlæg, som ønskes taget i betragtning ved landsrettens omkostningsafgørelse.

Yderligere information om behandlingen af civile sager ved landsretten
Der henvises i øvrigt til Østre Landsrets hjemmeside www.oestrelandsret.dk (sagsbehandling), hvor parterne kan finde nærmere oplysninger om sagsforberedelse, påstandsdokument, ekstrakt, tidsplan, materialesamling og hovedforhandling.

Sagen udsat.

Publiceret til portalen d. 19-08-2020 kl. 13:34
Modtagere: Advokat (H) Rass Markert Holdgaard, Sagsøgte
Justitsministeriet, Departementet, Advokat (L) Martin Von Haller Grønbæk,
Sagsøger Foreningen imod Ulovlig Logning

ØSTRE LANDSRET
RETSBOG

Den 23. november 2020 kl. 10.00 holdt Østre Landsret forberedende retsmøde for lukkede døre.

Landsdommer Benedikte Holberg behandlede sagen.

Sag BS-36799/2018-OLR
(14. afdeling)

Foreningen imod Ulovlig Logning
(advokat Martin Von Haller Grønbæk)

mod

Justitsministeriet
(advokat Rass Markert Holdgaard)

Retsmødet blev afholdt telefonisk.

I retsmødet var sagsøgeren repræsenteret af advokat Julie Bak-Larsen og sagsøgte af advokat Rass Markert Holdgaard og advokat Peter Ahlberg.

Dommeren bemærkede, at sagsøgeren ved meddelelse af 27. oktober 2020 har anmodet om, at hovedforhandlingen, der er berammet til den 5. og 6. oktober 2021, fremrykkes som følge af, at den dom fra EU-Domstolen, som sagen har været udsat på, nu er afsagt (dom af 6. oktober 2020 i sagerne C-511/18, C-512/18 og C-520/18). Sagsøgte har ved meddelelse af 3. november 2020 anført, at man ikke har bemærkninger hertil.

Advokat Rass Markert Holdgaard oplyste, at justitsministeren den 19. november 2020 har meddelt Folketingets Retsudvalg og Euroudvalg, at Justitsministeriet er ved at gennemgå dommen med henblik på at vurdere, i hvilket omfang Danmark vil kunne opretholde de gældende regler, og med henblik på at kun-

ne præsentere et udkast til revision af reglerne. I lyset heraf findes det for så vidt mere hensigtsmæssigt at opretholde den allerede foretagne berammelse.

Dommeren bemærkede, at sagen er anlagt i sommeren 2018, og at den EU-dom, som sagen efter ministeriets anmodning har været udsat på, nu foreligger, hvorfor mulighederne for en fremrykning af hovedforhandlingen bør afsøges.

Parterne meddelte på forespørgsel, at de fortsat finder, at der bør afsættes 1 ½ retsdag til hovedforhandlingen. Det er muligt, at sagen kan hovedforhandles på 1 retsdag, men det er hensigtsmæssigt for en sikkerheds skyld at afsætte 1 ½ dag hertil.

Sagen blev herefter efter aftale med parterne berammet til foretagelse **den 5. maj 2021, kl. 9.30-15, og den 6. maj 2021, kl. 9.30-12**, i landsrettens 16.afdeling, hvortil sagen vil blive omregistreret 2 uger før hovedforhandlingen. Den fortsatte forberedelse varetages indtil da af landsrettens 14. afdeling.

Den videre forberedelse af sagen
Dommeren bemærkede, at sagsøgte i svarskriftet af 24. september 2018 har opfordret sagsøgeren til at fremsende en medlemsliste med henblik på en vurdering af, om sagsøgeren har retlig interesse. Denne opfordring ses ikke besvaret.

Advokat Julie Bak-Larsen meddelte, at sagsøgeren vil fremsende en medlemsliste til sagsøgte straks.

Sagen blev efter aftale med parterne udsat på replik til **den 7. januar 2021** og derefter på duplik til **den 25. februar 2021**, idet begge parter herunder skal fremkomme med bemærkninger til betydningen af EU-dommen for sagens videre forløb.

Sagsøgeren skal **samtidig med replikken** indlevere endelig tidsplan. Tidsplanen skal være afstemt med sagsøgte.

Der blev endvidere fastsat frister for eventuelle yderligere processkrifter, for sagsøgerens vedkommende til **den 25. marts 2021** og for sagsøgtes vedkommende til **den 21. april 2021**.

Forberedelsen sluttes **den 21. april 2021**, jf. retsplejelovens § 356, stk. 1.

Det tidligere fastsatte forberedende retsmøde **den 3. maj 2021, kl. 10-11**, aflyses.

Påstandsdokumenter
Parterne skal senest **den 28. april 2021** indlevere påstandsdokument til landsretten. Påstandsdokumentet skal udformes således, at det umiddelbart kan indgå i en dom.

Overskridelse af fristen kan få udeblivelsesvirkning, jf. retsplejelovens § 360, stk. 5, jf. § 357, stk. 1.

Ekstrakt
Sagsøgeren skal senest 14 dage før hovedforhandlingen forelægge et ekstraktudkast for sagsøgte og efter anmodning medtage yderligere materiale fra sagen.
Sagsøgeren skal herefter senest **den 28. april 2021** indlevere ekstrakt til landsretten. Inden samme frist skal sagsøgeren indlevere 3 eksemplarer af ekstrakten i papirform.

Overskridelse af fristen for indlevering af ekstrakt til landsretten kan få udeblivelsesvirkning, jf. retsplejelovens § 360, stk. 6, jf. § 357, stk. 3.

Juridiske materialesamlinger samt opgørelse over afholdte udgifter og udlæg
Eventuelle juridiske materialesamlinger bør – gerne som en fælles materialesamling – indleveres til landsretten, herunder tillige i papirform i 3 eksemplarer, senest en uge inden hovedforhandlingen.

Parterne anmodes endvidere om senest ved hovedforhandlingen at indlevere en specificeret opgørelse over afholdte udgifter og udlæg, som ønskes taget i betragtning ved landsrettens omkostningsafgørelse.

Yderligere information om behandlingen af civile sager ved landsretten
Der henvises i øvrigt til Østre Landsrets hjemmeside www.oestrelandsret.dk (sagsbehandling), hvor parterne kan finde nærmere oplysninger om sagsforberedelse, påstandsdokument, ekstrakt, tidsplan, materialesamling og hovedforhandling.

Sagen udsat.

Publiceret til portalen d. 24-11-2020 kl. 07:57
Modtagere: Sagsøgte Justitsministeriet, Departementet, Advokat (L) Martin Von Haller Grønbæk, Sagsøger Foreningen imod Ulovlig Logning, Advokat (H) Rass Markert Holdgaard

Bird & Bird
Advokatpartnerselskab
Sundkrogsgade 21
2100 Copenhagen
Tel +45 72 24 12 12
Fax +45 72 24 12 13
twobirds.com

Københavns Byret
Domhuset
Nytorv 25
1450 København K

STÆVNING

Som advokat for

Foreningen imod Ulovlig Logning
CVR-nr. 39 30 93 86
Birkegade 15, 5. tv.
2200 København N
v./advokat Martin Von Haller
("Sagsøger")

Indstævner jeg herved

Justitsminister Søren Pape Poulsen
Justitsministeriet
Slotholmsgade 10
1216 København K
("Sagsøgte")

Bird & Bird

INDHOLDSFORTEGNELSE

Bird & Bird

Bird & Bird

1. PÅSTAND

Sagsøgte skal anerkende, at bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik er ugyldig.

2. INDLEDENDE BEMÆRKNINGER

Sagen handler om Sagsøgtes fortsatte uberettigede opretholdelse af en lovgivning i form af bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik ("Logningsbekendtgørelsen"). Sagsøger har insisteret på opretholdelsen, selvom sådanne generelle og vilkårlige krav til logning, der følger af Logningsbekendtgørelsen ved flere lejligheder er fundet i strid med EU-retten og retten til privatliv, beskyttelsen af sine personoplysninger og ytrings og informationsfriheden, som fastsat ved EMRK og EU-Chartret. Dette er direkte statueret af EU-Domstolen og anvendelsen af sådanne generelle og vilkårlige krav til logning er i øvrigt af samme årsag stoppet i andre sammenlignelige medlemsstater.

Logningsbekendtgørelsen indebærer en forpligtelse for alle teleudbydere til at logge sine kunders tele- og metadata med henblik på at give adgang til sådanne i efterforskningsøjemed.

De loggede oplysninger angår bl.a. for enhver kommunikation: hvem du har ringet til, hvornår, i hvor lang tid og hvor du og den, du har ringet til, befinder sig på tidspunktet for kommunikationen. Endvidere logges adgang til internettet, hvornår, hvordan og i hvilket omfang for hver internetaktivitet. De pågældende data gemmes af private udbydere i op til 1 år.

Som EU-Domstolen angiver i Digital Rights Ireland-dommen (C-293/12 og C-594) (herefter "Digital Rights Ireland"), jf. pkt. 3.5.1. nedenfor: *"Logningsdirektivets logningsregler omfatter alle personer, alle kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse, selv om personer ikke har nogen direkte eller indirekte forbindelse til grov kriminalitet. Det indebærer dermed et indgreb i de grundlæggende rettigheder for praktisk talt hele den europæiske befolkning."*

Der er således tale om logning af en særdeles stor mængde data af særlig indgribende karakter om alle i op til 1 år – bare for det tilfælde, at det kunne være belejligt for politiet at kigge ned i til efterforskning af særlige kriminelle handlinger i henhold til nogle særlige beskyttelsesforanstaltninger.

Logningsbekendtgørelsen er udstedt i medfør af Retsplejelovens § 786, stk. 4 og 7, der implementerer Europa Parlamentets og Rådets Direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (herefter "Logningsdirektivet").

I 2014 erklærede EU-Domstolen i Digital Rights Ireland Logningsdirektivet ugyldigt. EU-Domstolen begrundede dommen med, at Logningsdirektivet stred mod den Europæiske Unions Charter om Fundamentale Rettigheder ("Chartret"), henholdsvis art.

Bird & Bird

7 om respekt for retten til privatliv og familieliv, sit hjem og sin kommunikation, art. 8 om retten til beskyttelse af sine personoplysninger, samt med begrundelsen, at der ikke var tale om en proportional undtagelse efter art. 52, stk.1. De svenske og engelske nationale implementeringer af Logningsdirektivet blev tilsvarende fundet i strid med Chartret af EU-Domstolen i Tele2/Watson-dommen (C-203/15) ("Tele2/Watson-dommen").

Logning er således et område, der er underlagt EU-retten. Danmark kan derfor ikke under henvisning til det EU-retlige forrangsprincip indføre eller opretholde danske logningsforpligtelser i Logningsbekendtgørelsen, der strider imod EU-retten; herunder EU-Domstolens afgørelser.

Derudover er Logningsbekendtgørelsen i strid med dansk ret i form af Chartret og EMRK. Konkret Chartrets art. 7,8 og 11 og EMRK art. 8 og 10.

På trods heraf har Sagsøgte valgt fortsat at opretholde og håndhæve Logningsbekendtgørelsen i Danmark. Sagsøgte tager ikke effektive skridt til at ændre de nuværende uretmæssige danske logningskrav, men har gentagne gange udskudt behandlingen af revisionen af Logningsbekendtgørelsen og har endvidere vægret sig mod at ændre kravet i det hele taget.

De danske udbydere ønsker ikke at krænke borgernes rettigheder ved at være tvunget til en fortsat retsstridig generel logning og opbevaring af alle deres kunders teleoplysninger. Danske borgere vil heller ikke acceptere en fortsat indgribende krænkelse af deres privatliv og ytringsfrihed, der både er i strid med dansk lovgivning, EU-retten og menneskeretten.

Som EU-Domstolen anfører i Digital Rights Ireland, jf. punkt 3.5.1 nedenfor i præmis 51: "*Hvad angår spørgsmålet, om den datalagring, som er foreskrevet i Logningsdirektivet, er nødvendig, skal det fastslås, at bekæmpelse af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, ganske vist er af afgørende betydning for at sikre den offentlige sikkerhed, og at effektiviteten heraf i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker. **Et sådan mål af almen interesse kan imidlertid, hvor grundlæggende den end er, ikke i sig selv begrunde, at en foranstaltning med henblik på datalagring som den, der er anført i Logningsdirektivet, anses for nødvendig af hensyn til bekæmpelsen af grov kriminalitet.***"

Sagsøger har derfor som en bred repræsentant for udbydere og slutbrugere anlagt denne sag for at påbyde Sagsøgte at respektere EU retten og menneskeretten, efterleve EU-Domstolens afgørelser og begrænse det fortsatte brud på danske borgeres retssikkerhed i form af beskyttelse af deres teleoplysninger.

Logningsbekendtgørelsen er ugyldig. Sagsøger søger hermed Rettens bistand til at få stoppet justitsministerens fortsatte uhjemlede opretholdelse af Logningsbekendtgørelsen ved at stadfæste anerkendelse af Logningsbekendtgørelsen som ugyldig.

Bird & Bird

3. SAGSFREMSTILLING

3.1 Sagens parter

3.1.1 Sagsøger

Sagsøger er en forening, der er oprettet med henblik på at påtale Sagsøgtes ugyldige opretholdelse af Logningsbekendtgørelsen.

Foreningen består af en bred medlemsskare, som alle er berørte af Sagsøgtes opretholdelse af Logningsbekendtgørelsen. Blandt medlemskredsen er private, der er genstand for den uretmæssige logning, it-professionelle der gennemfører den uretmæssige logning, teleudbydere, der skal foretage indgrebet i deres kunders privatliv ved at gennemføre den uretmæssige logning, samt interesseorganisationer for opretholdelse af grundlæggende menneskerettigheder.

Sagsøgtes vedtægter fremlægges som **bilag 1.** Det følger af disses punkt 2.1, at foreningens formål er at "*forberede, koordinere og støtte, herunder økonomisk, sagsanlæg ved danske domstole med det formål at få kendt Logningsbekendtgørelsen ulovlig.*"

Foreningen er således en interessesammenslutning, der er stiftet med henblik på anlæggelse af nærværende sag.

3.1.1.1 Sagsøgers retlige interesse

Det lægges til grund, at Sagsøger har fornøden retlig interesse.

Foreningens medlemmer har stiftet Foreningen for at forfølge sit formål sammen, da Foreningens medlemmer enkeltvist, hverken fagligt eller økonomisk, har ressourcer til at forfølge sine rettigheder ved anlæggelse af separate sager. Dannelsen af interessesammenslutningen som en forening har således været en nødvendig forudsætning for, at medlemmerne kan forfølge deres retlige interesse i at få kendt logningskravet i Logningsbekendtgørelsen ugyldigt.

I dansk ret er retlig interesse et dynamisk begreb, der nærmere fastsættes i retspraksis. At have retlig interesse kan sidestilles med at have en i retligt henseende beskyttelsesværdig interesse.

I litteraturen antages det, jf. til eksempel U.2000.B.319 af professor lic.jur. Gorm Toftegaard Nielsen, at "retlig interesse" forudsætter, at tre kumulative betingelser er opfyldt:

i. om spørgsmålet, der ønskes forelagt domstolene, er **egnet til at blive afgjort af domstolene**,

ii. om spørgsmålet er **aktuelt**, og

iii. om **den potentielle sagsøger har tilstrækkelig tilknytning til sagen.**

Det lægges indledningsvist til grund, **at domstolene i deres natur har kompetence** til at afgøre dette retslige spørgsmål, idet spørgsmålet blandt andet vedrører afgrænsningen mellem national ret og EU-ret.

Bird & Bird

Dernæst har spørgsmålet **aktualitet**, idet logningskravet fortsat de facto opretholdes i strid med menneskeretten og EU-retten, som nærmere uddybet nedefor i afsnit 3.6.

I forhold til Sagsøgers **tilstrækkelige tilknytning til sagen** kan anføres, at Logningsbekendtgørelsen har danske udbydere som pligtsubjekter og danske statsborgere som retssubjekter. Således har Logningsbekendtgørelsen direkte virkning på Sagsøger (foreningens medlemmer), idet Logningsbekendtgørelsen indskrænker disses rettigheder, sådan som disse er fastsat i Chartret (art. 7,8 og 11)og EMRK (art. 10). Det bemærkes i den forbindelse, at EMRK artikel 8 beskytter såvel fysiske som juridiske personers privatliv, jf. Lorenzen et al, EMRK med kommentarer (2011), s. 642 f.

EMRK artikel 8 og Chartrets artikel 7 pålægger endvidere den danske stat at tilvejebringe en effektiv domstolskontrol mod indgreb i borgernes privatliv. Foreningens medlemmer har således en interesse i, at statens positive forpligtelse til at sikre individets ret til privatliv håndhæves.

Foreningers søgsmålsret er endvidere anerkendt i retspraksis, jf. U.1994.780 Ø ("Greenpeace-dommen"). I Greenpeace-dommen anerkendte landsretten, at Greenpeace som forening kunne anlægge et civilt søgsmål mod Trafikministeriet med påstand om, at en afgørelse var i strid med lovgivningen. Landsretten begrundede i sagen blandt andet søgsmålsretten med at: *"søgsmålet klart faldt inden for det formål, der er beskrevet i Greenpeaces vedtægter*." Med Greenpeace-dommen anerkendes således den ideelle foreningsinteresse som et legitimt og tilstrækkeligt motiv for at indlede en retssag.

Det følger af bilag 1, at formålet med Sagsøgers forening netop indeholder en retlig forfølgelse af sin interesse i at bringe uberettiget logning til ophør.

Videre henvises til Højesterets dom af 12. august 1996 ("Maastricht-dommen"), som vedrørte spørgsmålet om, hvorvidt Danmarks tiltrædelse af Maastrichttraktaten var grundlovsstridig. I denne sag fik en række borgere realitetsbehandlet deres sag, idet de af Højesteret blev anerkendt til at have retlig interesse. Højesteret udtalte i denne formalitetsafgørelse, at:

"Ved afgørelsen af, om appellanterne bør have adgang til at få dette spørgsmål prøvet ved domstolene, må der lægges vægt på, at tiltrædelsen af Traktaten om Den Europæiske Union indebærer overførsel af lovgivningskompetence inden for en række ***almene og væsentlige livsområder og derfor i sig selv er af indgribende betydning for den danske befolkning i almindelighed.***

[...]

"På grund af tiltrædelseslovens **generelle og indgribende betydning** *har appellanterne en væsentlig interesse i at få deres påstande prøvet."*

[...]

"Højesteret finder herefter, at appellanterne har fornøden retlig interesse i at få deres påstande prøvet. Der er ikke tilstrækkeligt grundlag for at fastslå, at påstandene efter deres udformning eller af andre grunde er uegnede til at blive taget under påkendelse."

Bird & Bird

Denne sag har tilsvarende generel og indgribende betydning for den danske befolkning, ligesom der er tale om almene og væsentlige livsområder, der derfor i sig selv er af indgribende betydning for den danske befolkning i almindelighed. Det er tilfældet, idet Logningsbekendtgørelsen indebærer en omfattende registrering af alle slutbrugere – dvs. næsten hele den danske befolknings trafik og lokaliseringsdata – i strid med Chartret og EMRK.

3.1.2 Sagsøgte

Sagsøgte er justitsministeren. Sagsøgte er i medfør af lovgivningen bemyndiget til at udstede lovgivning vedrørende logning af telekommunikation, hvorfor ansvaret for denne lovgivnings lovlighed tilsvarende påhviler justitsministeren, jf. også lov nr. 1964-04-15 nr. 117 (ministeransvarsloven) §§ 4-5, jf. også lov nr. 169 af 5. juni 1953 (grundloven) § 14 stk. 1, 4. pkt.

At sagsøge den ansvarlige minister frem for Justitsministeriet er i overensstemmelse med Maastricht-dommen, hvor sagsøgte i begge instanser tilsvarende var den relevante ressortminister.

3.2 Baggrund for Logningsdirektivet og Logningsbekendtgørelsen

3.2.1 Direktiv 95/46/EF om persondatabeskyttelse

Europa-Parlamentets og Rådets dagældende direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter "**Persondatadirektivet**") har i henhold til dets artikel 1, stk. 1 til formål at sikre beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger. Persondatadirektivet er implementeret i dansk ret ved dagældende persondatalov.

Med hensyn til sikkerheden af behandlingen af sådanne oplysninger bestemmer Persondatadirektivs artikel 17, stk. 1:

"Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling."

Foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

3.2.2 Direktiv 2002/58/EF om e-databeskyttelse

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (herefter "direktiv 2002/58") (herefter "**E-databeskyttelsesdirektivet**"), har i henhold til dets artikel 1, stk. 1, til formål at harmonisere medlemsstaternes be-

Bird & Bird

stemmelser, som er nødvendige for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Den Europæiske Union.

I henhold til artikel 1, stk. 2 specificerer og supplerer E-databeskyttelsesdirektivet bestemmelserne i Persondatadirektivet for så vidt angår telesektoren.

Med hensyn til **sikkerhed i forbindelse med behandlingen af** dataene bestemmer **artikel 4** i E-databeskyttelsesdirektivet:

"Udbyderen af en offentligt tilgængelig kommunikationstjeneste skal træffe passende tekniske og organisatoriske foranstaltninger for at beskytte sine tjenester, for netsikkerhedens vedkommende om nødvendigt sammen med udbyderen af det offentlige kommunikationsnet. Under hensyn til teknologiens stade og omkostningerne i forbindelse med gennemførelsen skal disse foranstaltninger garantere et sikkerhedsniveau, der står i forhold til risikoen."

De i E-databeskyttelsesdirektivet stk. 1 omhandlede foranstaltninger skal som minimum:

- *"sikre, at kun autoriserede personer får adgang til personoplysningerne til lovlige formål,*
- *beskytte lagrede eller sendte personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse, og*
- *gennemføre en sikkerhedspolitik for behandling af personoplysninger."*

De relevante nationale myndigheder skal kunne kontrollere foranstaltninger truffet af udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og udstede henstillinger om bedste praksis vedrørende det sikkerhedsniveau, som disse foranstaltninger bør føre til.

Hvor der er særlig risiko for brud på netsikkerheden, skal udbyderen af en offentligt tilgængelig kommunikationstjeneste informere abonnenterne herom samt, hvis risikoen ligger uden for de foranstaltninger, der skal træffes af udbyderen, om, hvorledes sådanne brud i givet fald kan forebygges, herunder angive de omkostninger, der sandsynligvis vil være forbundet hermed.

For så vidt angår **kommunikationshemmelighed og fortrolighed af trafikdata bestemmer E-databeskyttelsesdirektivets artikel 5, stk. 1 og 3:**

"Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. ***De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri,***

Bird & Bird

bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15 stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf."

Medlemsstaterne sikrer, at **lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med Persondatadirektivet at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen**.

Dette er ikke til hinder for **teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.**

E-databeskyttelsesdirektivets **artikel 6 stk. 1** bestemmer følgende:
"Trafikdata *vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste,* ***skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3 og 5 samt artikel 15 stk. 1."***

Artikel 15 stk. 1 i E-databeskyttelsesdirektivet bestemmer herefter:

*"**Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er:***

- *nødvendig, passende og forholdsmæssig i et demokratisk samfund*
- *af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv 95/46/EF.*
- *Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke.*
- *Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2."*

E-databeskyttelsesdirektivet indeholder dermed helt klare krav til behandling af persondata i telesektoren vedrørende sikkerhed, sikring af kommunikationshemmeligheden og privatlivets fred, herunder ved konkrete krav til, hvem der kan få adgang til data, forbud mod lagring i andre tilfælde end for trafikfremføring eller debitering og ellers alene efter abonnentens samtykke. Sådanne forhold kan dog undtages efter artikel 15 stk.1, hvis nogle af de pågældende undtagelsesforhold finder anvendelse – og dette er i overensstemmelse med Chartrets.

E-databeskyttelsesdirektivet er implementeret i dansk ret ved bekendtgørelse nr. 715 af 23/06/2011 om udbud af elektroniske kommunikationsnet og –tjenester ("**Ud-**

Bird & Bird

budsbekendtgørelsen") i medfør af bemyndigelse i Lovbekendtgørelse nr. 128 af 7. februar 2014 ("**Teleloven**").

3.2.3 Direktiv 2006/24 Logningsdirektivet

Efter at have iværksat en høring med deltagelse af repræsentanter for de retshåndhævende myndigheder, den elektroniske kommunikationssektor og eksperter i databeskyttelse fremlagde Kommissionen den 21. september 2005 en konsekvensanalyse af de politiske alternativer vedrørende regler om lagring af. Denne analyse dannede grundlag for udarbejdelsen af forslaget til Logningsdirektivet, der blev forelagt samme dag, og som førte til vedtagelsen af Logningsdirektivet på grundlag af artikel 95 EF.

Ved Logningsdirektivet blev medlemsstaterne uanset artikel 5 og 6 i E-databeskyttelsesdirektivet pålagt at sikre lagring af trafikdata.

Fjerde betragtning til Logningsdirektivet har følgende ordlyd:

"I artikel 15 stk. 1, i direktiv 2002/58/EF (E-databeskyttelsesdirektivet) fastsættes de betingelser, i henhold til hvilke medlemsstaterne kan indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i nævnte direktivs artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9. En sådan indskrænkning skal være nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den offentlige ro og orden, f.eks. den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem"

Ifølge første punktum i femte betragtning til Logningsdirektivet *"[har] [m]ange medlemsstater […] vedtaget lovgivning om tjenesteudbyderes lagring af data med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger«.*

Syvende til ellevte betragtning til Logningsdirektivet har følgende ordlyd:

"(7) I sine konklusioner af 19. december 2002 fremhæver Rådet (retlige og indre anliggender), at den betydelige vækst i de muligheder, der ligger i elektronisk kommunikation, har medført, at data vedrørende anvendelsen af elektronisk kommunikation udgør et særdeles vigtigt og brugbart redskab i forebyggelse, efterforskning, afsløring og retsforfølgning af kriminalitet og strafbare handlinger, især organiseret kriminalitet."

"(8) I erklæringen om bekæmpelse af terrorisme, der blev vedtaget af Det Europæiske Råd den 25. marts 2004, blev Rådet pålagt at behandle foranstaltninger vedrørende opstilling af regler for tjenesteudbyderes lagring af kommunikationsdata."

"(9) Ifølge artikel 8 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (den europæiske menneskerettighedskonvention) [undertegnet i Rom den 4. november 1950, herefter »EMRK«] har enhver ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. Offentlige myndigheder må kun gøre indgreb i udøvelsen af denne ret, hvis det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til bl.a. den nationale sikkerhed og den offentlige tryghed for at forebygge uro eller forbrydelse eller for at beskytte andres rettigheder og friheder. Da lagring af data har vist sig at

Bird & Bird

være et sådant nødvendigt og effektivt efterforskningsredskab for retshåndhævelsen i flere medlemsstater, herunder navnlig i alvorlige sager som organiseret kriminalitet og terrorisme, er det nødvendigt at sikre, at de lagrede data er tilgængelige i forbindelse med håndhævelsen af loven i en vis periode på de vilkår, der er fastsat i dette direktiv. […]"

"(10) Den 13. juli 2005 bekræftede Rådet på ny i sin erklæring om fordømmelse af terroristangrebene i London, at det er nødvendigt snarest muligt at vedtage fælles foranstaltninger vedrørende lagring af telekommunikationsdata."

"(11) Det er i undersøgelser blevet påvist, og medlemsstaterne har praktisk erfaring for, at trafikdata og lokaliseringsdata har stor betydning i efterforskning, afsløring og retsforfølgning af strafbare handlinger, og det er derfor nødvendigt på europæisk plan at sikre, at data, som genereres eller behandles af udbydere af elektronisk kommunikation, når de tilbyder offentlige elektroniske kommunikationstjenester eller offentlige kommunikationsnet, lagres i en vis periode på de i dette direktiv fastsatte betingelser."

16., 21. og 22. betragtning til Logningsdirektivet præciserer:

"(16) De forpligtelser, der i medfør af artikel 6 i direktiv 95/46/EF påhviler tjenesteudbyderne med hensyn til foranstaltninger til at sikre datakvaliteten samt deres forpligtelser i medfør af artikel 16 og 17 i nævnte direktiv med hensyn til foranstaltninger til at sikre fortrolighed og behandlingssikkerhed, finder fuldt ud anvendelse på data, der lagres i overensstemmelse med nærværende direktiv."

"(21) Målene for dette direktiv, nemlig at harmonisere udbydernes pligt til at lagre visse data og sikre, at disse data gøres tilgængelige i forbindelse med efterforskning, afsløring og retsforfølgning af alvorlige forbrydelser som defineret af de enkelte medlemsstater i deres nationale lovgivning, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor på grund af direktivets omfang og virkninger bedre gennemføres på fællesskabsplan. Fællesskabet kan derfor træffe foranstaltninger i overensstemmelse med subsidiaritetsprincippet, jf. traktatens artikel 5. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke ud over, hvad der er nødvendigt for at nå disse mål."

"(22) I dette direktiv overholdes de grundlæggende rettigheder og de principper, som bl.a. Den Europæiske Unions charter om grundlæggende rettigheder anerkender. Dette direktiv tilstræber sammen med direktiv 2002/58/EF navnlig at sikre, at de grundlæggende rettigheder overholdes i fuldt omfang, herunder at privatlivets fred og borgernes ret til kommunikation respekteres, samt at der sørges for beskyttelse af personoplysninger jf. artikel 7 og 8 i chartret."

Logningsdirektivets art. 3 fastsætter en pligt for udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet til at lagre visse data, der genereres eller behandles af dem.

Herudover fastsætter art. 4 en pligt for disse udbydere til at give kompetente nationale myndigheder adgang til disse data i særlige sager.

3.2.4 Retsplejelovens § 786, stk. 4 og 7

Logningsdirektivet blev implementeret ved Retsplejelovens § 786, stk. 4 og 7.

Bird & Bird

Bestemmelser om logning var allerede indsat i Retsplejeloven ved Lov nr. 378 af 6. juni 2002 om ændring af straffeloven, Retsplejeloven m.fl., som led i gennemførelsen af FN-konventionen til bekæmpelse af finansiering af terrorisme, FN's Sikkerhedsråds resolution nr. 1373 samt øvrige initiativer til bekæmpelse af terrorisme, men blev herefter tilpasset som følge af Logningsdirektivet den 15. september 2007 i henhold til bekendtgørelse nr. 986 af 28. september 2006.

Efter Retsplejelovens § 786, stk. 4, påhviler det således udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Ressortministeren kan fastsætte nærmere regler herom. Efter Retsplejelovens § 786, stk. 7 kan der fastsættes bestemmelser om bødestraf ved overtrædelse af de regler, som Sagsøgte fastsætter efter stk. 4.

Retsplejelovens regler fastsætter derudover, i hvilke tilfælde politiet i efterforskningsøjemed kan få adgang til loggede data, hvilket alene er ved forevisning af retskendelse og hovedsagligt ved mistanke om særlig farlig kriminalitet.

3.2.5 Logningsbekendtgørelsen

I medfør af Retsplejelovens § 786, stk. 4 og 7 blev Logningsbeføjelsen anvendt ved vedtagelsen af en bestemmelse Teleloven, der blev udmøntet ved Logningsbekendtgørelsen, der også trådte i kraft den 15. september 2007.

Det fremgår af Logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket *udbyder* skal forstås i overensstemmelse med samme udtryk i Telelovens § 2, nr. 1. Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Udbyderbegrebet er ganske bredt og dækker både traditionelle teleudbydere, såsom tele, mobil og bredbåndsudbydere, samt udbydere af nye teknologier, der baserer sig på internetforbindelse, samt generel wifi-adgang, mv. Der er således tale om en ganske bred skare af udbydere, der skal logge en meget stor mængde data.

Efter Logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a.:

i. oplysninger om det opkaldende og det opkaldte nummer,

ii. tidspunktet for kommunikationens start og afslutning,

iii. og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet,

iv. samt oplysninger om anonyme tjenester (taletidskort).

Bird & Bird

Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår, i hvor lang tid og hvor de befandt sig på tidspunktet for kommunikationen.

Efter Logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Ifølge Logningsbekendtgørelsens § 6 skal udbyderne også registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne er ikke pålagt at registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

De registrerede oplysninger opbevares i 1 år, jf. Logningsbekendtgørelsens, § 9, og manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. § 10, idet bødebestemmelsen dog endnu ikke er set anvendt i praksis.

Loggede data kan alene udleveres til politiet efter retskendelse, og der er endvidere et krav om, at personel hos udbyderne, der har adgang til de loggede data skal være sikkerhedsgodkendt.

3.3 Chartret

Det følger af Chartrets **artikel 7,** at *"enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation".*

Af Chartrets **artikel 8** følger, at "*enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til en berigtigelse heraf. […]*"

Videre følger af **Chartrets artikel 11,** at "*enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser."*

Slutteligt følger af **Chartrets artikel 52 stk. 1,** at *"enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved dette charter, skal være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste forhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder."*

Chartret er en fuldgyldig del af dansk ret, da Chartret med Lissabon-Traktatens ikrafttræden blev juridisk bindende på EU-niveau og dermed også finder direkte anvendelse i samtlige medlemsstater, inklusive Danmark.

Sagsøgte er derfor udtrykkeligt forpligtet til at overholde Chartret, jf. legalitetsprincippet og Chartrets art. 51, stk. 1, der foreskriver, at Chartret "*er rettet til Unionens in-*

Bird & Bird

stitutioner, organer, kontorer og agenturer under iagttagelse af nærhedsprincippet samt til medlemsstaterne, dog kun når de gennemfører EU-retten".

Danmark er derfor forpligtet til at overholde Chartret, når den gennemfører EU-retten, og er således, når den vedtager og håndhæver Logningsbekendtgørelsen, som er et område, der er underlagt EU-retten, forpligtet til at overholde Chartret og særligt fortolkningen heraf i EU-Domstolens afgørelser i Digital Rights Ireland og Tele2/Watson.

3.4 EU-retten

3.4.1 EU-rettens forrangsprincip

Danmark tiltrådte de Europæiske Fællesskaber den 1. januar 1973.

Ved Danmarks tiltrædelse af EF-samarbejdet (senere EU) blev der indført en særlig retsorden, som medførte en vis suverænitetsafgivelse til EU. Denne suverænitetsafgivelse er hjemlet i dansk ret ved grundlovens § 20 og lov 1972/447 om Danmarks tiltrædelse af EF ("Tiltrædelsesloven").

Suverænitetsafgivelsen medfører, at visse kompetencer kan overlades til mellemfolkelige myndigheder (EU). De konkrete suverænitetsafgivelser skal dog konkret vedtages i specifikke traktater.

Rådets kompetence til at harmonisere medlemsstaters love følger af bl.a. artikel 94 og 95 i traktaten om den Europæiske Union og traktaten om oprettelse af det europæiske fællesskab (2002/C 325/1) (herefter "Nice traktaten"). EU har med hjemmel heri kompetence til at fastsætte regler vedrørende *det fælles markeds oprettelse og funktion*.

Medlemsstaterne kan i naturlig forlængelse af denne kompetenceoverdragelse ikke have en national lovgivning, der strider mod EU-lovgivning, hvortil medlemsstaterne har overdraget dens kompetence til EU. Dette betegnes forrangsprincippet. Forrangsprincippet er ved flere lejligheder blevet fastslået. I EU 6/64, Costa mod Enel, udtalte EU-Domstolen til eksempel "*en senere ensidig retsakt kan ikke gå forud for fællesskabsretten*".

Også de danske domstole har taget stilling til forrangsprincippet, jf. Maastricht-dommen og U.2017.824 ("Ajos"). De danske domstole anerkender ligeledes forrangsprincippet under forudsætning af, at EU-retten ikke har forrang frem for grundloven samt at EU-retsakten ikke overskrider grænserne for den ved Tiltrædelsesloven afgivne suverænitet.

Tvisten i denne sag vedrører netop det forhold, at Logningsbekendtgørelsen går imod EU-retten bl.a. i form af EU-Domstolens afgørelser i Digital Rights Ireland og Tele2/Watson. Dette er i strid med det EU-retlige forrangsprincip. Danmark kan således ikke opretholde lokal lovgivning, der strider mod et område, som Danmark har afgivet kompetence til EU om at lovgive på.

Det er på denne baggrund Sagsøgers opfattelse, at Logningsbekendtgørelsen allerede under henvisning til det EU-retlige forrangsprincip må findes ugyldig.

Bird & Bird

3.4.2 Domstolen er forpligtet til EU-konform fortolkning

Danske domstole skal tage E-databeskyttelsesdirektivet, Chartret og EU-domstolens praksis i betragtning, når de behandler denne sag.

Domstolene er derfor forpligtet til at fortolke dansk ret på en måde, der er forenelig med EU-reguleringen på området, og som ikke kommer i konflikt med de grundlæggende rettigheder eller almindelige EU-retlige principper.

Denne fortolkningsregel er senest blevet fastslået ved EU-Domstolens afgørelse i Ajos-sagen (sag C-441/14), hvor EU-domstolen udtalte, at en national domstol er forpligtet til at anvende nationale retsregler i overensstemmelse med EU-retten, og at det endvidere ikke kan være en hindring for at foretage EU-konform fortolkning, at der foreligger en fast national praksis. I så fald skal nationale domstole ændre denne faste praksis.

Der er således ingen tvivl om, at danske domstole ved stillingtagen til danske regler altid er forpligtet til at fortolke i overensstemmelse med EU-retten og EU-Domstolens praksis. Retten er derfor forpligtet til at vurdere denne sag i overensstemmelse med bl.a. Digital Rights Ireland og Tele2/Watson.

3.5 EU-Domstolens afgørelser om, at Logningsdirektivet og nationale logningsregler strider mod Chartret

3.5.1 Digital Rights Ireland (C-293/12)

Ved dom af 8. april 2014 i Digital Rights Ireland erklærede EU-Domstolen Logningsdirektivet for ugyldigt med henvisning til, at EU-lovgiver havde overskredet de grænser, der følger af proportionalitetsprincippet i artikel 7, 8 og 52, stk. 1 i Chartret.

Sagen var en præjudiciel forelæggelse fra både den irske High Court og den tyske Verfassungsgerichtshof i nationale sager der vedrørte, hvorvidt Logningsdirektivet var i strid med EMRK art. 8 og 10 og Chartrets art. 7, 8 og 52. stk. 1..

EU-Domstolen indledte med at bemærke i præmis 27, at: "*Disse data vil tilsammen kunne gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter, der udøves, disse personers sociale relationer og de miljøer, de frekventerer*."

I afgørelsen fastlagde EU-Domstolen indledningsvist i præmis 34-36, at teleudbydernes pligt til at lagre trafik- og lokaliseringsdata og de kompetente myndigheders adgang til dataene **udgør et klart og alvorligt indgreb i retten til respekt for privatliv og retten til beskyttelse af personoplysninger, der er sikret ved Chartrets artikel 7 og 8**. Ligesom EU-Domstolene bemærkede, at "*den omstændighed, at lagringen af data og den efterfølgende anvendelse af dem finder sted, uden at abonnenten eller den registrerede bruger oplyses herom, er desuden [..] egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning*".

EU-Domstolen indledte herefter en undersøgelse af, om indgrebet var begrundet, proportionelt og hjemlet i lov. EU-Domstolen udtaler i præmis 38: "*I henhold til Chartrets artikel 52, stk. 1. skal enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved Chartret, være fastlagt i lovgivningen og respektere*

disse rettigheders og friheders væsentlige indhold, og der kan under iagttagelse af proportionalitetsprincippet kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder."

EU-Domstolen fastlagde i den forbindelse i præmis 38-40, at Logningsdirektivet ikke indebar en krænkelse af det væsentligste indhold af retten til respekt for privatliv og familieliv og retten til beskyttelse af personoplysninger. EU-Domstolen lagde i den forbindelse vægt på, at Logningsdirektivet ikke var i strid med art. 7 i Chartret, da Logningsdirektivet ikke indebærer lagring af kommunikationens indhold. Omfang og misbrug af metadata var anderledes i 2014 end i 2016 og i dag, og EU-Domstolen gik da også bort fra dette synspunkt i Tele2/Watson sagen, hvor metadata anses for en ligeså beskyttelsesværdig interesse som kommunikationens indhold, jf. pkt. 3.5.2 nedenfor.

EU-Domstolen fandt endvidere, at pligten til at gøre disse data tilgængelige for de kompetente myndigheder i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet forfølger et mål for EU af almen interesse, da det bidrager til bekæmpelsen af grov kriminalitet og international terrorisme og i sidste ende til den offentlige sikkerhed, jf. præmis 41-44.

EU-Domstolen undersøgte herefter om Logningsdirektivets indgreb i rettighederne fastlagt i Chartrets artikel 7 og 8 var proportionalt, herunder om reglerne i Logningsdirektivet er egnede til at gennemføre målet, og om det gik videre, end hvad der var nødvendigt og passende for at nå det tilsigtede mål.

I præmis 49 og 51-53 udtalte EU-Domstolen, at logningspligten var egnet til at gennemføre det mål, Logningsdirektivet forfølger, men at det imidlertid ikke er proportionelt, uanset Logningsdirektivet anses for nødvendig for at bekæmpe grov kriminalitet. **Efter EU-Domstolens faste praksis kræver beskyttelsen af personoplysninger endvidere, at undtagelser fra eller begrænsninger i beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige**, jf. C-473/12 af 7. november 2013 29 (IPI), præmis 39, C-73/07 af 16. december 2008 (Satakunnan Markkinapörssi og Satamedia) præmis 56 samt de forenede sager C-92/09 og C-93/09 af 9. november 2011 (Volker und Markus Schecke og Eifert) præmis 77 og 86.

EU-Domstolen anfører bl.a. i præmis 51, at *"Hvad angår spørgsmålet, om den datalagring, som er foreskrevet i Logningsdirektivet, er nødvendig, skal det fastslås, at bekæmpelse af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, ganske vist er af afgørende betydning for at sikre den offentlige sikkerhed, og at effektiviteten heraf i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker. Et sådan mål af almen interesse kan imidlertid, hvor grundlæggende den end er, ikke i sig selv begrunde, at en foranstaltning med henblik på datalagring som den, der er anført i Logningsdirektivet, anses for nødvendig af hensyn til bekæmpelsen af grov kriminalitet."*

På den baggrund anførte EU-Domstolen i præmis 54 at EU-lovgivning skulle fastsætte **klare og præcise regler, som regulerer rækkevidden og anvendelsen af logningen og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, det gør det muligt effektivt at beskytte deres personoplysninger mod risiko for misbrug og mod ulovlig adgang til og anvendelse af oplysningerne**.

I forhold til spørgsmålet om hvorvidt indgrebet var begrænset til det strengt nødvendige, fremhævede EU-Domstolen i præmis 56-58, at Logningsdirektivet foreskrev lagring af alle trafikdata vedrørende fastnettelefoni, mobiltelefoni, internetadgang samt e-mail og telefoni via internettet, hvilket omfatter alle elektroniske kommunikationsmidler, hvis anvendelse er meget udbredt og af stigende betydning i den enkeltes dagligdag. Derfor omfattede Logningsdirektivets logningsregler alle personer, alle kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse, selv om personer ikke har nogen direkte eller indirekte forbindelse til grov kriminalitet. Som EU-Domstolen anførte i præmis 56: "*Det indebærer dermed et indgreb i de grundlæggende rettigheder for praktisk talt hele den europæiske befolkning*."

EU-Domstolen anførte derudover i præmis 57 og 58, at Logningsdirektivet omfatter generelt alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe grov kriminalitet. Direktivet finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern - forbindelse til grov kriminalitet. Endvidere indeholder den ikke nogen undtagelsesbestemmelse, således at det finder anvendelse selv på personer, hvis kommunikation i henhold til nationale retsregler er omfattet a tavshedspligt.

EU-Domstolen fandt dermed, at Logningsdirektivet ikke krævede nogen sammenhæng mellem de data, der skal lagres, og truslen mod den offentlige sikkerhed, og at lagringen ikke var begrænset til en lagring rettet mod data vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller anden måde kan være indblandet i grov kriminalitet. Logningen var heller ikke begrænset til personer, der af andre grunde ville kunne bidrage til forebyggelsen, afsløringen eller retsforfølgningen af grov kriminalitet.

EU-Domstolen bemærkede endvidere i præmis 60-62, at Logningsdirektivet ikke fastsatte et objektivt kriterium, der muliggjorde afgrænsning af de kompetente myndighedernes adgang til de lagrede data og den efterfølgende anvendelse heraf, samt at den ikke fastsætter materielle og processuelle betingelser herfor.

Logningsdirektivet indeholdte således ikke regler for, at denne adgang og efterfølgende anvendelse er strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger. Logningsdirektivet fastsatte heller ikke et objektivt kriterium, der gør det muligt at begrænse antallet af personer bemyndiget til at få adgang til og efterfølgende anvende dataene til det strengt nødvendige, ligesom Logningsdirektivet ikke fastsatte regler for forudgående kontrol, foretaget af enten EU-Domstolen eller en uafhængig administrativ enhed, af de kompetente myndigheders adgang til de lagrede data.

Afslutningsvist anførte EU-Domstolen i præmis 63-64, at der ved fastlæggelsen af varigheden for datalagring ikke blev sondret mellem de forskellige kategorier af data, der skal lagres, og deres relevans for det mål, Logningsdirektivet forfølger.

På baggrund af ovenstående betragtninger konkluderede EU-Domstolen følgende i præmis 65: "*Det fremgår af det ovenstående, at direktiv 2006/24 ikke fastsætter klare og præcise regler, der regulerer rækkevidden af indgrebet i de grundlæggende rettigheder, som er fastslået i chartrets artikel 7 og 8. Det må derfor fastslås, at dette direktiv indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtræk-*

Bird & Bird

kende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige."

Derudover konkluderede EU-Domstolen i præmis 66-68, at **Logningsdirektivet ikke fastsatte tilstrækkelige garantier, der muliggjorde en effektiv beskyttelse af personoplysninger mod risiko for misbrug og mod ulovlig adgang til og benyttelse af oplysningerne**. Hertil kræver Logningsdirektivet ikke, at udbyderne implementerer tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer et højt beskyttelses- og sikkerhedsniveau, ligesom Logningsdirektivet ikke fastsætter krav om, at dataene skal lagres inden for EU's område.

I præmis 69 erklærede EU-Domstolen herefter Logningsdirektivet for ugyldigt med henvisning til, at EU-lovgiver havde overskredet de grænser, der følger af proportionalitetsprincippet i Chartrets artikel 7, 8 og 52, stk. 1.

3.5.2 Tele2/Watson-dommen (C-203/15)

Digital Rights Ireland fastslog, at Logningsdirektivet var ugyldigt som stridende mod Chartrets artikel 7, 8 og 52, stk. 1. Digital Rights Ireland indebar derimod ikke en stillingtagen til de konkrete nationale logningsregler.

Det blev ved Tele2/Watson-sagen anfægtet, om Digital Rights Ireland også indebar et generelt forbud mod logning, eller om nationale logningsregler alligevel kunne opretholdes i medfør af den særlige undtagelsesbestemmelse i 15, stk. 1 i E-databeskyttelsesdirektivet.

E-databeskyttelsesdirektivet indeholder klare krav til behandling af persondata i telesektoren vedrørende sikkerhed, sikring af kommunikationshemmeligheden og privatlivets fred, herunder ved konkrete krav til, hvem der kan få adgang til data, forbud mod lagring i andre tilfælde end for trafikfremføring eller debitering og ellers alene efter abonnentens samtykke. Sådanne forhold kan dog undtages efter E-databeskyttelsesdirektivets art. 15, stk.1, hvis nogle af de pågældende undtagelsesforhold finder anvendelse – og dette er i overensstemmelse med Chartret.

I afgørelsen bekræftede EU-Domstolen først og fremmest i præmis 81, at nationale logningsregler er omfattet af EU-retten, også nationale logningsregler, der er baseret på E-databeskyttelsesdirektivet.

E-databeskyttelsesdirektivets artikel 1, stk. 1 tager sigte på en harmonisering af de nationale bestemmelser, der er nødvendige for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatlivets fred og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor. E-databeskyttelsesdirektivets artikel 1, stk. 3 undtager dog medlemsstaternes aktiviteter inden for det strafferetlige område og områderne inden for den offentlige sikkerhed, forsvaret og statens sikkerhed. Derudover regulerer artikel 15, stk. 1, muligheden for, at medlemsstaterne kan indføre foranstaltninger, der begrænser rækkevidden af rettigheder og forpligtelser i E-databeskyttelsesdirektivet, når det er nødvendigt at hensyn til statens sikkerhed. Artikel 15, stk. 1, opregner som eksempel på sådanne foranstaltninger "lagring af data". Formålene, som logningsreglerne skal forfølge, herunder at efterforske, afsløre og retsforfølge grov kriminalitet, overlapper derved stærkt med formålene i artikel 3, stk.

1. Der var denne hjemmel som England og Sverige ønskede at basere sine lognings-regler på efter Digital Rights Ireland.

EU-Domstolen fastlog dog på trods af ovenstående, at de engelske og svenske nationale logningsregler – uanset overlappet - var omfattet af E-databeskyttelsesdirektivet, og at medlemsstaterne derfor ikke kunne indføre særlige nationale foranstaltninger vedrørende lagring og adgang til data med henvisning til offentlig sikkerhed, forsvaret og statens sikkerhed. EU-Domstolen begrundede dette med følgende:

i. E-databeskyttelsesdirektivet finder anvendelse på behandling af personoplysninger af udbydere af elektroniske kommunikationstjenester, jf. Tele2/Watson præmis 69,

ii. E-databeskyttelsesdirektivets artikel 15 stk. 1 vil miste ethvert formål, hvis E-databeskyttelsesdirektivet ikke finder anvendelse i den pågældende situation, jf. Tele2/Watson præmis 73,

iii. E-databeskyttelsesdirektivet tillader medlemsstaterne at give de nationale myndigheder adgang til de data, der opbevares af teleudbydere under visse betingelser, jf. Tele2/Watson præmis 76 samt

iv. fordi at en retsforskrift, hvorved medlemsstaterne på grundlag af E-databeskyttelsesdirektivets artikel 15 stk. 1 pålægger teleudbydere at give de nationale myndigheder adgang til de loggede data, vedrører behandling af personoplysninger, som foretages af teleudbydere og dermed er behandlingen omfattet af E-databeskyttelsesdirektivets anvendelsesområde, jf. Tele2/Watson præmis 78.

I afgørelsen undersøgte EU-Domstolen desuden, om de konkrete nationale logningsreglers indgreb i Chartres artikel 7 og 8 om retten til privatliv og retten til beskyttelse af personoplysninger var proportionale. **EU-Domstolen fulgte i det væsentlige sin afgørelse i Digital Rights Ireland og fastlog i præmis 107, at de engelske og svenske logningsregler overskrider rettighederne og garantierne i Chartret, idet reglerne overskrider grænserne for, hvad der er strengt nødvendigt.**

De nationale logningsregler foreskriver således en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med alle midler til elektronisk kommunikation. Lovgivningen pålægger endvidere teleudbyderen at logge teledata systematisk og uafbrudt uden nogen undtagelser. Derudover svarer de kategorier af data i lovgivningen i det væsentligste til de kategorier af data, der skulle logges i henhold til det nu ugyldigt erklærede Logningsdirektiv.

Disse data gør det i henhold til præmis 98 muligt at spore og identificere kilden til en kommunikation og dens bestemmelsessted, at fastslå en kommunikation dato, klokkeslæt, varighed og type, at identificere brugerens kommunikationsudstyr og lokalisere mobilt udstyr, som blandt andet omfatter navn og adresse på abonnenten eller den registrerede bruger, og identificere vedkommende der foretager opkaldets telefonnummer samt modtagerens telefonnummer og – hvis der er anvendt internettjenester – en IP-adresse.

Med disse data kan man fastlægge, hvem der har kommunikeret, med hvilke kommunikationsmidler, på hvilket tidspunkt og hvor de pågældende har befundet sig på tids-

punktet for kommunikationen. Herudover er det muligt at identificere hyppigheden af en brugers kommunikation med bestemte personer i en given periode.

Ud fra disse data er det således muligt at få kendskab til en fysisk persons vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller længere rejser, hvilke aktiviteter der udøves og vedkommendes sociale relationer, og dermed lave en profil om de berørte personer. EU-Domstolen betragter ifølge præmis 99-101 dette som værende en ligeså følsom en oplysning som selve indholdet af kommunikationen, og udgør derfor et meget vidtrækkende og særligt alvorligt indgreb i retten til privatliv. Logningen kan desuden have indvirkning på brugen af de elektroniske kommunikationsmidler og dermed på retten til ytringsfrihed, som fastslået i Chartrets artikel 11.

Herudover fastlog EU-Domstolen endnu engang i præmis 102-103, at det **alene er bekæmpelsen af grov kriminalitet**, der kan begrunde logning af trafik- og lokaliseringsdata, og at selv om effektiviteten af en sådan bekæmpelse i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker, kan det tilsigtede mål, uanset hvor grundlæggende det er, **ikke begrunde en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata**.

De nationale reglers vilkårlige og generelle logningspligt bevirker i den forbindelse at logningspligten er hovedreglen, mens det i henhold til E-databeskyttelsesdirektivet skal være undtagelsen.

På den baggrund blev det af EU-Domstolen slået fast, at de svenske og engelske nationale logningsregler overskred det strengt nødvendige og kunne derfor ikke anses for at være begrundet.

EU-Domstolen bekræftede endvidere i præmis 125, at **artikel 15, stk. 1 i E-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7, 8, 11 og 52, stk. 1, er til hinder for national logningslovgivning, der ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, der ikke begrænser myndighedernes adgang til de loggede data til målet om bekæmpelse af grov kriminalitet, der ikke undergive denne adgang en forudgående kontrol foretaget af en domstol eller uafhængig administrativ myndighed og som ikke stiller krav om, at de pågældende data skal lagres inden for EU.**

Ved præmis 106-108 udtalte EU-Domstolen, at EU-retten derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en **målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet**, forudsat at lagringen af disse data begrænses til det **strengt nødvendige for så vidt angår kategorierne af data,** der skal lagres, de **omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen**.

3.5.2.1 EU-Domstolens krav til nationale logningsregler i medfør af Tele2/Watson

I afgørelsen fastslog EU-Domstolen således hvilke betingelser, der skal være opfyldt, for at retfærdiggøre nationale logningsregler i præmis 108-112:

Bird & Bird

i. For det første skal logningen være **begrænset til grov kriminalitet**.

ii. For det andet skal medlemsstaterne kun indføre målrettet logning som **en forebyggende foranstaltning**. Dette indebærer, **at logningspligten skal være begrænset til**

a. **kategorier af data, der skal logges**,

b. de **omhandlede kommunikationsmidler**,

c. de **berørte personer**, og

d. den fastsatte **varighed af lagringen**.

e. Endelig er det et krav, at den nationale lovgivning indeholder **klare og præcise regler**, der regulerer, hvornår logningsforanstaltningen er tilladt og under hvilke omstændigheder og på hvilke betingelser en logningsforanstaltning kan gennemføres.

iii. For det tredje skal den målrettede logning være **begrænset til, hvad der er strengt nødvendigt**. National lovgivning skal derfor indeholde **objektive kriterier der fastsætter, hvornår data må logges og hvornår myndighederne må få adgang til disse data**. Disse objektive kriterier skal gøre det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse til grov kriminalitet eller bidrage til bekæmpelsen af grov kriminalitet eller forhindre en alvorlig fare for den offentlige sikkerhed. I den forbindelse henviste EU-Domstolen til muligheden for at bruge et geografisk kriterium til at afgøre, om der i et eller flere områder er en forhøjet risiko for, at alvorlig kriminalitet bliver planlagt eller begået. Derudover skal lovgivningen fastlægge, at myndighederne kun kan få adgang til de lagrede data om personer, der mistænkes for at planlægge, begå eller har begået en alvorlig forbrydelse og at denne adgang skal være undergivet en forudgående kontrol af en domstol eller uafhængig administrativ myndighed.

iv. For det fjerde skal de nationale myndigheder, der får adgang til de loggede trafikdata, **underrette de berørte personer**, så snart en sådan underretning ikke kan skade myndighedernes efterforskning. Dette har til formål at sikre retten til et retsmiddel.

v. For det femte skal teleudbydere **sikre effektiv beskyttelse og sikkerhed ved hjælp af passende tekniske og organisatoriske foranstaltninger**, som den nationale tilsynsmyndighed skal føre kontrol over med henblik på at sikre, at beskyttelsesniveauet er tilstrækkeligt.

vi. For det sjette skal **den lagrede data opbevares inden for EU og al data skal destrueres ved udløbet af logningsperioden**. Det er derfor ikke tilladt at opbevare den loggede data på servere placeret uden for EU eller at videregive data til andre myndigheder i lande uden for EU.

EU-Domstolen afgjorde dermed, at kun i de tilfælde, hvor **alle** ovennævnte krav er opfyldt, er målrettede nationale logningsforpligtelser tilladt i henhold til artikel 15,

stk. 1 i E-databeskyttelsesdirektivet sammenholdt med artikel 7, 8, 11 og 52, stk. 1 i Chartret.

3.5.3 Logningsbekendtgørelsen er i strid med EU-Domstolens afgørelser i Digital Rights Ireland og Tele2/Watson

Logningsbekendtgørelsen pålægger teleudbydere at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik. Logningsbekendtgørelsen indeholder – i strid med Digital Rights Ireland og Tele2/Watson - i § 4 en generel og vilkårlig regel om at logge en række oplysninger om, hvem der har kommunikeret, tidspunktet for kommunikationen og hvor de pågældende personer befandt sig på tidspunktet for kommunikationen. Reglen påvirker alle telekunder i Danmark.

Derudover pålægger §§ 5 og 6 teleudbyderne at logge oplysninger vedrørende deres kunders internetbrug, herunder adresserne på abonnenter, tidspunkter for internetkommunikations, den præcise geografiske placering af det trådløse internet samt afsenderens og modtagerens e-mailadresser.

Som anført i Folketingets EU-note af 13. januar 2017: "*EU-Domstolen bekræfter i ny dom, at generel logning af elektronisk kommunikation skal respektere retten til privatliv og beskyttelse af persondata*", vedlagt som **bilag 2.** Logningsbekendtgørelsen går derfor videre end det nu ugyldige Logningsdirektiv. Dertil anføres det, at de danske regler dog indeholder en del af de betingelser, som forudsættes for at retfærdiggøre nationale logningsregler, jf. Tele2/Watson.

Disse betingelser i Retsplejelovens §§ 781-784 omfatter blandt andet, at:

- det alene er politiet, der må få adgang til de loggede data,
- det loggede data skal være af afgørende betydning for efterforskningen, og
- efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, og
- der skal foreligge en retskendelse.

Disse betingelser ændrer dog ikke ved, at der i dansk lovgivning er indført en generel og vilkårlig logningsforpligtelse uden nogen begrænsning til geografiske områder, til gruppen af de personer vis trafikdata og lokaliseringsdata logges, samt hvilke typer af data der logges.

Derudover indeholder Logningsbekendtgørelsen ikke klare og præcise regler, der regulerer, hvornår logningsforanstaltningen er tilladt og på hvilke betingelser en logningsforanstaltning kan gennemføres, ligesom de berørte personer ikke underrettes, når politiet har fået adgang til deres data.

Herudover har SKAT i henhold til § 8 D, stk. 1 i den nugældende skattekontrollov (Lov nr. 1264 af 31. oktober 2013) anset det for muligt - uden en retskendelse - at få udleveret alle loggede oplysninger, som kan være relevante for skatteligningen af juridiske personer. I slutningen af 2012 ophørte teleselskaberne dog med at udlevere teledata til SKAT, og grundet uenighed mellem Skatteministeriet og Erhvervsstyrelsen af fortolkningen af artikel 15 i E-databeskyttelsesdirektivet rettede de i 2014 henvendelse til EU-Kommissionen, der fastlog at skattekontrollovens § 8 D savnede den præcision, der opfyldte kravet til klarhed og forudsigelighed. Som følge af usikkerheden af, om SKATS praksis var lovlig, har SKATs indhentning af teleoplysninger været sat i bero.

Bird & Bird

Der indføres nu en ny skattekontrollov (Lov nr. 1535 af 19. december 2017), som træder i kraft den 1. januar 2019. Heri afskæres SKAT fra at kræve adgang til borgernes teleoplysninger uden en retskendelse, men ordlyden i § 61, der regulerer oplysningspligten, er forsat meget bred, og hvis oplysningerne skønnes nødvendige for skattekontrollen, kræver det alligevel ikke en retskendelse at få dem udleveret.

I henhold til Retsplejelovens § 299 om tredjemands editionspligt er det endvidere muligt at få udleveret logningsdata fra teleselskaberne, hvis retten skønner, at de pågældende data har betydning for sagen. Bestemmelsen stiller hverken krav til, at de loggede data skal have afgørende betydning for sagen eller at sagen skal angå en lovovertrædelse, som kan straffes med fængsel i 6 år eller derover, jf. Telenor-dommen, se punkt 3.7. Rigspolitiet har beskrevet i notat af 3. juli 2014 i hvilken ret omfattende grad, politiet rent faktisk anvender editionsreglerne til udlevering af loggede oplysninger og derved går uden o det generelle krav om, at der skal være tale om særlig grov kriminalitet med en strafferamme over 6 år, jf. **bilag 3**.

Logning medfører, at udbyderne ligger inde med meget omfattende data, der kan kortlægge deres kunders færden i op til et år tilbage. Sådan data er særdeles værdigfuld både i efterforskningsøjemed, kommercielt og for aktører med uhensigtsmæssige hensigter. De loggede data udgør dermed en markant risiko for misbrug af kunders data. Logningsbekendtgørelsen har taget hensyn til dette ved at kræve, at personel med adgang til loggede data skal være sikkerhedsgodkendt, og idet at de alene kan udleveres til politiet ved fremvisning af en retskendelse. Sådanne foranstaltninger er dog ikke nødvendigvis 100 % effektive eller efterleves fuldtud. Risikoen for misbrug er dermed et yderligere element, der ikke gør logningskravet proportionelt.

Sagsøger har set flere generelle eksempler på misbrug af de loggede oplysninger, som sagsøger vil redegøre for ved vidneudsagn under sagen.

Logning af data kræver omfattende tekniske og administrative foranstaltninger. Det er forpligtelser, der har været særdeles omkostningstunge for udbyderne. Historikken har endvidere vist, at udbyderne faktisk ikke modtager særlig mange henvendelser fra politiet, således at logningsforpligtelsen ikke bare er dyr for udbyderne, men heller ikke rigtig anvendes af politiet. Også af denne grund af forpligtelsen uproportional.

Da logningsbekendtgørelsen blev vedtaget, dels med henblik på at implementere Logningsdirektivet, dels med henblik på at gennemføre regeringens handlingsplan for terrorbekæmpelse (terrorpakken fra 2006), blev ændringerne da også stærkt kritiseret af flere politikere, jurister, strafferetseksperter, Datatilsynet, CEPOS, Instituts for Menneskerettigheder m.fl. for at være alt for vidtgående og for at trække Danmark i retning af et overvågningssamfund. Herudover blev det kritiseret, at terrorpakken indeholdte regler om sessionslogning (overvågning af borgernes færden på internettet) med henvisning til, at de andre medlemsstater i lang højere grad lagde sig op af Logningsdirektivet, der ikke indeholdte regler om sessionslogning.

Kravene til hvornår logning eventuelt kan ske er som anført i Digital Rights Ireland og Tele2/Watson kumulative. Logningsbekendtgørelsen kan således ikke opretholdes med henvisning til at Danmark opretholder nogle af kravene, og ikke er lige så ekstreme som eksempelvis England.

Der er således ingen tvivl om, at de danske regler i sin nuværende form ikke lever op til betingelserne fastsat i Tele2/Watson. Logningsbekendtgørelsen er derfor utvivlsomt i strid med artikel 7, 8 og 11 i Chartret og medfører – som fastlagt i både Digital

Bird & Bird

Rights Ireland og Tele2/Watson - et alvorligt og uproportionalt indgreb i borgernes, inklusiv foreningens medlemmers rettigheder.

3.6 Den Europæiske Menneskerettighedskonvention (EMRK)

Den Europæiske Menneskerettighedskonvention (EMRK) fastslår i artikel 8 (Ret til respekt for privatliv og familieliv), stk. 1, at "*enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance*." Det følger af stk. 2, at "*ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.*"

EMRK art. 10 (Ytringsfrihed) angiver i stk. 1, at "*Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at give eller modtage meddelelser eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til grænser. Denne Artikel forhindrer ikke stater i at kræve, at radio-, fjernsyns- eller filmforetagender kun må drives i henhold til bevilling.*" Ligesom det angives i stk. 2, at, "*Da udøvelsen af disse frihedsrettigheder medfører pligter og ansvar, kan den underkastes sådanne formelle bestemmelser, betingelser, restriktioner eller straffebestemmelser, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed, territorial integritet eller offentlig sikkerhed, for at forebygge uorden eller forbrydelse, for at beskytte sundheden eller sædeligheden for at beskytte andres gode navn og rygte eller rettigheder, for at forhindre udspredelse af fortrolige oplysninger eller for at sikre domsmagtens autoritet og upartiskhed.*"

3.6.1 EMRK art. 8 (Retten til privatliv)

I henhold til EMRK art. 8, stk. 2, må ingen offentlig myndighed gøre indgreb i udøvelsen af retten til privatliv og familieliv, medmindre det sker i overensstemmelse med konventionen og er nødvendigt i et demokratisk samfund af hensyn til eksempelvis den nationale sikkerhed eller den offentlige tryghed.

Menneskerettighedsdomstolen har ved dom af 25. september 2001, P.G. og J.H. mod Storbritannien og ved dom af 1. marts 2007, Heglas mod Tjekkiet fastlagt, at offentlige myndigheders indhentelse af teleoplysninger fra teleoperatører om personers brug af telefoner etc., herunder hvem der har ringet til hvem, hvornår og hvor længe der har været forbindelse, vil udgør et indgreb i retten til privatliv, også selvom myndighederne ikke gøres bekendt med indholdet af kommunikationen.

Retten til respekt for privat- og familieliv i Chartret er skrevet i lyset af EMRK art. 8 og Menneskerettighedsdomstolens praksis herom, jf. Forklaringer til Chartret om grundlæggende rettigheder (2007/C 303/02). Af forklaringerne til Chartret fremgår endvidere, at de rettigheder, der sikres ved Chartrets art. 7, svarer til dem, der er sikret ved art. 8 i EMRK, og at de begrænsninger, der accepteres inden for rammerne af art. 8, er de samme, der accepteres inden for rammerne af art. 7. Der er således i vidt omfang tale om de samme rettigheder, med det samme indhold, samme fortolkning og samme tilladte begrænsninger til retten til privatliv.

Dette understøttes af, at det i forklaringerne til Chartrets art. 52, stk. 3 er anført, at bestemmelsen skal "*sikre den nødvendige sammenhæng mellem Chartret og EMRK, i det det fastlår reglen om, at i det omfang rettighederne i dette charter svarer til*

rettigheder, sikres ved EMRK, er deres betydning og rækkevidde, herunder de tilladte begrænsninger, de samme som i EMRK. Det følger navnlig heraf, at lovgiverne, når de fastsætter begrænsninger for disse rettigheder, skal overholde de samme standarder som dem, der er fastlagt i det detaljerede begrænsningsregime i EMRK, som derved bliver gældende for de rettigheder, der er omfattet af dette stykke".

Endvidere er det anført, at "*Under alle omstændigheder må chartrets beskyttelsesniveau aldrig være lavere end EMRK's*".

Det har således været hensigten, at Chartret i vidt omfang videreførte rettighederne i EMRK på EU-niveau, og fastsatte et beskyttelsesniveau, der som minimum svarer til beskyttelsesniveauet i henhold til EMRK.

EU-Domstolen fandt i både Digital Rights Ireland og Tele2/Watson, jf. pkt., 3.5.1 og 3.5.2 nedenfor, at den generelle og vilkårlige logning i medfør af Logningsdirektivet var et uproportionalt og dermed ulovligt indgreb i Chartrets art. 7. I henhold til overensstemmelsen mellem Chartrets art. 7 og EMRK art 8, gør vi derfor gældende, at den generelle og vilkårlige logning i Logningsbekendtgørelsen også er i strid med EMRK art. 8.

Baggrunden for, at EU-domstolen ikke specifikt nævner EMRK art. 8 i domskonklusionen men i øvrigt generelt henviser til EMRK i sammenhæng med Chartrets art. 7 er, at primært den Europæiske Menneskerettighedsdomstol har kompetencen til at fortolke EMRK. EU domstolen henviser generelt til EMRK i dommen, men i sin domskonklusion henvises alene til Chartret, der er EU domstolens jurisdiktion. EU-domstolen skriver konkret om samme i Tele2/Watson, præmis 127 og 128: "*Indledningsvist bemærkes, at selv om de grundlæggende rettigheder, som er anerkendt ved EMRK, udgør generelle principper i EU-retten, således som det bekræftes af artikel 6, stk. 3 TEU, udgør EMRK ikke et retligt instrument, der er formelt registreret i Unionens retsorden, så længe Unionen ikke har tiltrådt den. Den i det foreliggende tilfælde omhandlende fortolkning af direktiv 2002/58 skal således alene anlægges i lyset af de grundlæggende rettigheder, der er sikret ved Chartret.*"

3.6.2 EMRK art. 10 (Retten til ytrings- og informationsfrihed)

Ad forklaringerne til Chartret fremgår endvidere, at Chartres art. 11 om retten til ytrings svarer til art. 10 om retten til ytrings og informationsfrihed i EMRK, og at de begrænsninger, der må foretages i Chartrets art. 11, så vidt muligt ikke må være mere omfattende end dem, der accepteres i EMRK art. 10. Der er således også i denne henseende i vidt omfang tale om de samme rettigheder, med det samme indhold og samme tilladte begrænsninger.

Selvom Logningsbekendtgørelsen ikke omfatter logning af, og adgang til, indholdet af kommunikationen, er det dog ikke udelukket, at den omhandlende lagring kan have indvirkning på abonnenter og registrerede brugeres brug af de omfattede kommunikationsmidler og dermed på deres ytringsfrihed, jf. også Digital Rights Ireland, præmis 28. EU-Domstolen tager ikke i Digital Rights-dommen stilling til, om Logningsdirektivet også udgør en krænkelse af art. 11 i Chartret allerede fordi, der er tale om en krænkelse af art. 7 og 8 i Chartret.

EU-Domstolen henviser til art. 11 i sin domskonklusion i Tele2/Watson sammen med art. 7, 8 og 52, stk.1 som baggrund for, at undtagelsen i E-Databeskyttelsesdirektivets art. 15, stk. 1 ikke finder anvendelse. EU-domstolen anerkender dermed, at logning også kan være i strid med rette n til ytrings og informationsfrihed.

Bird & Bird

Dette må også være tilfældet, da kommunikation med udbredelsen af registrerede data om os i højere grad er mere end indholdet af vores kommunikation. Det er lige så meget karakteristikken af vores kommunikation; hvem taler vi med, hvornår, hvordan og hvorhenne. Ytringsfrihed og informationsfrihed er således et dynamisk begreb, der skal ses i samtidens kontekst, og i dag er ytringers metadata også ytringer, hvis de har et omfang og en detaljering, der faktisk i højere grad end indholdet af kommunikationen kan sige noget om den registrerede.

I kernen af ytrings- og informationsfriheden er den frie og uafhængige presse, og deres brug af kilder. Se eksempelvis the Observer and Guardian v. the United Kingdom (1991), afsnit 59. Pressens brug af anonyme kilder og "whistleblowers" er direkte truet af logningen, for magthaver vil principielt kunne trække en liste over hvem der har kommunikeret med den pågældende journalist. Indskrænkningen er både formel og materiel, både reaktivt og proaktivt. For udover at finde og straffe kilder, kan den omfattende overvågning afskrække personer fra at delagtiggøre offentligheden i emner af stor samfundsmæssig relevans.

De danske logningsregler udgør derfor også et uproportionalt indgreb i EMRK art. 10.

EMRK er en del af dansk ret, da EMRK blev ratificeret i Danmark den 3. september 1953, og formelt blev en del af dansk ret ved lov nr. 285 af 29. april 1992 om Den Europæiske Menneskerettighedskonventionen ("Menneskerettighedskonventionsloven"). Danmark er i naturlig forlængelse heraf også forpligtet til at overholde EMRK.

3.7 Telenor-dom (Østre Landsret dom af 8. maj 2018)

Forhold om adgang til trafikdata, der er lagret i medfør af Logningsbekendtgørelsen, er også vurderet af de danske domstole.

Østre Landsret afsagde den 8. maj 2018 dom i sag, hvor Telenor og Telia nægtede at efterkomme et editionspålæg og krav om isoleret bevisoptagelse om udlevering af IP-adresser i forbindelse med mulig ulovlig deling af ulovligt kopierede filer på internettet. De pågældende IP-adresser var lagret af Telenor og Telia i medfør af kravene til logning i Logningsbekendtgørelsen.

Landsretten fandt, at Telenor og Telia ikke var forpligtet til at udlevere de pågældende trafikdata bl.a. under henvisning til hemmeligholdelseskravene i E-Databeskyttelsesdirektivet, som er implementeret i Danmark i Udbudsbekendtgørelsen, herunder at sådan udlevering også skal ses i lyset af kravene i Chartrets art. 7 og 8, som angivet i Tele2/Watson og Digital Rights Ireland. Udlevering til privat retsforfølgelse for IP krænkelser var ikke et proportionalt forhold, eller et forhold der specifikt var angivet i E-Databeskyttelsesdirektivets art. 15, stk.1.

Dommen understreger, at de danske regler om editionspligt for den konkrete sag strider mod E-Databeskyttelsesdirektivet og Chartret.

3.8 Sagsøgtes fortsatte uberettigede opretholdelse af Logningsbekendtgørelsen

3.8.1 Sagsøgtes indstilling til Digital Rights Ireland – ophævelse af sessionslogning

I lyset af Digital Rights Ireland udarbejdede Justitsministeriet notat af 2. juni 2014 med henblik på at undersøge afgørelsens betydning for Logningsbekendtgørelsen. Notatet er vedlagt som **bilag 4**.

I notatet fastlagde Sagsøgte, at der ikke var grundlag for at antage, at den gældende Logningsbekendtgørelse var i strid med art. 7 og 8 i Chartret. Dog var det tvivlsomt, om reglerne om sessionslogning i Logningsbekendtgørelsens § 5, stk. 1, hvor teleselskaberne skulle logge alle danskernes færden på internettet, herunder hvilken hjemmeside en person havde besøgt, om vedkommende havde sendt en e-mail og til hvem, etc., var egnet til at opnå formålet, herunder skabe mulighed for anvendelse af oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold.

På den baggrund besluttede Sagsøgte, at alene kravet om sessionslogning skulle ophæves, men ikke forbydes, og at lovforslag om revision af logningsreglerne skulle fremsættes i folketingsåret 2014-15. Sidstnævnte førte dog ikke til nogen revision, da revisionen sidenhen er blevet udskudt gentagne gange.

Sagsøgtes ændring af sessionslogning er dog ikke en umiddelbart konsekvens af Tele2/Watson eller Digital Rights Ireland, idet reglerne om sessionslogning allerede far starten af, var en dansk opfindelse og overimplementering af Logningsdirektivet.

Sagsøgte har overfor Folketingets retsudvalg i brev af 11. januar 2018 anført, at Logningsdirektivet fortsat anvendes i de øvrige EU-lande. Brevet vedlægges som **bilag 5**. Dette er som nævnt ikke tilfældet, og er således ikke en undskyldning for den særlige danske tilgang.

3.8.2 Lovhjemlet revision af Retsplejeloven, der aldrig er blevet gennemført

I forbindelse med indførelsen af Retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle Sagsøgte således i folketingsåret 2005-06 fremsætte forslag om revision af Retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder, at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet derfor fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således, at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen.

Ved lov nr. 573 af 18. juni 2012 blev revisionen igen udskudt til folketingsåret 2012-13.

Ved lov nr. 635 af 12. juni 2013 blev revisionen yderligere udskudt til folketingsåret 2014-15. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget om udskydelse af revisionen, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af Logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår.

Bird & Bird

I folketingsåret 2014-15 blev der endnu engang fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området, efter EU-Domstolen erklærede Logningsdirektivet ugyldigt ved dom af 8. april 2014 i Digital Rights Ireland.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17.

Ved lov nr. Lov nr. 673 af 8. juni 2017 bliver revisionen igen udskudt til folketingsåret 2017-18, idet EU-Domstolens dom af 21. december 2016 i 16 Tele2-Watson skulle inkorporeres i revisionsarbejdet.

Sagsøger har nu fremsat endnu et lovforslag, vedlagt som **bilag 6**, af 9. februar 2018 vedrørende ændring af lov nr. 378 af 6. juni 2002 § 8, hvilket vil medføre en yderligere udskydelse af revisionen til folketingsåret 2018-19. Lovforslaget er endnu ikke blevet vedtaget.

Således er revisionen af bestemmelsen foreløbigt blevet udskudt hele seks gange i en periode på over 10 år.

3.8.3 Sagsøgtes manglende konsekvensændring af Logningsbekendtgørelsen efter Tele2/Watson

Inden Tele2/Watson havde regeringen i januar 2017 planer om at introducere ny lovgivning, der skulle erstatte logningsbekendtgørelsen. Dette blev dog i lyset af Tele2/Watson udskudt til efteråret 2017. Sagsøgte fastholdte imidlertid ved åbent samråd den 2. marts 2017, at de gældende logningsregler ikke ville blive ophævet indtil ny lovgivning blev vedtaget, og at teleselskaberne derfor stadig var pålagt den generelle og vilkårlige logningsforpligtelse.

Justitsministeren udtalte i den forbindelse, at de loggede oplysninger simpelthen er for vigtige og at "*Indhentelse af loggede oplysninger er således en fast og velafprøvet del af politiets daglige arbejde med at bekæmpe alvorlig kriminalitet og beskytte os*". Justitsministerens talepapir til samrådet, dateret den 24. februar 2017, er vedlagt som **bilag 7**.

Sagsøgte pålagde dermed teleselskaberne at overtræde EU-retten og de grundlæggende rettigheder i Chartret med henblik på at opretholde logning efter Logningsbekendtgørelsen.

Den 9. februar 2018 fremsatte Sagsøgte forslag om at udskyde den lovbestemte revision af Retsplejelovens § 786, stk. 4 til folketingsåret 2018-2019, jf. bilag 6.

I bemærkningerne til lovforslaget udtaler Sagsøgte, at revisionen af logningsreglerne udskydes med henblik på at gennemføre en grundig dialog med andre berørte EU-lande og EU-Kommissionen, som er ved at udarbejde retningslinjer for, hvordan medlemsstaterne kan fastsætte nationale logningsregler i overensstemmelse med dommen i Tele2/Watson. Det er på nuværende tidspunkt stadig uklart, hvornår disse retningslinjer vil blive offentliggjort.

Sagsøgte udtalte endvidere i bemærkningerne, at de gældende logningsregler i Retsplejelovens § 786, stk. 4, og Logningsbekendtgørelsen ikke ophæves, før revisionen af

logningsreglerne er gennemført, da det vil have uproportionelle konsekvenser for beskyttelses mod terror og alvorlig kriminalitet.

Sagsøgte bemærkede videre i lovforslaget, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. **Efter EU-Domstolens praksis skal medlemsstaterne blot "*hurtigst muligt*" iværksætte foranstaltninger til opfyldelse af en dom.**

Sagsøgte henviste i den forbindelse til at have reageret tids nok i henhold til Ajos-sagen (U.2017.824) vedrørende opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom. Højesteret fastslog her, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser, herunder på at tilvejebringe et fyldestgørende beslutningsgrundlag, som bl.a. indebar dialog med andre EU-lande om deres opfølgning på dommen.

Imidlertid var U.2017.824 (Ajos) dels en ansættelsesretlig sag mellem to private parter, hvorfor sagens principielle værdi er af et noget lavere omfang end nærværende sag, og der var ikke tale om en vedvarende krænkelse af menneskeretten. På denne baggrund var implementeringen af en ændring mindre presserende. Dernæst kommer, at dommen næppe gyldigt kan legitimere, at Sagsøgte har brugt foreløbigt knap 4 år på udredningen af Digital Rights Irelands konsekvenser samt på tilvejebringelsen af et fyldestgørende beslutningsgrundlag.

Til sammenligning af den danske fodslæbende tilgang, har den engelske High Court i april 2018 fastslået, at de engelske logningsregler i form af "Investigatory Powers Act" er i strid med EU-retten og i denne forbindelse alene givet den engelske regering 6 måneder til at vedtage nye regler på området.

3.8.4 England og Sverige tilpasser i modsætning til Danmark deres logningsregler som følge af Tele2/Watson

Andre medlemsstater har rettet ind efter EU-Domstolen og trukket deres logningskrav tilbage eller foretaget gennemgående revision.

Ved beslutning af 7. marts 2017 valgte Kammerrätten i Stockholm (den svenske administrative appeldomstol) at suspendere Tele2's logningspligt. I forlængelse heraf meddelte Tele2 og Telenor, at de ville stoppe med at logge borgernes trafikdata og lokaliseringsdata.

I mellemtiden iværksatte den svenske regering i februar 2017 gennemgribende undersøgelser af de svenske logningsregler. Resultaterne heraf blev offentliggjort i oktober 2017 og en række ændringsforslag blev fremsat af undersøgelseskomitéen, som foreslås at træde i kraft den 1. december 2018.

Retten i Haag (Rechtbank Den Haag) har den 11. marts 2015 endvidere besluttet, at der ikke længere kunne støttes ret på Logningsdirektivet og at den lokale implementation ikke længere havde retskraft.

3.8.5 Teleindustriens henvendelse til EU

Efter at Sagsøgte endnu engang har besluttet sig for at udskyde behandlingen af nye logningsregler har Teleindustrien (teleudbydernes brancheorganisation) den 12. januar 2018 rettet henvendelse til EU's reguleringskommissær.

Bird & Bird

I brevet, som vedlægges som **bilag 8**, påpegede Jacob Willer, Teleindustriens direktør, at den danske telesektor er underlagt en juridisk uholdbar tvetydighed, og at regeringen ikke har fremsat nye regler inden for det tidsrum, den selv har vurderet ville være passende, dvs. 1 år. Han opfordrer derfor EU til at skride ind og kigge nærmere på den danske retstilstand, da teleselskaberne er i overhængende fare for at blive sagsøgt og ikke har mulighed for at svare ordentligt på borgernes henvendelser om den ulovlige logning.

Kommissionen har 8. marts 2018 besvaret Teleindustriens henvendelse, jf. **bilag 9**. Kommissionen oplyser, at Kommissionen er fuldt ud bevidst om Tele2/Watson sagens indflydelse på nationale logningsregler, og at Kommissionen er i indgående diskussioner med medlemsstaterne og EU institutionerne for at vurdere, om der kan og skal indføres logningsregler, der lever op til kravene i Tele2/Watson sagen.

Hermed indikerer Kommissionen, at medlemsstaternes hidtidige nationale logningsregler på nuværende tidspunkt ikke lever op til kravene i Tele2/Watson.

3.9 Opsummering af status

I Danmark har vi således en retstilstand, der strider mod EMRK og Chartret, herunder retten til privatliv, retten til beskyttelse af personoplysninger og retten til ytringsfrihed.

Derudover agter Sagsøgte, at opretholde denne ulovlige retstilstand indtil der kommer nye logningsregler, hvilket først forventes at blive endeligt vedtaget i folketingsåret tidligst 2018-19. Det er endvidere ikke klart, i hvilket omfang Sagsøgte overhovedet har til hensigt at tilpasse de danske logningskrav til at være i overensstemmelse med Chartret, som angivet i EU-Domstolens afgørelser Digital Rights Ireland og Tele2/Watson.

Dette medfører, at såfremt den nuværende ulovlige retstilstand overhovedet bliver stoppet, bliver dette først tidligst tilvejebragt 2,5 år efter, at det har stået klart, at logningskravene i Logningsbekendtgørelsen er i strid med EU-retten.

Med henvisning til Sagsøgtes hidtidige manglende reaktion på EU-Domstolens afgørelser, har Sagsøger ikke tillid til, at Sagsøgte egenhændigt får bragt retstilstanden i orden, hvorfor Sagsøger finder sin påstand nødvendig at få fastslået af Retten.

Bird & Bird

4. ANBRINGENDER

Til støtte for den af Sagsøger nedlagte påstand gøres gældende:

4.1 Sagsøger har retlig interesse og Sagsøgte har processuel partsevne

Sagsøger har fornøden retlig interesse i sagen, idet Sagsøger opfylder de tre kumulative betingelser: Først og fremmest er sagen **egnet** til at blive afgjort af domstolene, idet domstolene har kompetence til at afgøre dette retslige spørgsmål vedrørende afgrænsningen mellem national ret og EU-ret.

Sagen har endvidere den fornødne **aktualitet**, idet Logningsbekendtgørelsen de facto fortsat opretholdes i strid med menneskeretten og EU-retten.

Sagsøger har dernæst **tilstrækkelig tilknytning til sagen**, idet Sagsøgers (foreningens medlemmers) rettigheder i Chartret og EMRK ved Logningsbekendtgørelsen indskrænkes. Logningsbekendtgørelsen har således direkte virkning på Sagsøger, har indgribende betydning for den danske befolkning i almindelighed, og har dermed også indgribende betydning for Sagsøger. Som Højesteret udtalte i Maastricht-dommen, har netop det forhold, at der er tale om almene og væsentlige livsområder, som i sig selv er af indgribende betydning for den danske befolkning i almindelighed (hvilket Logningsbekendtgørelsen har) afgørende betydning for, om Sagsøger bør have adgang til at få sin sag prøvet ved domstolene. Det kan således ikke bestrides, at Sagsøger har den fornødne retlige interesse i at føre denne sag.

Foreningens søgsmålsret anerkendes endvidere i retspraksis, idet Landsretten i Greenpeace-dommen begrundende appellantens (foreningens) søgsmålsret med, at søgsmålet klart faldt inden for det formål, der var beskrevet i foreningens vedtægter.

Sagsøger er netop oprettet med henblik på at forfølge formålet om at få kendt Logningsbekendtgørelsen ugyldig, og har dermed den fornødne retlige interesse i sagen. Sagsøgers enhed har været en nødvendighed, idet Sagsøgers medlemmer ikke enkeltvis ville have været i stand til, hverken fagligt eller økonomisk, at beskytte disses grundlæggende menneskerettigheder.

Derudover har Sagsøgte processuel partsevne, idet Sagsøgte i medfør af ministeransvarsloven §§ 4-5 samt grundlovens § 14 stk. 1 4. pkt. er ansvarlig for Logningsbekendtgørelsens lovlighed. Desuden er en ministers processuelle partsevne fastslået i retspraksis, jf. Maastricht-dommen.

4.2 Logningsbekendtgørelsen kan ikke opretholdes med hjemmel i det nu ugyldige Logningsdirektiv

Logningsbekendtgørelsen er baseret på Logningsdirektivet, der blev kendt ugyldigt ved Digital Rights Ireland.

Sagsøgte har dermed ikke hjemmel til at opretholde Logningsbekendtgørelsen i Logningsdirektivet.

4.3 Logningsbekendtgørelsen kan heller ikke opretholdes med hjemmel i E-Databeskyttelsesdirektivet

Bird & Bird

Logningsbekendtgørelsen kan heller ikke baseres på den særlige undtagelse i E-databeskyttelsesdirektivets art. 15, stk. 1, da dette blev underkendt ved Tele2/Watson.

Sagsøgte har dermed ikke hjemmel til at opretholde Logningsbekendtgørelsen i medfør af E-databeskyttelsesdirektivet.

4.4 Logningsbekendtgørelsen er i strid med Chartrets art. 7, 8 og 52, stk. 1

Det er ubestridt, at Logningsbekendtgørelsen er i strid med Chartret.

Dette forhold følger både af Digital Rights Ireland og Tele2/Watson, som begge klart konstaterer, at generelle og vilkårlige logningskrav er i strid med Chartrets artikel 7, 8, og 52, stk. 1.

Selvom EU-domstolen i Digital Rights Ireland eller Tele2/Watson sagen ikke har taget direkte stilling til den danske Logningsbekendtgørelse, kan der ikke herske nogen tvivl om, at Logningsbekendtgørelsen er i strid med rettighederne i Chartret.

Dette finder især sin begrundelse i, at Logningsbekendtgørelsen indeholder en generel og vilkårlig logningsforpligtelse for teleudbydere uden nogen begrænsninger til geografiske områder, til gruppen af registrerede personer eller den registrerede data. Derudover er det ikke krav om, at de berørte registrerede personer underrettes, når myndighederne har fået adgang til deres teledata. Logningsbekendtgørelsen overskrider derved grænserne for, hvad der er strengt nødvendigt og indebærer et meget alvorligt indgreb i borgernes rettigheder, særligt da man ud fra det loggede data kan få kendskab til en fysisk persons vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller længere rejser, hvilke aktiviteter der udøves og vedkommendes sociale relationer, og dermed lave en profil om de berørte personer.

Chartret er en fuldgyldig del af dansk ret. Sagsøgte er derfor udtrykkeligt forpligtet til at overholde Chartret, jf. legalitetsprincippet og Chartrets art. 51, stk. 1.

4.5 Logningsbekendtgørelsen er i strid med EMRK art. 8

EMRK er en del af dansk ret, Menneskerettighedskonventionsloven, og Danmark har således pligt til at respektere menneskeretten, som den er fastlagt i EMRK samt i Menneskerettighedsdomstolens retspraksis herom.

Danmark har dermed pligt til at respektere retten til privatliv, som denne er fastlagt i EMRK art. 8.

Logningsbekendtgørelsen udgør et alvorligt og uproportionalt indgreb i art. 8 om retten til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.

Dette er bl.a. tilfældet, idet art, 7 i Chartret er skrevet i lyset af EMRK art. 8 og Menneskerettighedsdomstolens praksis herom, jf. Forklaringer til Chartret om grundlæggende rettigheder (2007/C 303/02). Af forklaringerne til Chartret fremgår endvidere, at de rettigheder, der sikres ved Chartrets art. 7, svarer til dem, der er sikret ved art. 8 i EMRK, og at de begrænsninger, der accepteres inden for rammerne af art. 8, er de samme, der accepteres inden for rammerne af art. 7. Der er således i vidt omfang tale om de samme rettigheder, med det samme indhold, samme fortolkning og samme tilladte begrænsninger til retten til privatliv.

Bird & Bird

Dette understøttes af, at det i forklaringerne til Chartrets artikel 52, stk. 3 er anført, at bestemmelsen skal "*sikre den nødvendige sammenhæng mellem Chartret og EMRK, i det det fastlår reglen om, at i det omfang rettighederne i dette charter svarer til rettigheder, sikres ved EMRK, er deres betydning og rækkevidde, herunder de tilladte begrænsninger, de samme som i EMRK. Det følger navnlig heraf, at lovgiverne, når de fastsætter begrænsninger for disse rettigheder, skal overholde de samme standarder som dem, der er fastlagt i det detaljerede begrænsningsregime i EMRK, som derved bliver gældende for de rettigheder, der er omfattet af dette stykke*".

Endvidere er det anført, at "*Under alle omstændigheder må chartrets beskyttelsesniveau aldrig være lavere end EMRK's*".

Det har således været hensigten, at Chartret i vidt omfang videreførte rettighederne i EMRK på EU niveau, og fastsatte et beskyttelsesniveau, der som minimum svarer til beskyttelsesniveauet i henhold til EMRK.

Da EU-domstolen i Digital Rights Ireland og Tele2/Watson fandt, at den generelle og vilkårlige logning i medfør af Logningsdirektivet var et uproportionalt og dermed ulovligt indgreb i Chartrets art. 7, medfører dette dermed også, at der er tale om et indgreb i strid med EMRK art 8.

Baggrunden for, at EU-domstolen ikke specifikt nævner EMRK art. 8 i domskonklusionen men i øvrigt generelt henviser til EMRK i sammenhæng med Chartrets art. 7 er, at den Europæiske Menneskerettighedsdomstol har kompetence til at fortolke EMRK, hvorfor EU domstolen ikke bevæger sig ind på EMRK's område men fokuserer på Chartret, der er EU domstolens jurisdiktion. EU-domstolen skriver konkret om samme i Tele2/Watson, præmis 127 og 128: "*Indledningsvist bemærkes, at selv om de grundlæggende rettigheder, som er anerkendt ved EMRK, udgør generelle principper i EU-retten, således som det bekræftes af artikel 6, stk. 3 TEU, udgør EMRK ikke et retligt instrument, der er formelt registreret i Unionens retsorden, så længe Unionen ikke har tiltrådt den. Den i det foreliggende tilfælde omhandlende fortolkning af direktiv 2002/58 skal således alene anlægges i lyset af de grundlæggende rettigheder, der er sikret ved Chartret.*"

Vi gør imidlertid gældende, at Menneskerettighedsdomstolen ville have kommet frem til det samme resultat, at logning også er i strid med EMRK art. 8.

4.6 Logningsbekendtgørelsen er i strid med retten til ytrings og informationsfrihed, som angivet i Chartrets artikel 11 og EMRK artikel 10

Af forklaringerne til Chartret fremgår, at Chartres artikel 11 om retten til ytringsfrihed svarer til artikel 10 i EMRK om retten til ytrings og informationsfrihed, og at de begrænsninger, der må foretages i Chartrets artikel 11, så vidt muligt ikke må være mere omfattende end dem, der accepteres i EMRK artikel 10. Der er således også i denne henseende i vidt omfang tale om de samme rettigheder, med det samme indhold og samme tilladte begrænsninger.

Selvom Logningsbekendtgørelsen ikke omfatter logning af og adgang til indholdet af kommunikationen, er det dog ikke udelukket, at den omhandlende lagring kan have indvirkning på abonnenter og registrerede brugeres brug af de omfattede kommunikationsmidler og dermed på deres ytringsfrihed, jf. også Digital Rights Ireland, præmis 28. EU-Domstolen tager ikke i Digital Rights Ireland stilling til, om Logningsdirektivet også udgør en krænkelse af art. 11 i Chartret allerede fordi, der er tale om en krænkelse af art. 7 og 8 i Chartret.

Bird & Bird

EU-Domstolen henviser til art. 11 i sin domskonklusion i Tele2/Watson sammen med art. 7, 8 og 52, stk.1 som baggrund for, at undtagelsen i E-Databeskyttelsesdirektivets art. 15, stk. 1 ikke finder anvendelse. EU-domstolen anerkender dermed, at logning også kan være i strid med rette n til ytrings og informationsfrihed.

Dette må også være tilfældet, da kommunikation med udbredelsen af registrerede data om os i højere grad er mere end indholdet af vores kommunikation. Det er lige så meget karakteristikken af vores kommunikation; hvem taler vi med, hvornår, hvordan og hvorhenne. Ytringsfrihed og informationsfrihed er således et dynamisk begreb, der skal ses i samtidens kontekst, og i dag er ytringers metadata også ytringer, hvis de har et omfang og en detaljering, der faktisk i højere grad end indholdet af kommunikationen kan sige noget om den registrerede.

De danske logningsregler udgør derfor også et uproportionalt indgreb i retten til ytrings og informationsfrihed, som angivet i EMRK art. 10 og Chartrets artikel 11.

4.7 Sagsøgte fortsatte insisteren på opretholdelse af Logningsbekendtgørelsen er endvidere i sig selv en krænkelse af Chartrets art. 7 og EMRK art 8.

I henhold til Chartrets artikel 7 og EMRK artikel 8 har Sagsøgte endvidere en positiv forpligtelse til at sikre borgernes privatliv, både horisontalt og vertikalt.

Sagsøgtes insisteren på fortsat at opretholde Logningsbekendtgørelsen, herunder bl.a. ved Sagsøgtes brev af 16. marts 2017, jf. **bilag 10**, udgør i sig selv et pålæg til én privat part om at krænke en andens privatliv i strid med den danske stats positive forpligtelse til at sikre privatliv efter Chartrets art. 7og EMRK art. 8.

4.8 EU retten har forrang

Det er ubestridt, at EU-retten har forrang på områder, hvor Danmark har afgivet lovgivningskompetence til EU.

Logningsdirektivet fastlægger i sin art. 1, stk.1 af formålet er at harmonisere medlemsstaternes bestemmelse om de pligter, der er pålagt udbydere af offentligt tilgængelige elektroniske kommunikationsnet for så vidt angår lagring af data i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet, som defineret i de enkelte medlemsstater. At logning er underlagt EU-retten er også fastlagt i Digital Rights Ireland.

E-databeskyttelsesdirektivet har i henhold til dets artikel 1, stk. 1, til formål at harmonisere medlemsstaternes bestemmelser, som er nødvendige for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Den Europæiske Union. At logning er underlagt E-databeskyttelsesdirektivet, og der ikke kan indføres særlige nationale regler i strid hermed er også fastslået i Tele2/Watson.

Det gøres derfor gældende, at nationale logningsregler er underlagt EU-retten.

Der kan dermed ikke indføres særlige nationale regler i strid med EU-retten på området for lagring af og adgang til teledata, og Danmark har pligt til at følge E-

Bird & Bird

Databeskyttelsesdirektivet samt afgørelserne i Digital Rights Ireland og Tele2/Watson, som alle har forrang fremfor danske regler.

Sagsøgte skal dermed anerkende, at Logningsbekendtgørelsen er ugyldig allerede med henvisning til det EU-retlige forrangsprincip.

4.9 Domstolen er underlagt en forpligtelse til EU konform fortolkning

Danske domstole er forpligtet til at fortolke danske retsregler i overensstemmelse med EU-retten, og skal dermed tage E-databeskyttelsesdirektivet, Chartret og EU-domstolens praksis i betragtning, når de behandler denne sag.

4.10 Sagsøgte har ikke reageret "hurtigst muligt"

Efter EU-Domstolens praksis skal medlemsstaterne "*hurtigst muligt*" iværksætte foranstaltninger til opfyldelse af en dom

At Logningbekendtgørelsen har været i strid med Chartret har været en kendsgerning for Sagsøgte siden Digital Rights Ireland, som blev afsagt den 8. april 2014. Sagsøgte har således siden denne dag konsekvent opretholdt en lovgivning, der var EU-retsstridig. Sagsøgte har endvidere fortsat opretholdt en ugyldig lovgivning, da dette også blev understreget i december 2016 ved Tele2/Watson dommen.

Sagsøgte har dermed ikke reageret *hurtigst muligt* på kendsgerningen om, at Logningsbekendtgørelsen er i strid med EU-retten.

Opretholdelsen af Logningsbekendtgørelsen medfører, at alle danske borgeres menneskerettigheder bliver krænket samtidigt med, at teleselskaberne pålægges at krænke borgernes menneskerettigheder.

Sagsøgtes reference til U.2017.824 (Ajos) kan i den forbindelse ikke danne grundlag for hverken en anerkendelse af Sagsøgtes opretholdelse af Logningsbekendtgørelsen eller Sagsøgtes manglende stillingtagen til revisionen. Dels vedrørte U.2017.824 (Ajos) en ansættelsesretlig problemstilling imellem to private parter og ikke en vedvarende krænkelse af borgernes grundlæggende menneskerettigheder, hvorfor vigtigheden af revisionen ikke meningsfuldt kan sammenlignes. Dernæst anerkendte retten i sagen kun, at ét års revisionsarbejde var acceptabelt i den givne situation. Der er i nærværende situation tale om revisionsarbejde, der foreløbigt først forventes at være færdig i folketingsåret 2018-19, dvs. 6 år efter at Logningsbekendtgørelsen er blevet konstateret ulovlig. Hertil skal nævnes, at det engelske High Court kun har givet den engelske regering bare 6 måneder til at vedtage nye regler, efter at retten fandt de engelske logningsregler i strid med EU-retten.

Idet Sagsøgte har udskudt, og fortsat udskyder, revisionen, kan Sagsøger ikke længere have tillid til, at Sagsøgte kan behandle situationen og varetage Sagsøgers såvel som resten af den danske befolknings centrale frihedsrettigheder. Det er derfor nødvendigt, at retten pålægger Sagsøgte at ophæve Logningsbekendtgørelsen.

Bird & Bird

5. BEVISFØRELSE

Sagsøger agter at føre bevis ved vidneforklaring.

Der tages forbehold for yderligere bevisføring.

6. PROCESSUELLE MEDDELELSER

Sagsøger anmoder om, at retten henviser sagen til Østre Landsret under henvisning til Retsplejelovens § 226, idet nærværende sag findes af principiel karakter, idet den vedrører indgribende menneskerettigheds- og EU-retskrænkelser ved myndighedsudøvelse, hvorfor den har generel betydning for retsanvendelsen og retsudviklingen, ligesom at sagen findes at have væsentlig samfundsmæssig rækkevidde.

København den 1. juni 2018

Martin Von Haller
Advokat (L)

og

Julie Bak-Larsen
advokat

Bird & Bird

7. BILAG

Bilag 1:	Sagsøgers vedtægter af 23. januar 2018
Bilag 2:	Europaudvalget, Retsudvalgets EU-note af 13. januar 2017
Bilag 3:	Rigspolitiets notat af 3. juli 2014
Bilag 4:	Justitsministeriets notat af 2. juni 2014
Bilag 5:	Sagsøgtes brev til Folketinget af 11. januar 2018
Bilag 6:	Lovforslag af 9. februar 2018 vedrørende ændring af revisionsbestemmelse
Bilag 7:	Sagsøgtes talepapir til samråd af 24. februar 2017
Bilag 8:	Teleindustriens brev til EU-kommissionen af 12. januar 2018
Bilag 9:	EU-kommissionens svarbrev af 8. marts 2018
Bilag 10:	Sagsøgtes brev til Teleindustrien af 16. marts 2017

Kammeradvokaten

24. SEPTEMBER 2018

4000587 RHO/SFS/PEAH

Svarskrift

Til

København Byret

I sagsnr. BS-19085/2018-KBH: Foreningen imod Ulovlig Logning
(Advokat Martin von Haller)

mod

Justitsminister Søren Pape Poulsen
Justitsministeriet
(Advokat Rass Holdgaard)

København
Vester Farimagsgade 23
DK-1606 København V

Aarhus
Åboulevarden 49
DK-8000 Aarhus

Telefon +45 33 15 20 10
Fax +45 33 15 61 15
www.kammeradvokaten.dk

Indhold

1. PÅSTAND

Frifindelse

2. PROCESSUELLE BEMÆRKNINGER

2.1 Søgsmålskompetence

Sagsøgte bemærker, at sagsøgeren ikke har fremlagt en liste over sine medlemmer. Det betyder, at det ikke er muligt for sagsøgte at vurdere, hvorvidt foreningen har retlig interesse.

Sagsøgte **opfordrer (A)** på den baggrund sagsøgeren til at fremlægge en medlemsliste.

2.2 Henvisning

Sagsøgte kan tilslutte sig sagsøgerens anmodning om henvisning af sagen til landsretten, jf. retsplejelovens § 226. Sagen rejser efter Justitsministeriets opfattelse bl.a. spørgsmål om forhold, der for øjeblikket er genstand for præjudicielle forelæggelser ved EU-Domstolen. Ifølge bemærkningerne til retsplejelovens § 226 i lovforslag nr. L 168 af 1. marts 2006 er en sag som udgangspunkt principiel, hvis den angår fortolkning af EU-lovgivning eller i øvrigt angår et principielt EU-retligt spørgsmål.

3. TVISTEN I SAGEN

Denne sag handler, som sagsøgte forstår det, grundlæggende om, i hvor lang en periode efter EU-Domstolens afsigelse af dom af 21. december 2016 i Tele2 Sverige AB, forenede sager C-203/15 og C-698/15, ECLI:EU:C:2016:970 (herefter Tele2-dommen), Danmark kan opretholde bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (herefter logningsbekendtgørelsen) uden at handle i strid med EU-retten og Den Europæiske Menneskerettighedskonvention (herefter EMRK).

Sagsøgeren har i sagen nedlagt påstand om, at logningsbekendtgørelsen er ugyldig. Sagsøgeren gør overordnet gældende, at logningsbekendtgørelsen strider mod EU-retten, således som denne er fortolket i Tele2-dommen, og EMRK, at bekendtgørelsen på nuværende tidspunkt skulle have været ændret, og at bekendtgørelsen derfor er ugyldig og uanvendelig. Efter sagsøgerens opfattelse har Danmark ikke hurtigt nok efter Tele2-dommen ændret den danske logningslovgivning i overensstemmelse med anvisningerne i Tele2-dommen.

Sagsøgte bestrider ikke, at Tele2-dommen giver anledning til at udrede, i hvilket omfang den danske logningslovgivning, herunder logningsbekendtgørelsen, skal revideres, ligesom det ikke bestrides, at udredningen og den revision, som udredningen måtte give anledning til, skal foretages hurtigst muligt.

Sagsøgte gør imidlertid gældende, at medlemsstaterne efter fast retspraksis har en vis periode til at efterleve en præjudiciel dom fra EU-Domstolen. Det følger således af EU-Domstolens og Højesterets praksis, at medlemsstaterne i en midlertidig periode efter afsigelsen af en EU-domstolsdom kan opretholde den nationale retsstilling, indtil en ændring af den nationale lovgivning er gennemført hurtigst muligt.

Sagsøgte har indtil nu handlet så hurtigt som muligt i lyset af vanskelighederne ved implementeringen af Tele2-dommen.

Vanskelighederne ved implementeringen af Tele2-dommen skyldes navnlig, at det ikke er muligt at udlede direkte af Tele2-dommen, i hvilket nærmere omfang de danske regler er i strid med EU-retten. Dommen efterlader således betydelig tvivl om den fremtidige indretning af nationale logningsregler i samtlige EU-medlemsstater. Da en lang række europæiske teleselskaber opererer på tværs af landegrænser, har dommen nødvendiggjort og nødvendiggør fortsat et omfattende arbejde i hele EU med henblik på at opnå en fælles europæisk forståelse af dommens konsekvenser.

Hertil kommer, at det konkrete indgreb efter de nugældende logningsregler i den enkelte persons rettigheder efter e-databeskyttelsesdirektivet og Charteret i sig selv er ganske begrænset. Endelig vil det have væsentlige samfundsmæssige skadevirkninger, hvis de gældende logningsregler tilsidesættes eller suspenderes i deres helhed uden samtidig at blive erstattet af reviderede regler.

Under disse omstændigheder er det ikke i strid med EU-retten, at Danmark på nuværende tidspunkt opretholder og anvender logningsbekendtgørelsen.

Parterne er således i denne sag uenige om, hvorvidt logningsbekendtgørelsen allerede på nuværende tidspunkt er ugyldig og dermed uanvendelig, eller om Danmark uden at handle i strid med EU-retten kan opretholde bekendtgørelsen midlertidigt, indtil retsstillingen er afklaret, og arbejdet med at ændre lovgivningen er færdiggjort.

For så vidt angår EMRK gør sagsøgte i første række gældende, at den gældende logningsbekendtgørelse ikke er i strid med EMRK. Der er ikke støtte i retspraksis fra Den Europæiske Menneskeretsdomstol (herefter EMD) for de af sagsøgeren fremførte anbringender. I anden række gøres det gældende, at det under alle omstændigheder ikke er i strid med EMRK at opretholde reglerne midlertidigt i overensstemmelse med EU-retten, jf. ovenfor.

Dette uddybes nedenfor.

4. SUPPLERENDE SAGSFREMSTILLING - OM UDVIKLINGEN I DET DANSKE RETSGRUNDLAG FOR LOGNING

Sagsøgerens sagsfremstilling er på en række punkter mangelfuld og foregriber sagsøgerens anbringender. Det væsentligste faktum af betydning for sagen er indholdet af og baggrunden for indførslen af de danske logningsregler samt det faktiske forløb af arbejdet med revision af logningsreglerne siden afsigelsen af Tele2-dommen. Disse forhold berøres kun ganske kort i den sidste del af sagsøgerens sagsfremstilling. Sagsøgte finder det derfor nødvendigt at redegøre sammenhængende i det følgende.

4.1 Lov nr. 378 af 6. juni 2002 – vedtagelse af retsplejelovens § 786, stk. 4, og revisionspligt i 2005-06

Den nugældende bestemmelse i retsplejelovens § 786, stk. 4, hvorefter det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, blev indført ved lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven bl.a. som led i gennemførelsen af FN-konventionen til bekæmpelse af finansiering af terrorisme og FN's Sikkerhedsråds resolution nr. 1373 (2001). Ændringslovens § 8 bestemmer følgende:

> *"§ 8. Justitsministeren fremsætter i folketingsåret 2005-06 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3."*

Af de specielle bemærkninger til bestemmelsen i lovforslaget, jf. lovforslag nr. L 35 af 13. december 2001, fremgår følgende:

> *"Til § 8*
> *Ordningen med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold er en nyskabelse i forhold til den gældende retstilstand. Forslaget om, at den nærmere tekniske udmøntning skal ske administrativt, giver i vid udstrækning mulighed for løbende at tage højde for det praktiske behov for logning og den tekniske udvikling på området. Den foreslåede bestemmelse i retsplejelovens § 786, stk. 4, indebærer imidlertid, at der skal ske pligtmæssig registrering og opbevaring i 1 år af oplysningerne.*
>
> *Justitsministeriet finder det på denne baggrund hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse. Bestemmelsen i lovforslagets § 8 indebærer, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse."*

4.2 Lov nr. 542 af 8. juni 2006 – udskydelse af revisionen til 2009-10

Ved § 7 i lov nr. 542 af 8. juni 2006 blev ændringslovens § 8 ændret, således at tidspunktet for revisionen blev udskudt fra folketingsåret 2005-06 til 2009-10. Baggrunden for udskydelsen var ifølge pkt. 10.2 i de almindelige bemærkninger i lovforslag nr. L 217 af 31. marts 2006, at udarbejdelsen af bekendtgørelsen om logning i en nedsat ekspertgruppe havde været sat i bero med henblik på at afvente udfaldet af forhandlinger i EU-regi, som den 21. februar 2006 resulterede i vedtagelsen af et direktiv om logning i Rådet. Herefter anførtes følgende i lovforslaget:

> *"Spørgsmålet om gennemførelse af direktivet om opbevaring af trafikdata vil blive behandlet i ekspertgruppen om logning, og det forventes, at arbejdet i ekspertgruppen kan afsluttes i løbet af sommeren 2006 med henblik på udstedelse af en bekendtgørelse om logning i efteråret 2006. Når logningsbekendtgørelsen udstedes, vil forpligtelsen i retsplejelovens § 786, stk. 4, for udbydere af telenet eller teletjenester til at registrere og opbevare oplysninger om teletrafik blive sat i kraft.*
>
> *Med henblik på at sikre en evaluering af ordningen med logning af oplysninger om teletrafik på et tidspunkt, hvor der har været mulighed for over et relevant tidsrum at indhøste erfaringer med en sådan forpligtelse, foreslås det at fastsætte et nyt tidspunkt for revisionen af logningsbestemmelsen. Det foreslås således, at justitsministeren i folketingsåret 2009-10 fremsætter forslag om revision af retsplejelovens § 786, stk. 4. Med en forventet udstedelse af logningsbekendtgørelsen og ikrafttræden af retsplejelovens § 786, stk. 4, i efteråret 2006 indebærer dette, at ordningen tages op til fornyet overvejelse efter et tidsrum, der svarer til det oprindelig forudsatte ved vedtagelsen af anti-terrorpakken i sommeren 2002."*

Logningsbekendtgørelsen blev i overensstemmelse med det forudsatte i lovforslaget udstedt den 28. september 2006 med ikrafttrædelse den 15. september 2007.

4.3 Lov nr. 650 af 15. juni 2010 – udskydelse af revisionen til 2011-12

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt fra folketingsåret 2009-10 til folketingsåret 2011-12. Af bemærkningerne i lovforslag nr. L 180 af 24. marts 2010, pkt. 1.5, fremgår bl.a., at man havde indhentet positive udtalelser om reglerne fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste. Endvidere anførtes følgende for så vidt angik en eventuel ophævelse af revisionsbestemmelsen:

> *"Rigsadvokaten og Rigspolitiet har endvidere anført, at der ud fra hensynet til strafforfølgning kan være behov for at forlænge den gældende opbevaringsperiode på 1 år og behov for at registrere og opbevare flere typer af data. Rigsadvokaten har foreslået, at nærmere overvejelser herom i givet fald sker i lyset af resultatet af det*

igangværende arbejde i EU-regi med evaluering af det såkaldte logningsdirektiv, jf. pkt. 2.2 nedenfor. Endvidere har Rigspolitiet oplyst, at man vil følge udviklingen på området fremover med henblik på at overveje behovet for en længere opbevaringsperiode og behovet for at registrere og opbevare flere typer af data.

Evalueringen af logningsdirektivet forventes at finde sted i efteråret 2010.

I forbindelse med høringen over et udkast til dette lovforslag har flere organisationer mv., herunder tele- og internetbranchen, bl.a. anført, at revisionsbestemmelsen ikke bør ophæves på nuværende tidspunkt, og at branchens erfaringer mv. bør inddrages ved en kommende revision.

Justitsministeriet foreslår på den anførte baggrund, at revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, ikke ophæves på nuværende tidspunkt, men at revisionen af bestemmelsen udsættes til folketingsåret 2011-12, således at resultatet af den evaluering af logningsdirektivet, der forventes at finde sted i efteråret 2010, også kan indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet er endvidere enig med bl.a. Rigspolitiet i, at det vil være hensigtsmæssigt at indhente yderligere erfaring med reglerne med henblik på at vurdere behovet for eventuelle ændringer.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4."

4.4 Lov nr. 573 af 18. juni 2012 – udskydelse af revisionen til 2012-13

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt fra folketingsåret 2011-12 til folketingsåret 2012-13. Om baggrunden for udskydelsen anførtes i lovforslag nr. L 53 af 14. december 2011, pkt. 5, bl.a. følgende:

"Som anført ovenfor under pkt. 3.3 gennemfører logningsbekendtgørelsen, der er udstedt i medfør af retsplejelovens § 786, stk. 4, væsentlige dele af logningsdirektivet. Danmarks EU-retlige forpligtelser sætter således grænser for, hvilke ændringer der kan foretages af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen, der er fastsat i medfør heraf. Overvejelser om eventuelle ændringer af retsplejelovens § 786, stk. 4, må således ske i lyset af logningsdirektivet, der bl.a. fastsætter, at visse oplysninger om teletrafik skal registreres og opbevares i en vis periode.

Som nævnt ovenfor under pkt. 4 forventes Kommissionen at fremlægge et forslag til revision af logningsdirektivet i løbet af 2012. Herefter vil forslaget skulle forhandles af EU-medlemsstaterne i Rådet.

Justitsministeriet foreslår på den baggrund, at revisionen af retsplejelovens § 786, stk. 4, udsættes til folketingsåret 2013-14, så revisionen af de danske logningsregler afventer den kommende revision af logningsdirektivet."

4.5 Lov nr. 635 af 12. juni 2013 – udskydelse af revisionen til 2014-15

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt fra folketingsåret 2012-13 til folketingsåret 2014-15, hvilket ifølge lovforslag nr. L 142 af 6. februar 2013 skyldtes, at den varslede ændring af logningsdirektivet fortsat ikke var gennemført. I lovforslagets pkt. 4 anførtes således bl.a.:

"Kommissionen har i tilknytning til evalueringen oplyst, at den vil foreslå en revision af de nuværende logningsregler. Kommissionen vil finde frem til en række løsningsmuligheder i samråd med de retshåndhævende myndigheder, dommerstanden, erhvervssektoren, forbrugergrupper, datatilsynsmyndigheder og organisationer mv. Kommissionen vil undersøge offentlighedens opfattelse af logning, og logningens indflydelse på adfærden. Resultaterne heraf vil indgå i en konsekvensanalyse af den valgte løsningsmodel, som vil danne grundlag for Kommissionens forslag.

Ifølge de senest foreliggende oplysninger forventes det, at Kommissionen vil fremsætte det tidligere bebudede forslag til revision af logningsdirektivet i løbet af 2013, evt. 2014. Kommissionens forslag til revision af logningsdirektivet vil herefter skulle forhandles i EU-regi.

Forsinkelsen af revisionen i forhold til den oprindelige tidshorisont, jf. pkt. 2.4 ovenfor, skyldes efter det oplyste blandt andet, at der i forbindelse med forhandlingerne om Kommissionens forslag til en generel forordning om databeskyttelse KOM (2012) 0011) er identificeret nogle problemstillinger, som efter Kommissionens opfattelse må afklares, inden logningsdirektivet kan revideres."

Om baggrunden for udskydelsen af revisionen anførtes herefter i pkt. 5.2:

"5.2. Logningsbekendtgørelsen, der er udstedt i medfør af retsplejelovens § 786, stk. 4, bygger som anført under pkt. 3.3 i vidt omfang på logningsdirektivet. Danmarks EU-retlige forpligtelser sætter således grænser for, hvilke ændringer der kan foretages af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Endvidere vil fremtidige ændringer af logningsdirektivet med stor sandsynlighed nødvendiggøre tilpasning af de danske logningsregler.

En revision af de danske logningsregler er et meget omfattende arbejde, som indebærer inddragelse af relevante myndigheder og organisationer mv., herunder tele- og internetbranchen. Hvis arbejdet gennemføres inden revisionen af logningsdirektivet, er der en nærliggende risiko for, at væsentlige forudsætninger for arbejdet brister, idet et revideret logningsdirektiv må forventes at ændre de EU-retlige krav til de danske regler.

Hertil kommer, at hvis der gennemføres en ændring af de gældende danske logningsregler, inden det reviderede logningsdirektiv foreligger, vil dette formentlig indebære, at reglerne skal ændres flere gange inden for kort tid, hvilket kan være til gene for bl.a. de virksomheder, andelsforeninger, ejerforeninger mv., der skal efterleve reglerne.

Justitsministeriet foreslår på den anførte baggrund, at revisionen af retsplejelovens § 786, stk. 4, udsættes til folketingsåret 2014-15, så revisionen af de danske logningsregler afventer den kommende revision af logningsdirektivet.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4."

Under lovforslagets behandling i Retsudvalget oplyste justitsministeren som svar på udvalgets spørgsmål nr. 14 til lovforslaget, at det var Justitsministeriets opfattelse, at reglerne om sessionslogning burde revideres i folketingsåret 2014-15, uanset om revisionen af EU-reglerne om logning (logningsdirektivet) måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der bygger på direktivet, ikke kunne revideres i det pågældende folketingsår.

4.6 Digital Rights-dommen af 8. april 2014 og ophævelse af sessionslogning

På baggrund af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. (Digital Rights-dommen), som tilsidesatte direktiv 2006/24/EF af 15. marts 2006, udarbejdede Justitsministeriet et notat af 2. juni 2014 til Folketinget (notatet er fremlagt som bilag 4). Justitsministeriet fandt samlet set, at der ikke var grundlag for at antage, at de gældende danske logningsregler skulle være i strid med Charteret, navnlig fordi dansk ret i modsætning til logningsdirektivet indeholder klare og præcise regler for myndighedernes mulighed for at få adgang til de loggede oplysninger og for den periode, hvor oplysningerne skulle opbevares.

Samtidig blev det anført i notatet, at ministeriet fandt det tvivlsomt, om den del af reglerne, som vedrører sessionslogning, kunne anses for egnede til at opnå deres formål, som var at skabe mulighed for anvendelse af oplysningerne som led i efterforskning og retsforfølgning

af strafbare forhold. Justitsministeriet ville derfor tage skridt til at ophæve reglerne om sessionslogning. Disse blev ophævet ved bekendtgørelse nr. 660 af 19. juni 2014 om ændring af logningsbekendtgørelsen.

4.7 Lov nr. 640 af 8. juni 2016 – udskydelse af revisionen til 2016-17

I folketingsåret 2014-15 blev der igen fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger til lovforslag nr. L 193 af 29. april 2015), at man ønskede at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd.

Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Lovforslaget om udskydelse af revisionen blev genfremsat som lovforslag nr. L 183 af 27. april 2016 og vedtaget som lov nr. 640 af 8. juni 2016. Et afgørende element i den forestående revision var ifølge lovforslagets pkt. 2.2 at udarbejde nye og forbedrede regler om logning af oplysninger om internetkommunikation til erstatning af de nu ophævede regler om sessionslogning. Sådanne regler skulle dog ikke medføre uforholdsmæssige omkostninger for udbyderne. I lovforslagets pkt. 2.2 anførtes videre bl.a. følgende om baggrunden for udskydelsen af revisionen:

> *"Rigspolitiet anbefaler på den baggrund at udvide teleudbydernes pligt til at logge internetoplysninger, navnlig ved at genindføre regler om logning af oplysninger om internettrafik i en forbedret form, som vil gøre de loggede oplysninger mere anvendelige i politiets efterforskning.*
>
> *For så vidt angår mobil internettrafik anbefaler Rigspolitiet endvidere, at der logges oplysninger om de celler, den mobile kommunikationsenhed er forbundet til ved kommunikationens start og afslutning, og eventuelle celleskift i løbet af kommunikationen samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen.*
>
> *Herudover anbefaler Rigspolitiet, at den gældende logningsforpligtelse i det væsentlige fastholdes.*
>
> *Justitsministeriet har med afsæt i Rigspolitiets anbefalinger fået et eksternt konsulenthus til at beregne anbefalingernes erhvervsmæssige konsekvenser for tele- og internetudbyderne. Konsulenthusets beregninger peger på omstillingsomkostninger for*

udbyderne i omegnen af en milliard kr. Det overstiger efter Justitsministeriets opfattelse grænsen for det acceptable.

Justitsministeriet har samtidig med beregningen af de erhvervsøkonomiske konsekvenser afholdt møder med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen. På møderne er der blevet etableret en nyttig og konstruktiv dialog om udformningen af fremtidens logningsregler.

Efter Justitsministeriets opfattelse er der ingen tvivl om, at behovet for nye logningsregler er reelt og presserende. Omvendt ønsker ministeriet ikke, at udbyderne pålægges økonomiske byrder for nye logningsregler i en størrelsesorden, som ikke er acceptabel.

Justitsministeriet finder på den baggrund, at revisionen af logningsreglerne bør udsættes med henblik på at fortsætte den gode dialog med udbyderne, således at de nye regler både i tilstrækkelig grad tilgodeser politiets behov, og samtidig ikke pålægger udbyderne unødige økonomiske byrder."

4.8 Tele2-dommen og udskydelse af revision til 2017-18

EU-Domstolen afsagde den 21. december 2016 dom i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (Tele2-dommen) om de britiske og svenske logningsreglers forenelighed med EU-retten. Dommens konklusion var som nærmere beskrevet nedenfor, at e-databeskyttelsesdirektivet sammenholdt med Charteret var til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

Den 26. april 2017 fremsattes lovforslag nr. L 191, hvorefter revisionen af logningsbestemmelserne foresloges udskudt fra folketingsåret 2016-17 til folketingsåret 2017-18. Forslaget blev vedtaget som lov nr. 673 af 8. juni 2017. Om baggrunden for forslaget anførtes bl.a. i de almindelige bemærkningers pkt. 3:

*"**3. Justitsministeriets overvejelser og den foreslåede ordning***
De danske logningsregler indebærer, at teleudbyderne skal foretage logning af en række oplysninger om alle deres kunder, på alle tidspunkter og i hele landet, jf. nærmere herom pkt. 2.3.

Det må derfor forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.4 ovenfor, vil skulle foretages nogle tilpasninger af de danske logningsregler, således at reglerne målrettes. EU-Domstolen har ikke taget stilling til, hvordan målrettede logningsregler nærmere kan udfærdiges.

Justitsministeriet er på den baggrund for tiden ved at udrede, hvordan de danske logningsregler kan tilpasses i lyset af dommen i Tele2-sagen. Et centralt element i den udredning er en dialog med en række andre EU-lande, der står i samme situation som Danmark for så vidt angår spørgsmålet om tilpasning af deres nationale logningsregler.

EU-Kommissionen har desuden tilkendegivet, at Kommissionen - i tæt samarbejde med medlemsstaterne - vil udarbejde retningslinjer for, hvordan medlemsstaterne kan fastsætte nationale logningsregler i overensstemmelse med dommen i Tele2-sagen. EU-Kommissionen har ikke på nuværende tidspunkt tilkendegivet, hvornår disse retningslinjer forventes at foreligge.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2017-18 bl.a. med henblik på at kunne gennemføre en grundig dialog med de andre berørte EU-lande og EU-Kommissionen om, hvordan logningsregler fremadrettet kan indrettes. En udskydelse af revisionen vil desuden give bedre tid at sikre det bedste operationelle resultat for politiet og PET i forbindelse med ændringer af logningsreglerne, der udgør et centralt efterforskningsredskab for myndighederne. Endelig vil en udskydelse af revisionen af logningsreglerne give mulighed for en grundig drøftelse med bl.a. telebranchen om de tekniske muligheder - og de forventede omkostninger - ved at tilpasse logningsreglerne i lyset af dommen i Tele2-sagen."

4.9 Arbejdet med revision af telelovgivningen

Umiddelbart efter Tele2-dommen blev EU-Domstolens afgørelse drøftet i EU-regi ad flere omgange, herunder på ministerniveau på et uformelt rådsmøde på Malta den 26.-27. januar 2017. EU-Kommissionen udtrykte i den forbindelse forståelse for de vanskeligheder, som Tele2-dommen medførte for medlemsstaterne, og tilkendegav, at Kommissionen ville udarbejde retningslinjer for, hvordan nationale logningsregler kan udfærdiges i overensstemmelse med Tele2-dommen. Endvidere har spørgsmålet om logning efter Tele2-dommen været drøftet på ministerniveau på flere rådsmøder i Rådet for Retlige og Interne Anliggender, senest på rådsmødet i december 2017.

I marts 2017 blev EU-medlemsstaterne enige om at nedsætte en særlig arbejdsgruppe om logning inden for rammerne af Arbejdsgruppen vedrørende Udveksling af Oplysninger og

Databeskyttelse (DAPIX). Det første møde fandt sted i april 2017, og Justitsministeriet har siden deltaget i en lang række møder i arbejdsgruppen, hvor medlemsstaterne med deltagelse af EU-Kommissionen har drøftet forskellige problemstillinger og spørgsmål, der er opstået som konsekvens af Tele2-dommen. Der er i arbejdsgruppen blevet set bredt på mulighederne for at begrænse og målrette logningsreglerne på en lang række forskellige parametre. I forbindelse med arbejdet i arbejdsgruppen har også bl.a. Europol og EU's Antiterrorkoordinator deltaget i drøftelserne. Der har senest været afholdt møde i arbejdsgruppen den 11. september 2018.

4.10 Lov nr. 716 af 8. juni 2018 – udskydelse af revisionen til 2018-19

Den 11. april 2018 fremsattes lovforslag nr. L 218, hvorefter revisionen af reglerne blev udskudt til 2018-19. Forslaget blev vedtaget som lov nr. 716 af 8. juni 2018. Om baggrunden for denne udskydelse anførtes bl.a. følgende i lovforslagets pkt. 3:

> *"**3. Justitsministeriets overvejelser og den foreslåede ordning***
> *Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18 for, at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).*
>
> *Af pkt. 3 i de almindelige bemærkninger til loven, jf. Folketingstidende 2016-17, A, lovforslag nr. L 191 som fremsat den 26. april 2017, side 6-7, fremgår det bl.a. at Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, at et centralt element i den udredning var en dialog med de andre EU-lande, at EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen, og at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.*
>
> *Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.*
>
> *Det er efter Justitsministeriets opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig*

kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2018-19."

For så vidt angik opretholdelsen af de gældende regler indtil videre anførtes følgende i lovforslaget:

"Det bemærkes, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ophæves, før revisionen af logningsreglerne er gennemført.

Det skal i den forbindelse bemærkes, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. Efter EU-Domstolens praksis skal medlemsstaterne blot hurtigst muligt iværksætte foranstaltninger til opfyldelse af en dom.

I den foreliggende situation har sagen vist sig at være for kompliceret til, at arbejdet i EU om konsekvenserne af Tele2-sagen har kunnet afsluttes, og at EU-Kommissionen har kunnet udstede de forudsatte retningslinjer om logning. Der foreligger derfor efter Justitsministeriets opfattelse ikke et tilstrækkeligt oplyst grundlag for gennemførelsen af en revision af logningsreglerne i Danmark på nuværende tidspunkt.

I forlængelse heraf bemærkes, at Højesteret i en dom af 19. januar 2017 i en sag om opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom har fundet, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser og tilvejebringe et fyldestgørende beslutningsgrundlag, herunder ved at undersøge opfølgningen i andre lande på dommen. Først efter at der var udarbejdet et fyldestgørende beslutningsgrundlag, der pegede på, at der skulle foretages en ifølge Højesteret afgrænset og relativ enkel ændring af ferieloven, var de danske myndigheder forpligtet til at fremsætte et lovforslag om at ændre ferieloven hurtigst muligt.

Det bemærkes, at EU-Kommissionen er orienteret om, at Danmark såvel som de øvrige berørte medlemslande opretholder deres gældende logningsregler indtil videre, hvilket ikke har givet EU-Kommissionen anledning til bemærkninger.

Regeringen vil hurtigst muligt fremsætte et lovforslag for Folketinget om tilpasning af de gældende danske logningsregler."

4.11 Det videre revisionsarbejde

Som det fremgår ovenfor af afsnit 4.9, deltager Justitsministeriet i en arbejdsgruppe i EU-regi, hvor en række spørgsmål siden foråret 2017 er blevet drøftet under inddragelse af medlemsstaterne og bl.a. EU-Kommissionen og Europol. Dette arbejde er fortsat i gang, og har høj prioritet hos formandskabet, ligesom Danmark fortsat arbejder på at finde en fælles løsning på EU-niveau.

.....

Som det fremgår ovenfor, er der således en række forskellige og konkrete begrundelser for de fastsatte revisionsfrister og forskellige årsager til, at det har været nødvendigt at udskyde revisionen af logningsreglerne ved forskellige lejligheder. Det er således ikke retvisende, når sagsøgeren uden nogen yderligere forklaring nøjes med at anføre (stævningens side 29), at revision af bestemmelsen er udskudt hele seks gange i en periode på over 10 år.

5. SUPPLERENDE OM RETSGRUNDLAGET I SAGEN

5.1 Charteret

Den Europæiske Unions Charter om Grundlæggende Rettigheder (Charteret) bestemmer følgende i artikel 7, 8 og 11:

"Artikel 7
Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Artikel 8
Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende.

2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til berigtigelse heraf.

3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

[...]

Artikel 11
Ytrings- og informationsfrihed

1. Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser.

2. Mediefrihed og mediernes pluralisme respekteres."

Charterets anvendelsesområde er reguleret i artikel 51, som bestemmer følgende:

"Artikel 51
Anvendelsesområde

1. Bestemmelserne i dette charter er rettet til Unionens institutioner og organer under iagttagelse af nærhedsprincippet samt til medlemsstaterne, dog kun når de gennemfører EU-retten. De respekterer derfor rettighederne, overholder principperne og fremmer anvendelsen heraf i overensstemmelse med deres respektive beføjelser.

2. Dette charter skaber ingen nye kompetencer eller nye opgaver for Fællesskabet og Unionen og ændrer ikke de kompetencer og opgaver, der er fastlagt i traktaterne."

Charterets artikel 52 fastsætter de generelle betingelser for indgreb i grundrettighederne. Bestemmelsen har følgende ordlyd:

"Artikel 52
Rækkevidden af de sikrede rettigheder

1. Enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved dette charter, skal være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

2. De rettigheder, der anerkendes i dette charter, og som er baseret på fællesskabstraktaterne eller traktaten om Den Europæiske Union, udøves på de betingelser og med de begrænsninger, der er fastlagt i disse traktater.

3. I det omfang dette charter indeholder rettigheder svarende til dem, der er sikret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, har de samme betydning og omfang som i konventionen. Denne bestemmelse er ikke til hinder for, at EU-retten kan yde en mere omfattende beskyttelse."

5.2 Direktiv 2002/58/EF

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (herefter "e-databeskyttelsesdirektivet") indeholder en række bestemmelser, som har til formål at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig privatlivets fred i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, jf. direktivets artikel 1.

Direktivets artikel 5 bestemmer bl.a. følgende:

"Artikel 5

Kommunikationshemmelighed

1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

2. Stk. 1 vedrører ikke lovmedholdelig registrering af kommunikation og de dermed forbundne trafikdata, hvis den foretages som led i lovlig forretningspraksis med henblik på at kunne forelægge bevis for en handelstransaktion eller enhver anden forretningsmæssig kommunikation.

3. Medlemsstaterne sikrer, at anvendelse af elektroniske kommunikationsnet med henblik på lagring af oplysninger eller med henblik på at opnå adgang til oplysninger, der er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren får klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen i overensstemmelse med direktiv 95/46/EF og ret til

at nægte den registeransvarlige en sådan behandling. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationssamfundstjeneste, abonnenten eller brugeren udtrykkelig ønsker."

Direktivets artikel 15 indeholder en generel undtagelsesbestemmelse, som har følgende ordlyd:

"Artikel 15

Anvendelsesområdet for visse bestemmelser i direktiv 95/46/EF

1. Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv 95/46/EF. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2."

5.3 EU-Domstolens dom i C-203/15 og C-698/15 – Tele2

EU-Domstolen fastslog ved dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson (Tele2-dommen), følgende:

"1. Artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsæt-

ter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

2. *Artikel 15, stk. 1, i direktiv 2002/58, som ændret ved direktiv 2009/136, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Charteret om grundlæggende rettigheder, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der regulerer beskyttelsen af og sikkerheden vedrørende trafikdata og lokaliseringsdata, og navnlig de kompetente nationale myndigheders adgang til de lagrede data, uden i forbindelse med bekæmpelsen af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet, uden at undergive den nævnte adgang en forudgående kontrol foretaget af en domstol eller af en uafhængig administrativ myndighed og uden at stille et krav om, at de pågældende data lagres på EU's område."*

5.4 Retsplejelovens § 786 og logningsbekendtgørelsen

Logningsbekendtgørelsen, jf. bekendtgørelse nr. 988 af 28. september 2006, er udstedt i medfør at retsplejelovens § 786, stk. stk. 4 og 7. Denne bestemmelse fastsætter følgende:

§ 786. Det påhviler postvirksomheder og udbydere af telenet eller teletjenester at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler m.v., ved at give de i § 780, stk. 1, nr. 3 og 4, nævnte oplysninger samt ved at tilbageholde og udlevere forsendelser m.v.

Stk. 2. Uden for de i § 780, stk. 1, nr. 3, nævnte tilfælde kan retten efter begæring fra politiet med samtykke fra indehaveren af en telefon eller andet kommunikationsapparat give de i stk. 1 nævnte selskaber m.v. pålæg om at oplyse, hvilke andre apparater der sættes i forbindelse med det pågældende apparat.

Stk. 3. Bestemmelsen i § 178 finder tilsvarende anvendelse på den, som uden lovlig grund undlader at yde den bistand, som er nævnt i stk. 1, eller at efterkomme et pålæg, som er givet efter stk. 2.

Stk. 4. Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Stk. 5. Justitsministeren kan efter forhandling med erhvervs- og vækstministeren fastsætte regler om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Stk. 6. Overtrædelse af stk. 4, 1. pkt., straffes med bøde.

Stk. 7. For overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af stk. 4, 2. pkt., og stk. 5 kan der fastsættes bestemmelser om bødestraf.

Stk. 8. Justitsministeren kan fastsætte regler om økonomisk godtgørelse til de i stk. 1 nævnte virksomheder for udgifter i forbindelse med bistand til politiet til gennemførelse af indgreb i meddelelseshemmeligheden.

Bekendtgørelsen indeholder i kapitel 2 (§§ 4 og 5) bestemmelser om, hvilke typer af hhv. tele- og sessionsoplysninger som udbydere af elektroniske kommunikationsnet eller -tjenester skal registrere og opbevare. Bekendtgørelsens § 4 om teleoplysninger har følgende ordlyd:

"Kapitel 2

Registrerings- og opbevaringspligt

§ 4. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation:

1) *opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,*

2) *opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,*

3) *ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,*

4) *kvittering for modtagelse af meddelelser,*

5) *identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre),*

6) *den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,*

7) tidspunktet for kommunikationens start og afslutning og

8) tidspunktet for første aktivering af anonyme tjenester (taletidskort)."

Bekendtgørelsens § 5 som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 har følgende ordlyd:

"*§ 5. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om en brugers adgang til internettet:*

1) den tildelte brugeridentitet,

2) den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,

3) navn og adresse på den abonnent eller registrerede bruger, til hvem en internet-protokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet og

4) tidspunktet for kommunikationens start og afslutning.

Stk. 2. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, der udbyder trådløs adgang til internettet, skal endvidere registrere oplysninger om det lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr. "

Bekendtgørelsens § 6 indeholder bestemmelser om udbydernes forpligtelse til at registrere oplysninger om egne e-mail-tjenester og internettelefoni-tjenester, som har følgende ordlyd:

"*§ 6. Udover de i § 5 nævnte oplysninger skal en udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere registrere følgende oplysninger om egne e-mail-tjenester:*

1) afsendende e-mail-adresse og

2) modtagende e-mail-adresse.

Stk. 2. For så vidt angår oplysninger om kommunikation foretaget ved brug af udbyderens egne internettelefoni-tjenester, skal de i § 5, stk. 1 – 2, nævnte oplysninger registreres."

Bekendtgørelsens § 3 indeholder en begrænsning af logningsforpligtelsen, der har følgende ordlyd:

> *"§ 3. Bekendtgørelsen finder ikke anvendelse for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder."*

5.5 Retsplejelovens kapitel 71 og 74

5.5.1 Kapitel 71 – Indgreb i meddelelseshemmeligheden

Retsplejelovens kapitel 71 indeholder bestemmelser om indgreb i meddelelseshemmeligheden. Lovens § 780, stk. 1, bestemmer bl.a. følgende:

> *"Kapitel 71*
>
> *Indgreb i meddelelseshemmeligheden, observation, dataaflæsning, forstyrrelse eller afbrydelse af radio- eller telekommunikation og blokering af hjemmesider*
>
> *§ 780. Politiet kan efter reglerne i dette kapitel foretage indgreb i meddelelseshemmeligheden ved at*
>
> ...
>
> *3) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning),*
>
> *4) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning)*
>
> ..."

De generelle betingelser for at foretage indgreb i meddelelseshemmeligheden fremgår af retsplejelovens § 781, stk. 1, som fastsætter:

"§ 781. Indgreb i meddelelseshemmeligheden må kun foretages, såfremt

1) der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt,

2) indgrebet må antages at være af afgørende betydning for efterforskningen og

3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitler 12 eller 13 eller en overtrædelse af straffelovens §§ 124, stk. 2, 125, 127, stk. 1, 233, stk. 1, 235, 266, 281 eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5."

Bestemmelsens stk. 2 og 3 oplister en række yderligere betingelser, hvorunder teleoplysning kan foretages, selvom den ovenfor citerede nummer 3 ikke er opfyldt. Det gælder, hvis mistanken angår en række nærmere opregnede forhold.

Retsplejelovens §§ 782 og 783, stk. 1, bestemmer følgende:

"§ 782. Et indgreb i meddelelseshemmeligheden må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.

Stk. 2. Telefonaflytning, anden aflytning, brevåbning og brevstandsning må ikke foretages med hensyn til den mistænktes forbindelse med personer, som efter reglerne i § 170 er udelukket fra at afgive forklaring som vidne.

§ 783. Indgreb i meddelelseshemmeligheden sker efter rettens kendelse. I kendelsen anføres de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår, jf. dog stk. 2. Endvidere anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres."

Retten beskikker en advokat for den, som udsættes for et indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 784, stk. 1:

"§ 784. Inden retten træffer afgørelse efter § 783, skal der beskikkes en advokat for den, som indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig. Angår

efterforskningen en overtrædelse af straffelovens kapitler 12 eller 13, beskikkes advokaten fra den særlige kreds af advokater, som er nævnt i stk. 2. Rettens beslutning om, at advokaten ikke skal beskikkes fra denne særlige kreds, kan påkæres til højere ret."

Ifølge § 788 gives der underretning til den person, som har været udsat for indgrebet i meddelelseshemmeligheden:

"§ 788. Efter afslutningen af et indgreb i meddelelseshemmeligheden skal der gives underretning om indgrebet, jf. dog stk. 4 og 5. Har den person, til hvem underretning efter stk. 2 skal gives, været mistænkt i sagen, skal der tillige gives underretning herom og om, hvilken lovovertrædelse mistanken har angået.

Stk. 2. Underretningen gives

1) ved telefonaflytning og teleoplysning til indehaveren af den pågældende telefon,

...

Stk. 3. Underretningen gives af den byret, som har truffet afgørelse efter § 783. Underretningen gives snarest muligt, såfremt politiet ikke senest 14 dage efter udløbet af det tidsrum, for hvilket indgrebet har været tilladt, har fremsat begæring om undladelse af eller udsættelse med underretning, jf. stk. 4. Er der i medfør af § 784, stk. 1, beskikket en advokat, skal genpart af underretningen sendes til denne.

Stk. 4. Vil underretning som nævnt i stk. 1-3 være til skade for efterforskningen eller til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller taler hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt imod underretning, kan retten efter begæring fra politiet beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum, der kan forlænges ved senere beslutning. Er der efter § 784, stk. 1, beskikket en advokat, skal denne have lejlighed til at udtale sig, inden retten træffer beslutning om undladelse af eller udsættelse med underretningen.

Stk. 5. Efter afslutningen af et indgreb i meddelelseshemmeligheden i form af udvidet teleoplysning efter § 780, stk. 1, nr. 4, skal der ikke gives underretning om indgrebet til indehaverne af de pågældende telefoner."

5.5.2 *Kapitel 74 – Edition*

Retsplejelovens regler om edition findes i kapitel 74 og omhandler bl.a. betingelserne for at pålægge tredjemand at forevise eller udlevere genstande til brug for bevis. Retsplejelovens § 804 indeholder hovedbestemmelsen og bestemmer bl.a. følgende:

> *"§ 804. Som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning kan der meddeles en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande (edition), hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. Når pålæg meddeles en erhvervsvirksomhed, finder § 189 tilsvarende anvendelse for andre, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen.*
>
> ...
>
> *Stk. 4. Der kan ikke meddeles pålæg om edition, såfremt der derved vil fremkomme oplysning om forhold, som den pågældende ville være udelukket fra eller fritaget for at afgive forklaring om som vidne, jf. §§ 169-172."*

Retsplejelovens § 805, stk. 1, bestemmer bl.a., at pålæg om edition ikke må meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

Fremgangsmåden ved editionspålæg er reguleret i retsplejelovens § 806, som bl.a. fastsætter følgende:

> *"§ 806. Afgørelse om beslaglæggelse og om pålæg om edition træffes efter politiets begæring. Begæring om beslaglæggelse til sikring af erstatningskrav kan tillige fremsættes af forurettede.*
>
> *Stk. 2. Afgørelsen træffes af retten ved kendelse, jf. dog stk. 8. I kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres.*
>
> ...
>
> *Stk. 4. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om beslaglæggelse og om edition, jf. dog stk. 5. Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest*

muligt og senest inden 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes.

...

Stk. 6. Inden retten træffer afgørelse efter stk. 4, 2. pkt., skal der være givet den, mod hvem indgrebet retter sig, adgang til at udtale sig. § 748, stk. 5 og 6, finder tilsvarende anvendelse.

Stk. 7. Inden retten træffer afgørelse om pålæg om edition efter § 804, skal der være givet den, der har rådighed over genstanden, adgang til at udtale sig. § 748, stk. 5 og 6, finder tilsvarende anvendelse. Bestemmelsen i 1. pkt. finder ikke anvendelse, hvis rettens afgørelse skal danne grundlag for en international retsanmodning om edition."

6. ANBRINGENDER

6.1 Sammenfatning af sagsøgtes anbringender

Som det fremgår af afsnit 4.8 og 4.10 ovenfor, bestrider sagsøgte ikke, at Tele2-dommen giver anledning til at udrede, i hvilket omfang den danske logningslovgivning, herunder logningsbekendtgørelsen, skal revideres, ligesom det ikke bestrides, at udredningen og den revision, som udredningen måtte give anledning til, skal foretages hurtigst muligt.

Til støtte for frifindelsespåstanden gør sagsøgte imidlertid overordnet gældende, at opretholdelsen af logningsbekendtgørelsen *i en midlertidig periode* efter Tele2-dommen ikke er i strid med EU-retten, herunder e-databeskyttelsesdirektivets artikel 15 sammenholdt med artikel 7, 8, 11 og 52, stk. 1, i Charteret.

I afsnit 6.2 nedenfor uddybes dette anbringende.

Først redegøres for retsgrundlaget vedrørende den tidsperiode, som medlemsstaterne har til at efterkomme præjudicielle afgørelser fra EU-Domstolen. Som det vil fremgå, følger det af EU-Domstolens og Højesterets praksis, at medlemsstaterne skal efterkomme en præjudiciel dom fra EU-Domstolen *"hurtigst muligt"* og dermed også i en midlertidig periode efter afsigelsen af en sådan dom kan opretholde den nationale retsstilling, indtil en ændring af den nationale lovgivning er gennemført (afsnit 6.2.1).

Dernæst redegøres for de uklarheder ved Tele2-dommen, som bevirker, at det ikke uden videre kan udledes af dommen, i hvilket omfang de danske regler måtte være i modstrid med EU-retten, og hvordan de i givet fald skal revideres. Tele2-dommen efterlader således i alle

EU-lande betydelig tvivl om den fremtidige indretning af nationale logningsregler i overensstemmelse med den retsstilling, som Domstolen har fastslået i dommen (afsnit 6.2.2).

Henset til det arbejde, som har været i gang på EU-niveau siden begyndelsen af foråret 2017 og fortsat står på, har det ikke været muligt at tilpasse dansk lovgivning endnu, og den danske stat har derfor handlet og handler fortsat "hurtigst muligt" (afsnit 6.2.3). Dette skal ses i lyset af, at indgrebet efter de nugældende logningsreglerisoleret set er af ringe intensitet (afsnit 6.2.4), og at en øjeblikkelig tilsidesættelse af logningsbekendtgørelsen i sin helhed vil have væsentlige samfundsmæssige skadevirkninger (afsnit 6.2.5).

Samlet set indebærer de ovennævnte momenter, at det ikke er i strid med EU-retten, at Danmark på nuværende tidspunkt opretholder og anvender logningsbekendtgørelsen.

Sagsøgte gør desuden gældende, at der ikke er noget grundlag for at antage, at den danske logningsbekendtgørelse er i strid med EMRK, jf. nærmere afsnit 6.3.

Endelig redegøres i afsnit 6.4 for, at sagsøgerens beviser og anbringender på en række væsentlige punkter er udokumenterede og/eller ukorrekte.

6.2 Logningsbekendtgørelsen kan opretholdes midlertidigt, indtil en revision er gennemført og sat i kraft

Da det ikke følger af Tele2-dommen, at logning af teledata til kriminalitetsbekæmpelse altid er uforeneligt med e-databeskyttelsesdirektivets artikel 15 sammenholdt med Charterets artikel 7, 8 og 11, og da det heller ikke kan udledes direkte af dommen, i hvilket nærmere omfang den danske logningsbekendtgørelse er uforenelig med de nævnte bestemmelser, gøres det gældende, at de nuværende logningsregler kan opretholdes midlertidigt, indtil en revision er gennemført og sat i kraft.

6.2.1 Retspraksis om midlertidig opretholdelse af national ret efter en præjudiciel dom fra EU-Domstolen

Det følger af fast EU-retspraksis, jf. EU-Domstolens dom af 21. juni 2007 i de forenede sager C-231/06-C-233/06 Jonkman, ECLI:EU:C:2007:373, præmis 38, at medlemsstaterne har en vis tid efter en præjudiciel dom til at bringe national ret i overensstemmelse med EU-retten. Det påhviler således de nationale myndigheder at træffe *"de almindelige eller særlige foranstaltninger, der er egnede til at sikre overholdelsen af fællesskabsretten på deres område"*. Samtidig bevarer medlemsstaterne *"retten til at vælge, hvilke foranstaltninger der skal træffes"*, idet de dog skal påse, *"at national ret så hurtigt som muligt bringes i overensstemmelse med fællesskabsretten, og at borgernes rettigheder i henhold til fællesskabsretten gennemføres fuldt ud."*

Ligeledes er det anerkendt af Højesteret, at myndighederne uden at handle ansvarspådragende kan opretholde en ellers EU-retsstridig lovgivning i en vis periode. Højesteret har i U 2017.1243H (som sagsøgeren fejlagtigt benævner Ajos-sagen, der er gengivet i U 2017.824) fastslået, at den danske stat ikke ifaldt erstatningsansvar på et tidspunkt, som lå inden for den hurtigst mulige implementering af *Pereda*-dommen. Det forhold, at en medlemsstat ikke ifalder erstatningsansvar, selv om en national lovgivning opretholdes i en periode efter afsigelsen af en EU-domstolsdom, som rejser tvivl om lovligheden af national ret, indikerer således også, at medlemsstaten skal indrømmes en vis tid til at tilpasse den nationale retsorden til EU-retsudviklingen.

Sagsøgte gør gældende, at det heraf følger, at medlemsstaterne i denne midlertidige periode kan opretholde den eksisterende lovgivning, indtil en ny og revideret lovgivning er trådt i kraft. Det gøres i den forbindelse gældende, at processen med revision af de danske logningsregler indtil nu er blevet fremmet hurtigst muligt i lyset af de ekstraordinære vanskeligheder, som den frembyder, at det samlede indgreb i rettighederne efter e-databeskyttelsesdirektivet og Charteret i form af generel logning under alle omstændigheder i sig selv er stærkt begrænset, og at det vil have væsentlige samfundsmæssige skadevirkninger at tilsidesætte logningsreglerne i deres helhed uden at sætte andre regler i stedet.

Disse forhold, som er nærmere uddybet nedenfor, fører tilsammen til, at der ikke på nuværende tidspunkt er grundlag for at tilsidesætte logningsbekendtgørelsen.

6.2.2 De retlige og faktiske konsekvenser i lyset af Tele2-dommen frembyder ekstraordinære vanskeligheder

Et hovedsynspunkt i stævningen er, at det efter Tele2-dommen er klart og utvivlsomt, at den danske logningsbekendtgørelse er i strid med EU-retten, at bekendtgørelsen derfor i sin helhed er ugyldig og ikke kan håndhæves, og at andre EU-medlemsstater i øvrigt allerede har suspenderet anvendelsen af deres logningsregler som følge af dommen.

Denne fremstilling bestrider sagsøgte.

Tele2-dommen angår de svenske og britiske regler om logning af teleoplysninger og tager ikke stilling til de danske reglers forenelighed med EU-retten. Det kan heller ikke på nogen måde udledes af Tele2-dommen, præcis hvilke dele af den gældende danske logningsbekendtgørelse, der måtte være i modstrid med e-databeskyttelsesdirektivet sammenholdt med Charteret, og i givet fald hvilke tilpasninger det vil kræve at rette op på en sådan modstrid.

Rækkevidden af Tele2-dommen er således på en række punkter uklar.

Såvel Digital Rights-dommen som Tele2-dommen fastslår, at bekæmpelse af grov kriminalitet og navnlig organiseret kriminalitet og terrorisme er af afgørende betydning for at sikre den

offentlige sikkerhed, og at effektiviteten heraf i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker såsom anvendelse af lagrede teleoplysninger.

Tele2-dommen fastslår, at e-databeskyttelsesdirektivets artikel 15 sammenholdt med Charterets artikel 7, 8 og 11 samt artikel 52, stk. 1, er til hinder for nationale regler, som fastsætter en *"generel og udifferentieret lagring af alle trafik- og lokaliseringsdata"* med henblik på bekæmpelse af grov kriminalitet.

De nævnte bestemmelser i e-databeskyttelsesdirektivet og Charteret er derimod ikke til hinder for en lovgivning, der fastsætter en *"målrettet lagring af trafikdata og lokaliseringsdata"* med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data *"begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen"*, jf. dommens præmis 108.

For at opfylde disse krav skal en sådan national lovgivning for det første fastsætte *"klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data"*, ligesom lovgivningen skal indeholde *"tilstrækkelige garantier"* for den effektive beskyttelse af de personlige oplysninger mod misbrug. Lovgivningen skal navnlig angive, *"under hvilke omstændigheder og på hvilke betingelser"* der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, jf. dommens præmis 109.

Om de materielle betingelser, som den nationale lovgivning skal overholde, fremgår det af dommens præmis 110, at betingelserne *"kan variere i forhold til de foranstaltninger, der træffes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet"*, men at lagringen altid skal opfylde *"objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål"*. Afgrænsningen af personkredsen skal være baseret på *"objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed."* En sådan afgrænsning kan ifølge præmis 111 *"sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået."*

Ud over disse helt overordnede og abstrakte retningslinjer indeholder dommen imidlertid ingen konkrete anvisninger til, hvorledes kravene efter e-databeskyttelsesdirektivets artikel 15 sammenholdt med Charteret kan opfyldes samtidig med, at de i bestemmelsen anerkendte hensyn til bl.a. den offentlige sikkerhed og efterforskning af straffesager kan beskyttes.

Som anført i pkt. 178-184 i generaladvokat Henrik Øes forslag til afgørelse i Tele2-sagen, består nytten af en generel pligt til datalagring i forbindelse med bekæmpelsen af grov kriminalitet i den begrænsede mulighed for at læse fortiden ved hjælp af data, som gengiver kommunikationshistorikken for en person, selv *inden* denne person var mistænkt for at have forbindelse til grov kriminalitet. Herved adskiller den generelle datalagring sig fra den målrettede overvågningsforanstaltning.

Det er således vanskeligt at udlede direkte af Tele2-dommen, hvordan en almindelig pligt til logning teknisk set kan erstattes med en mere målrettet lagring, som samtidig opfylder de væsentlige hensyn af almen interesse i form af bl.a. bekæmpelse af grov kriminalitet m.v., som er udtrykkeligt oplistet i e-databeskyttelsesdirektivets artikel 15 og anerkendt i EU-retsordenen i øvrigt, jf. også justitsministerens talepapir af 24. februar 2017 til brug for besvarelsen af samrådsspørgsmål AA og AB (Alm. del) fra Folketingets Retsudvalg den 2. marts 2017 (sagens bilag 7).

En yderligere betydelig vanskelighed ved målrettet logning er, at reglerne ikke må føre til uproportionale omkostninger for teleselskaberne, jf. også fælles høringssvar af 6. marts 2018 fra Dansk Erhverv, DI Digital, IT-Branchen og TeleIndustrien i forbindelse med høringen over udkast til lovforslag nr. L 218 som fremsat 11. april 2018.

Disse vanskeligheder kommer også til udtryk ved, at Kommissionen endnu ikke har udstedt retningslinjer for, hvordan logning fremadrettet vil kunne konstrueres, jf. også justitsministerens udkast til tale af 20. marts 2018 til brug for besvarelsen af samrådsspørgsmål O og P fra Folketingets Retsudvalg den 5. april 2018 (REU Alm. del 2017-18, Endeligt svar på spørgsmål 588).[1]

Hertil kommer, at dommen ikke forholder sig til, at mange nationale logningsregler, herunder de danske, ikke kun anvendes til almindelig efterforskning af grov kriminalitet, men også bl.a. bidrager til at sikre, at medlemsstaternes internationale forpligtelser overholdes, herunder FN-forpligtelser til terrorbekæmpelse. Som det fremgår ovenfor under afsnit 4.1, blev bestemmelsen i retsplejelovens § 786, stk. 4, om logning af teleoplysninger netop indført i anledning af terrorangrebene den 11. september 2001 med henblik på at styrke det strafferetlige værn mod terrorisme og forbedre politiets efterforskningsmuligheder.

Der verserer på nuværende tidspunkt flere sager ved EU-Domstolen, hvor der er forelagt præjudicielle spørgsmål vedrørende sådanne problemstillinger, jf. bl.a. den belgiske forfatningsdomstols afgørelse nr. 96/2016 af 19. juli 2018[2] og den britiske sag C-623/17, Privacy Inter-

[1] Udkastet til tale kan tilgås på følgende link:
https://www.ft.dk/samling/20171/almdel/REU/spm/588/svar/1485102/1887584/index.htm

[2] Forelæggelsen er endnu ikke forkyndt af EU-Domstolen. Afgørelsen kan tilgås via følgende link: http://www.const-court.be/public/f/2018/2018-096f.pdf

national. Den nævnte belgiske sag angår bl.a. spørgsmålet om, hvorvidt e-databeskyttelsesdirektivets artikel 15 også er til hinder for logning af teleoplysninger ikke bare til bekæmpelse af grov kriminalitet, men også bl.a. til opretholdelse af den nationale sikkerhed, rigets forsvar og bekæmpelse af seksuelt misbrug af børn. Den nævnte britiske sag angår bl.a. spørgsmålet om, hvorvidt e-databeskyttelsesdirektivet i lyset af TEUF artikel 4 og Charterets artikel 51 i det hele taget omfatter nationale regler om logning til brug for opretholdelse af den nationale sikkerhed, og i givet fald hvordan Tele2-dommens krav skal anvendes på sådanne regler.

Retsstillingen er altså med andre ord i høj grad uklar efter Tele2-dommen.

Af disse grunde er det usædvanligt vanskeligt at tilpasse den danske lovgivning til Tele2-dommen.

6.2.3 Der er ikke forløbet urimelig lang tid siden afsigelsen af Tele2-dommen i lyset af det nødvendige arbejde

Tele2-dommen blev afsagt i december 2016, og der er således på nuværende tidspunkt gået mindre end 2 år fra dommens afsigelse.

I denne periode har Justitsministeriet uden ophold arbejdet med at revidere logningslovgivningen. Justitsministeriet har således siden afsigelsen af Tele2-dommen deltaget i en lang række møder i en EU-arbejdsgruppe, hvor EU-medlemsstaterne sammen med Kommissionen har drøftet forskellige problemstillinger og spørgsmål, der er opstået som konsekvens af Tele2-dommen. Derudover har spørgsmålet om logning været behandlet på flere rådsmøder i Rådet for Retlige og Interne Anliggender. Der henvises i den forbindelse til afsnit 4.9 ovenfor.

Disse forhold taler for, at den midlertidige periode, som Danmark har til at tilpasse dansk ret i lyset af Tele2-dommen, endnu ikke er udløbet. Det bemærkes til sammenligning, at Højesteret i ferielovs-sagen (U 2017.1243) fandt det velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser og tilvejebringe et fyldestgørende beslutningsgrundlag, herunder ved at undersøge opfølgningen i andre lande på dommen, selvom den pågældende ændring af ferieloven var "*afgrænset og relativ enkel*". Herefter, og i lyset af at ændringen af logningsbekendtgørelsen ikke er enkel, må det også anses for velbegrundet, at sagsøgte indtil videre har brugt godt halvandet år på i samarbejde med de øvrige EU-medlemsstater at drøfte konsekvenserne af Tele2-dommen fra december 2016 med henblik på at nå frem til en fælles løsning på de problemstillinger, som dommen medfører.

6.2.4 *Indgrebet i form af den generelle logningsforpligtelse er af begrænset intensitet*

Sagsøgte gør herudover gældende, at virkningerne af de indgreb, som logningsbekendtgørelsen i dag måtte indebære i virksomheders og borgeres rettigheder i medfør af Charterets artikel 7, 8 og 11, jf. artikel 52, stk. 1, er begrænsede på flere måder.

Det følger således udtrykkeligt af bl.a. præmis 101 i Tele2-dommen, at et indgreb i rettighederne efter Charterets artikel 7 og 8 i form af logning af teleoplysninger netop ikke kan indebære en krænkelse af det væsentligste indhold af disse rettigheder, idet der ikke sker nogen registrering af indholdet af kommunikationen.

Hertil kommer, at den danske logningsforpligtelse ikke omfatter internetkommunikation, ligesom logningsbekendtgørelsens § 3 undtager en række mindre foreninger m.v. Retsplejeloven opstiller endvidere strenge krav til myndighedernes adgang til de lagrede oplysninger. Det betyder alt andet lige, at det samlede indgreb er mindre intensivt end det, som EU-Domstolen bedømte i Tele2-dommen.

6.2.5 *En øjeblikkelig tilsidesættelse af logningsbekendtgørelsen vil have væsentlige samfundsmæssige skadevirkninger*

Endelig gør sagsøgte gældende, at de samfundsmæssige skadevirkninger, som en øjeblikkelig tilsidesættelse af logningsbekendtgørelsen vil indebære, potentielt vil være meget betydelige, herunder for politiets efterforskningsmuligheder og dermed for den nationale sikkerhed. Det fremgår således af Rigsadvokatens, Rigspolitiets og Politiets Efterretningstjenestes udtalelser i forbindelse med bl.a. lovforslag nr. L 180 af 24. marts 2010, at adgangen til loggede teleoplysninger i adskillige tilfælde har været af væsentlig eller afgørende betydning for efterforskning og retsforfølgning af alvorlige forbrydelser, herunder bl.a. i sager om drab, terror, bandekriminalitet, narkokriminalitet, hjemmerøverier og seksuelle overgreb mod børn.

Det fremgår endvidere senest af Rigspolitiets udtalelse til brug for Justitsministeriets besvarelse af 19. juni 2018 af spørgsmål nr. 627 (Alm. del) fra Folketingets Retsudvalg[3], at politiet i 2017 på landsplan rekvirerede almindelig eller udvidet teleoplysning efter retskendelse 3.037 gange. I alle disse tilfælde har retten således konkret vurderet, at adgangen til de loggede teleoplysninger var afgørende for efterforskningen, jf. retsplejelovens § 781, stk. 1, nr. 2. Det bemærkes samtidig, at den særlige undtagelse fra kravet om forudgående retskendelse i retsplejelovens § 783, stk. 4, til sammenligning kun blev anvendt 89 gange. Det fremgår endvidere af besvarelsen, at politiet derudover i en lang række sager indhenter oplysninger om bl.a. historiske lokaliseringsdata eller navnet på brugeren af en IP-adresse eller en telefon med et givent IMEI-nummer, uden at det dog er muligt at opgøre det præcise antal.

[3] Besvarelsen kan tilgås på følgende link: https://www.ft.dk/samling/20171/almdel/reu/spm/627/svar/1498872/1913155.pdf

Hertil kommer, at det også er anerkendt i Tele2-dommens præmis 103 og Digital Rights-dommens præmis 51, at effektiviteten af efterforskning og bekæmpelse af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, er afhængig af moderne efterforskningsteknikker såsom anvendelsen af lagrede teleoplysninger.

Samlet set er der i lyset af ovenstående ikke tvivl om, at en øjeblikkelig tilsidesættelse af logningsbekendtgørelsen vil have betydelige samfundsmæssige skadevirkninger.

Sagsøgte gør gældende, at det af de ovennævnte grunde ikke strider mod EU-retten og EMRK at opretholde logningsbekendtgørelsen som gyldig indtil videre.

Det bemærkes i denne forbindelse, at sagsøgtes synspunkt synes at være i overensstemmelse med synspunkter, der er fremsat i en sag, der verserer ved den belgiske forfatningsdomstol. Denne domstol har den 19. juli 2018 besluttet at forelægge et præjudicielt spørgsmål om muligheden for at opretholde nationale bestemmelser om logning på midlertidig basis. Sagen har fået sagsnr. C-520/18 ved EU-Domstolen. Det pågældende præjudicielle spørgsmål har følgende ordlyd (understregning tilføjet):[4]

> " *3. Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi?* "

Sagsøgte er ikke bekendt med de nærmere omstændigheder i sagen. På baggrund af de offentligt tilgængelige oplysninger er det dog sandsynligt, at EU-Domstolens besvarelse af de forelagte spørgsmål vil have betydning for udfaldet af denne sag.

[4] Dommen kan læses i sin helhed på følgende link: http://www.const-court.be/public/f/2018/2018-096f.pdf

6.3 Logningsbekendtgørelsen er ikke i strid med EMRK

Sagsøgerne gør i stævningens afsnit 4.5 gældende, at logningsbekendtgørelsen strider mod EMRK artikel 8. Sagsøgerne har imidlertid ikke på nogen måde konkretiseret, hvilken konkret praksis fra Den Europæiske Menneskerettighedsdomstol (EMD) man påberåber sig, eller hvori denne modstrid nærmere bestemt skulle bestå. Den omstændighed, at *EU-Domstolen* ved Tele2-dommen fandt, at *Charteret* var til hinder for regler som de *svenske*, er selvsagt ikke tilstrækkelig til at fastslå, at *EMD* ville nå til samme konklusion for så vidt angår *de danske reglers* forhold til *EMRK*.

Hertil kommer, at der ikke er nogen støtte for synspunktet i EMD's praksis.

EMD har taget stilling til nationale regler om masseindsamling af data i fire domme (jf. afgørelse af 29. juni 2006 i sagen Weber og Saravia mod Tyskland (54934/00), afgørelse af 1. juli 2008 i Liberty m.fl. mod Det Forenede Kongerige (58243/00) og afgørelse af 19. juni 2018 i sag Centrum för Rättvisa mod Sverige (35252/08)). Disse sager angik egentlig overvågning, dvs. at oplysningerne kunne tilgås og anvendes umiddelbart af myndighederne uden forudgående kontrol, ligesom alle sagerne angik regler, som indebar, at selve indholdet af kommunikationen blev registreret. I øvrigt blev både Tyskland og Sverige frifundet for den påståede krænkelse af artikel 8, idet EMD konkret fandt, at disse landes regler overholdt de seks minimumsgarantier udviklet i domstolens praksis.

Eftersom logningsforpligtelsen efter de danske regler ikke indebærer en registrering af indholdet af kommunikationen og i øvrigt ikke engang kan karakteriseres som hemmelig overvågning i den forstand, som EMD anvender dette udtryk, fordi myndighederne ikke har umiddelbar adgang til de loggede oplysninger, er der intet grundlag for at antage, at de danske regler om logning skulle være i strid med EMRK, jf. nærmere Justitsministeriets notat om Digital Rights-dommen, side 23f (sagens bilag 4).

I anden række gøres det gældende, at det under alle omstændigheder er foreneligt med EMRK at opretholde den danske logningsbekendtgørelse midlertidigt, jf. ovenfor afsnit 6.2.

6.4 Bemærkninger til sagsøgerens anbringender

Sagsøgeren fremfører en række udokumenterede og/eller forkerte oplysninger og anbringender i stævningen, herunder navnlig i afsnit 3 og 4. Disse giver – ud over det, der er anført ovenfor – anledning til følgende overordnede bemærkninger:

6.4.1 Logning misbruges

Sagsøgeren hævder, at der er *"flere generelle eksempler på misbrug af de loggede oplysninger, som sagsøger vil redegøre for ved vidneudsagn under sagen"* (stævningen, side 24). Sagsøgeren **opfordres (B)** til at redegøre for disse eksempler, så sagsøgte har reel mulighed for at forholde sig til dem. I modsat fald må disse overordnede bemærkninger anses for udokumenterede i deres helhed, ligesom der må tages forbehold for afbrydelse og udsættelse af hovedforhandlingen.

6.4.2 Logning er dyrt, og data anvendes sjældent af politiet

Sagsøgeren anfører (stævningen, side 24), at logning af data kræver omfattende og omkostningstunge tekniske og administrative foranstaltninger af udbyderne, og at politiet sjældent anvender de loggede data i praksis.

Sagsøgte bestrider ikke, at logning er en byrde for de omfattede pligtsubjekter, men bestrider, at byrden er omfattende og står i misforhold til politiets behov for disse data. Der henvises i den forbindelse til det anførte ovenfor under afsnit 6.2.5

I øvrigt bemærkes, at teleselskabernes eventuelle vanskeligheder ved at efterkomme reglerne ikke indgår som relevant moment i vurderingen af, hvorvidt og i hvilket omfang reglerne krænker individuelle borgeres rettigheder. Hertil kommer, at der intet belæg er for at antage, at en differentieret logning i overensstemmelse med Tele2-dommen skulle være mindre ressourcekrævende.

6.4.3 Logning truer pressefriheden/kildebeskyttelsen

Sagsøgeren hævder (stævningen, side 27), at logningsbekendtgørelsen truer den frie og uafhængige presse, idet *"magthaver vil principielt kunne trække en liste over hvem der har kommunikeret med den pågældende journalist"*. Dette bestrides. Sagsøgeren overser, at der i retsplejeloven er fastsat begrænsninger for myndighedernes adgang til de loggede oplysninger, som sikrer, at myndigheder netop ikke "principielt" kan få adgang til disse oplysninger.

Den omstændighed, at det som påstået af sagsøgerne i en hypotetisk situation med mangelfuld sikkerhed hos en udbyder af elektroniske kommunikationstjenester skulle kunne lade sig gøre at få adgang til og misbruge de lagrede oplysninger på den beskrevne måde, er naturligvis uden betydning ved vurderingen af reglernes gyldighed som sådan.

6.4.4 De danske regler om editionspligt strider mod EU-retten – Telenor-dommen

Sagsøgeren anfører (stævningens side 27), at de danske regler om edition er i strid med e-databeskyttelsesdirektivet og Charteret.

Hertil bemærkes for det første, at den nedlagte påstand i sagen udelukkende angår gyldigheden af logningsbekendtgørelsen. Regler om adgang til de lagrede data – herunder regler om underretning og edition – findes i bestemmelser i retsplejeloven, hvis gyldighed ikke er anfægtet under sagen.

For det andet, og under alle omstændigheder, bestrides det, at de danske regler om edition strider mod e-databeskyttelsesdirektivet eller Charteret.

Østre Landsrets kendelse af 7. maj 2018, som er det eneste grundlag, sagsøgeren henviser til, er ikke udtryk for en underkendelse af reglerne om edition. Kendelsen viser tværtimod, at de danske regler om (civilretlig) edition kan anvendes under hensyntagen til de begrænsninger i adgangen til teleoplysninger, som e-databeskyttelsesdirektivet og Charteret foreskriver.

Det fremgår udtrykkeligt af kendelsen, at Østre Landsret foretager en afvejning inden for rammerne af retsplejelovens § 299 af de tungtvejende hensyn i Charteret og e-databeskyttelsesdirektivet over for sagsøgerens interesse i oplysningerne, og at denne afvejning fører til et afslag på adgang til de pågældende oplysninger.

6.4.5 Starttidspunktet for fastlæggelsen af det tidsrum, som Danmark har til at efterkomme EU-Domstolens dom

Sagsøgeren anfører i stævningen, side 29-30, at sagsøgte har brugt ca. 4 år på at udrede konsekvenserne af Digital Rights-dommen, og at High Court i Det Forenede Kongerige har *"givet den engelske regering 6 måneder til at vedtage nye regler på området."*

Dette bestrides. Den dom, som Danmark nu skal efterleve, og som er omdrejningspunktet i denne sag, er ikke Digital Rights-dommen, men Tele2-dommen. Den tid, som Danmark har til at indrette den danske logningslovgivning i overensstemmelse med EU-Domstolens praksis skal derfor fastlægges med udgangspunkt i Tele2-dommen, som blev afsagt den 21. december 2016. Justitsministeriet har således allerede analyseret konsekvenserne af Digital Rights-dommen og foretaget de fornødne ændringer i dansk ret (ophævelse af sessionslogning), jf. ovenfor afsnit 4.6.

6.4.6 Kommissionen har ikke indikeret, at de gældende danske logningsregler er i strid med EU-retten

Sagsøgeren hævder (stævningens side 31), at Kommissionen til teleindustrien har indikeret, at de danske logningsregler er i strid med EU-retten. Dette bestrides. Kommissionen har ikke indikeret dette, og det fremgår ikke af det brev af 8. marts 2018 fra Kommissionen til teleindustrien (bilag 9), som sagsøgeren støtter denne påstand på.

6.4.7 Digital Rights-dommen påvirker ikke logningsbekendtgørelsens gyldighed

Sagsøgerne anfører i stævningens afsnit 4.2, at logningsbekendtgørelsen ikke kan opretholdes med hjemmel i logningsdirektivet, som blev ophævet ved Digital Rights-dommen. Dette beror på en misforståelse. For det første er henvisningen til direktivet udgået, jf. ændringen af logningsbekendtgørelsen ved bekendtgørelse nr. 660 af 19. juni 2014. For det andet udgør direktivet ikke "hjemlen" for logningsbekendtgørelsen. Bekendtgørelsen er udstedt i medfør af retsplejelovens § 786, stk. 4 og 7, som giver hjemmel til at fastsætte regler om telenet- og teletjenesteudbydernes praktiske hjælp med indgreb i meddelelseshemmeligheden. Bekendtgørelsens lovlighed afhænger derfor ikke af direktivets gyldighed.

Det samme gør sig gældende i forhold til e-databeskyttelsesdirektivet, hvor sagsøgerne i afsnit 4.3 anfører, at logningsbekendtgørelsen ikke kan opretholdes med henvisning til de nu ophævede undtagelsesbestemmelser i dette direktiv. Konsekvensen af ophævelsen af undtagelsesbestemmelserne ved Digital Rights-dommen er ikke, at logningsbekendtgørelsen ikke har "hjemmel". Konsekvensen er udelukkende, at bekendtgørelsen efter ophævelsen skal bedømmes efter direktivets øvrige bestemmelser.

6.4.8 Regler om adgang til loggede oplysninger

I stævningens afsnit 4.4 anfører sagsøgerne bl.a. som argument for logningsbekendtgørelsens ugyldighed, at der ikke er krav om, at de berørte registrerede personer underrettes, når myndighederne har fået adgang til deres teledata.

Dette er ikke korrekt. Retsplejelovens § 788, stk. 1, bestemmer tværtimod, at der efter afslutningen af et indgreb i meddelelseshemmeligheden – herunder i form af teleoplysning – som hovedregel skal gives underretning om indgrebet. Har den person, til hvem underretning efter stk. 2 skal gives, været mistænkt i sagen, skal der også gives underretning herom og om, hvilken lovovertrædelse mistanken har angået. Undtagelse gøres efter § 788, stk. 4, alene, hvis underretningen vil være til skade for efterforskningen.

7. PROCESSUELLE MEDDELELSER

til sagsøgte kan stiles til advokat Rass Holdgaard, Vester Farimagsgade 23, 1606 København V (j.nr. 4000587).

8. MOMSREGISTRERING

Sagsøgte er ikke momsregistreret.

Kammeradvokaten

– Rass Holdgaard
Partner, Advokat (H)

Sag BS-36799/2018-OLR
Østre Landsret
14. Afdeling
Bredgade 59
1260 København K.

Bird & Bird
Advokatpartnerselskab
Sundkrogsgade 21
2100 Copenhagen
Tel +45 72 24 12 12
Fax +45 72 24 12 13
twobirds.com

REPLIK

Sagsøger	Foreningen imod Ulovlig Logning CVR-nr. 39 30 93 86 Birkegade 15, 5. tv. 2200 København N v./advokat Martin Von Haller ("Sagsøger")
mod	
Sagsøgte	Justitsminister Nick Hækkerup Justitsministeriet Slotholmsgade 10 1216 København K v./advokat Rass Holdgaard ("Sagsøgte")

INDHOLDSFORTEGNELSE

1. PÅSTAND

Sagsøger fastholder sin påstand, som fremsat i stævningen.

2. INDLEDENDE BEMÆRKNINGER

Sagen blev anlagt den 1. juni 2018. Sagsøgte indleverede svarskrift den 24. september 2018. Sagsøgte anmodede sagen udsat i medfør af retsplejelovens § 345 første gang den 5. december 2018 med henblik på at afvente EU-Domstolens afgørelse i sag C-520/18, Ordre des barreaux francophones et germanophone m.fl., ("C-520/18 Ordre des Barreaux, m.fl."). Sagsøger bestred grundlaget for at udsætte sagen, men Retten afsagde desuagtet første gang kendelse den 26. februar 2019 om at udsætte sagen for at afvente afgørelse af C-520/18 Ordre des Barreaux, m.fl. Udsættelserne blev løbende forlænget af Retten efter begæring fra Sagsøgte på trods af protest fra Sagsøger.

EU-Domstolen traf afgørelse i sag C-520/18, Ordre des Barreaux den 6. oktober 2020, hvorefter indeværende sag igen kunne fremmes. Sagen har således på nuværende tidspunkt været udsat i mere end 2 år.

Digital Rights Ireland (C-293/12 og C-594) ("Digital Rights Ireland") blev afsagt for 6½ år siden den 8. april 2014. Tele2/Watson (C-03/15, C-698/15) ("Tele 2/Watson") blev afsagt for 4 år siden den 21. december 2016, og nu senest C-520/18, Ordre des Barreaux, m.fl. den 6. oktober 2020. Det har været et langstrakt forløb, hvor EU-Domstolens grundlag for at underkende medlemsstaternes ulovlige logning gentagne gang er blevet udfordret. EU-domstolen har imidlertid hver gang opretholdt sit standpunkt og endvidere til stadighed bestyrket og nuanceret vurderingen af generel og udifferentieret logning som ulovlig. I mellemtiden har de berørte personer i medlemsstaterne, herunder i Danmark, fortsat fået krænket deres grundlæggende rettigheder ved ulovligt at få indsamlet og lagret deres teledata.

Replikken skal således læses i lyset af:

- at EU-Domstolens afgørelse i sag C-520/18, Ordre des Barreaux, m.fl. den 6. oktober 2020 stadfæstede, hvad der allerede var blevet afgjort i Tele2/Watson (C-03/15, C-698/15) og Digital Rights Ireland (C-293/12 og C-594), og i øvrigt fastlagde at medlemsstaternes domstole ikke må håndhæve national lovgivning, der strider mod EU-domstolens afgørelser i de nævnte sager;

- at der i mellemtiden har været flere alvorlige tilfælde af misbrug/systemiske fejl i håndteringen af de teledata, som er indsamlet og lagret ulovligt efter den danske lovgivning. Risici for at sådanne forhold kunne forekomme var netop nogle af de selvsamme årsager, som EU-domstolen lagde vægt på ved sin afgørelser af national lovgivning om logning som ulovlig;

- at de danske borgeres grundlæggende rettigheder således fortsat krænkes, herunder i strid med EU Chartrets art. 7 (respekt for retten til privatliv og familieliv, sit hjem og sin kommunikation), art. 8 (retten til beskyttelse af sine personoplysninger), art. 11 (ytrings -og informationsfrihed), art. 52, stk.1 (manglende proportionalitet), EMRK art. 8 (retten til privatliv) og art. 10 (retten til ytrings- og informationssikkerhed);

- at Sagsøgte ikke troværdigt eller med henvisning til gældende praksis kan fastholde, at Sagsøgte har handlet "hurtigst muligt";

- at Sagsøgtes tilgang til spørgsmålet generelt, og som påvist i forløbet under denne sag, viser, at Logningsbekendtgørelsen ikke bliver ophævet eller ændret før Retten pålægger Sagsøgte det ved at fastlægge ved dom, at Logningsbekendtgørelsen er ugyldig.

3. SUPPLERENDE SAGSFREMSTILLING

3.1 Præjudiciel dom C-520/18, C-511/18, C-512/18: Ordre des Barreaux, m.fl.

3.1.1 Baggrund

Sagen omfattede præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) (sag C-511/18 og C-512/18), og af Cour constitutionnelle (forfatningsdomstol, Belgien) (sag C-520/18).

Begge sager omhandlede franske og belgiske logningsregler, der i høj grad var tilsvarende med de danske.

De franske sager: (C-511/18 og C-512/18):

C-511/18: Ved søgsmål anlagt den 30. november 2015 og den 16. marts 2016 ved Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig), og senere forenet i hovedsagen, havde Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs og Igwan.net nedlagt påstand om annullation af dekret 2015-1185, 2015-1211, 2015-1639 og 2016-67, bl.a. med den begrundelse, at disse dekreter tilsidesatte den franske forfatning, EMRK samt direktiv 2000/31 og 2002/58, sammenholdt med chartrets artikel 7, 8 og 47, jf. præmis 56.

C-512/18: Ved et søgsmål anlagt den 1. september 2015 ved Conseil d'État (øverste domstol i forvaltningsretlige sager) havde French Data Network, Quadrature du Net og Fédération des fournisseurs d'accès à Internet associatifs nedlagt påstand om annullation af den stiltiende afgørelse om afslag, der fulgte af premierministerens manglende reaktion på deres anmodning om ophævelse af CPCE's artikel R. 10-13 og af dekret 2011-219, bl.a. med den begrundelse, at disse tekster var i strid med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11.

Den belgiske sag: (C-520/18):

Ved søgsmål anlagt den 10. januar, den 16. januar, den 17. januar og den 18. januar 2017 ved Cour constitutionnelle (forfatningsdomstol, Belgien), og senere forenet i hovedsagen, havde Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL og UA, Liga voor Mensenrechten ASBL og Ligue des Droits de l'Homme ASBL samt VZ, WY og XX nedlagt påstand om annullation af lov af 29. maj 2016 med den begrundelse, at denne lov tilsidesatte artikel 10 og 11 i den belgiske forfatning, sammenholdt med EMRK's artikel 5, 6-11, 14, 15, 17 og 18, chartrets artikel 7, 8, 11 og 47 samt artikel 52, stk. 1, artikel 17 i den internationale konvention om borgerlige og politiske rettigheder, vedtaget af De Forenede Nationers Generalforsamling den 16. december 1966 og trådt i kraft den 23. marts 1976, generelle principper om retssikkerhed, proportionalitet, og selvbestemmelse på informationsområdet samt artikel 5, stk. 4, TEU.

3.1.2 De præjudicielle spørgsmål

Præjudicielt spørgsmål 1:

(Det første spørgsmål i sagerne C-511/18 og C-512/18 og det første og det andet spørgsmål i sag C-520/18)

> *"om artikel 15, stk. 1, i direktiv 2002/58 skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, pålægger udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata."* jf. præmis 81.

Præjudicielt spørgsmål 2:

(det andet og det tredje spørgsmål i sag C-511/18)

> *"om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at anvende foranstaltninger i deres netværk, der gør det muligt dels at foretage automatiseret analyse og indsamling i realtid af trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, uden at der er fastsat bestemmelse om, at de berørte personer skal underrettes om disse behandlinger og disse indsamlinger."* jf. præmis 169.

Præjudicielt spørgsmål 3:

(det andet spørgsmål i sag C-512/18)

> *"om bestemmelserne i direktiv 2000/31, sammenholdt med chartrets artikel 6-8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at disse bestemmelser er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, som disse tjenester gør brug af."* jf. præmis 193.

Præjudicielt spørgsmål 4:

(Det tredje spørgsmål i sag C-520/18)

> *"om en national ret kan anvende en bestemmelse i den nationale lovgivning, som giver denne ret bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester med henblik på bl.a. at forfølge formålene om at beskytte den nationale sikkerhed og om at bekæmpe kriminalitet, at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som følge af, at denne lovgivning er uforenelig med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1."* jf. præmis 213.

3.1.3 Afgørelsen

3.1.3.1 Generelt

Sagen omfattede de samme data, som lagres efter Logningsbekendtgørelsen.

> *"De data, som udbyderne af elektroniske kommunikationstjenester i medfør af disse lovgivninger skal lagre, er endvidere navnlig de data, der er nødvendige for at spore kilden til en kommunikation og dens bestemmelsessted, fastslå en kommunikations dato, tidspunkt, varighed og type, identificere det anvendte kommunikationsudstyr og foretage lokalisering af terminaludstyret og kommunikationerne, dvs. data, der navnlig omfatter navn og adresse på brugeren, telefonnummer på den, der foretager opkaldet, og det kaldte nummer samt for internettjenester en IP-adresse. De nævnte data omfatter derimod ikke indholdet af den pågældende kommunikation."* jf. præmis 82.

> *"De data, der i henhold til de i hovedsagerne omhandlede nationale lovgivninger skal lagres i et år, gør det således navnlig muligt at få kendskab til, med hvilken person brugeren af et elektronisk kommunikationsmiddel har kommunikeret, og ved hjælp af hvilket middel denne kommunikation har fundet sted, at fastslå datoen og tidspunktet for samt varigheden af kommunikationen og internetforbindelsen, og den lokalitet, hvorfra den har fundet sted, og at få kendskab til lokaliseringen af terminaludstyr, uden at der nødvendigvis er sket overføring af kommunikation. Desuden gør disse data det muligt at få kendskab til hyppigheden af brugerens kommunikation med bestemte personer i en given periode. Hvad endelig angår den i sagerne C-511/18 og C-512/18 omhandlede nationale lovgivning synes denne lovgivning, for så vidt som den også omfatter de data, der vedrører overføring af elektronisk kommunikation via netværk, at gøre det muligt at identificere arten af de oplysninger, der er tilgået online."* jf. præmis 83.

Sagen vedrørte lagring med henblik på nogle af de samme formål som Logningsbekendtgørelsen og Tele 2/Watson behandlede, idet sagen dog i højere grad fokuserede på lagring til forebyggelse og håndtering af trusler mod national sikkerhed.

> *"Hvad angår de forfulgte formål skal det bemærkes, at de i sagerne C-511/18 og C-512/18 omhandlede lovgivninger bl.a. har til formål at gøre det muligt at efterforske, fastslå og retsforfølge strafbare handlinger i almindelighed og at sikre hensynet til statens uafhængighed, den territoriale integritet og det nationale forsvar, væsentlige udenrigspolitiske interesser, opfyldelsen af Frankrigs europæiske og internationale forpligtelser, Frankrigs væsentlige økonomiske, industrielle og videnskabelige interesser samt hensynet til at forebygge terrorisme, angreb mod institutioners republikanske grundlag og kollektive voldshandlinger, der alvorligt påvirker opretholdelsen af lov og orden. Hvad angår den i sag C-520/18 omhandlede lovgivning har denne bl.a. til formål at gøre det muligt at efterforske, afsløre og retsforfølge strafbare handlinger samt at varetage hensynet til beskyttelsen af den nationale sikkerhed, forsvaret af territoriet og den offentlige sikkerhed."* jf. præmis 84.

3.1.3.2 Præjudicielt spørgsmål 1:

> *"om artikel 15, stk. 1, i direktiv 2002/58 skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, pålægger udbydere af elektroniske*

kommunikationstjenester at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata." jf. præmis 81.

"Det skal bemærkes, at Domstolen i de domme, hvori den har foretaget en fortolkning af direktiv 2002/58, endnu ikke konkret har taget stilling til det formål om beskyttelse af den nationale sikkerhed, som de forelæggende retter og de regeringer, der har afgivet indlæg, har henvist til" jf. præmis 134.

"Formålet om beskyttelse af den nationale sikkerhed, sammenholdt med artikel 4, stk. 2, TEU, vejer tungere end de andre formål, der er indeholdt i artikel 15, stk. 1, i direktiv 2002/58, bl.a. formålet om bekæmpelse af kriminalitet i almindelighed, herunder også grov kriminalitet, og om beskyttelse af den offentlige sikkerhed. Trusler som dem, der er nævnt i den foregående præmis, adskiller sig nemlig på grund af deres art og særligt alvorlige karakter fra den generelle risiko for, selv alvorlige, spændinger eller forstyrrelser, for den offentlige sikkerhed. Med forbehold for overholdelsen af de øvrige krav, der er fastsat i chartrets artikel 52, stk. 1, kan formålet om beskyttelse af den nationale sikkerhed derfor begrunde foranstaltninger, der indebærer indgreb i de grundlæggende rettigheder, som er mere alvorlige end dem, som disse andre formål kan begrunde." jf. præmis 136.

"En national lovgivning, der foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, overskrider det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 107)." jf. præmis 141.

- *"at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for lovgivningsmæssige foranstaltninger, der med henblik på de formål, der er fastsat i denne artikel 15, stk. 1, i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata. Den nævnte artikel 15, stk. 1, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, er derimod ikke til hinder for lovgivningsmæssige foranstaltninger*:

- *der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består.

- *der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af*

berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges.

- *der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige;*

- *der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler,*

- *der med henblik på bekæmpelse af grov kriminalitet og a fortiori med henblik på beskyttelsen af den nationale sikkerhed, gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over;*

- *for så vidt som disse foranstaltninger ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.*

3.1.3.3 Præjudicielt spørgsmål 2:

"om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at anvende foranstaltninger i deres netværk, der gør det muligt dels at foretage automatiseret analyse og indsamling i realtid af trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, uden at der er fastsat bestemmelse om, at de berørte personer skal underrettes om disse behandlinger og disse indsamlinger." jf. præmis 169.

"Henset til samtlige ovenfor anførte betragtninger skal det andet og det tredje spørgsmål i sag C-511/18 besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse ikke er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester dels at gøre brug af automatiseret analyse og indsamling i realtid af navnlig trafikdata og lokaliseringsdata, dels at foretage indsamling i realtid af de tekniske data, der vedrører lokaliseringen af det anvendte terminaludstyr, når

- *brugen af automatiseret analyse er begrænset til de situationer, hvor en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, og brugen af denne analyse kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om der foreligger en situation, der*

kan begrunde den nævnte foranstaltning, og om de betingelser og garantier, der skal være fastsat, er overholdt, og når

- *indsamlingen i realtid af trafikdata og lokaliseringsdata er begrænset til de personer, med hensyn til hvilke der foreligger rimelig grund til at mistænke, at de på den ene eller den anden måde er involveret i terrorvirksomhed, og er underlagt en forudgående prøvelse, der foretages af enten en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, for at sikre, at en sådan indsamling i realtid kun tillades inden for rammerne af, hvad der er strengt nødvendigt. I et behørigt begrundet hastende tilfælde skal denne prøvelse foretages hurtigst muligt.*

- *Hvad angår de oplysninger, der kræves i forbindelse med en automatiseret analyse af trafikdata og lokaliseringsdata, har den kompetente nationale myndighed pligt til at offentliggøre generelle oplysninger om denne analyse uden at skulle foretage en individuel underretning af de berørte personer. I det tilfælde, hvor dataene opfylder de parametre, der er præciseret i den foranstaltning, som gør det muligt at foretage en automatiseret analyse, og hvor denne myndighed identificerer den berørte person med henblik på at foretage en mere dybtgående analyse af de data, der vedrører den pågældende, er det til gengæld nødvendigt at give vedkommende en individuel underretning. En sådan underretning skal imidlertid kun ske for så vidt som og fra det tidspunkt, hvor den ikke kan skade udførelsen af de opgaver, der påhviler den nævnte myndighed (jf. analogt udtalelse 1/15 (PNR-aftalen mellem EU og Canada) af 26.7.2017, EU:C:2017:592, præmis 222-224).* jf. præmis 192.

3.1.3.4 Præjudicielt spørgsmål 3:

"om bestemmelserne i direktiv 2000/31, sammenholdt med chartrets artikel 6-8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at disse bestemmelser er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, som disse tjenester gør brug af." jf. præmis 193.

"Henset til de ovenfor anførte betragtninger skal det andet spørgsmål i sag C-512/18 besvares med, at direktiv 2000/31 skal fortolkes således, at dette direktiv med hensyn til informationssamfundstjenester ikke finder anvendelse på området for beskyttelse af kommunikationshemmeligheden og af fysiske personer i forbindelse med behandlingen af personoplysninger, idet denne beskyttelse alt efter omstændighederne er reguleret ved direktiv 2002/58 eller forordning 2016/679. Artikel 23, stk. 1, i forordning 2016/679, sammenholdt med chartres artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, der er forbundet med brugen af disse tjenester." jf. præmis 212.

3.1.3.5 Præjudicielt spørgsmål 4:

(Det tredje spørgsmål i sag C-520/18)

"om en national ret kan anvende en bestemmelse i den nationale lovgivning, som giver denne ret bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester med henblik på bl.a. at forfølge formålene om at beskytte den nationale sikkerhed og om at bekæmpe kriminalitet, at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som følge af, at denne lovgivning er uforenelig med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1." jf. præmis 213.

" Ifølge princippet om EU-rettens forrang har EU-retten en fortrinsstilling i forhold til medlemsstaternes nationale ret. Dette princip medfører derfor en forpligtelse for alle instanser i medlemsstaterne til at sikre, at de forskellige EU-retlige regler gennemføres fuldt ud, idet medlemsstaternes nationale ret ikke kan ændre den virkning, som disse forskellige regler tillægges på disse staters område (dom af 15.7.1964, Costa, 6/64, EU:C:1964:66, s. 1159 og 1160, og af 19.11.2019, A.K. m.fl. (Den øverste domstols disciplinærafdelings uafhængighed), C-585/18, C-624/18 og C-625/18, EU:C:2019:982, præmis 157 og 158 og den deri nævnte retspraksis)." jf. præmis 214.

"Den nationale ret, der inden for sit kompetenceområde skal anvende EU-retlige bestemmelser, har i henhold til princippet om forrang pligt til – såfremt det ikke er muligt at anlægge en fortolkning af national lovgivning, der er i overensstemmelse med de EU-retlige krav – at sikre disse bestemmelsers fulde virkning, idet den om fornødent af egen drift skal undlade at anvende enhver modstående bestemmelse i national lovgivning, endog en senere national bestemmelse, uden at den behøver at anmode om eller afvente en forudgående ophævelse af denne bestemmelse ad lovgivningsvejen eller ved noget andet forfatningsmæssigt middel." jf. præmis 215.

"Den forelæggende ret kan derfor ikke anvende en bestemmelse i den nationale lovgivning, der giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til den i hovedsagen omhandlede nationale lovgivning." jf. præmis 220.

"Effektivitetsprincippet pålægger derfor den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder." jf. præmis 227.

3.1.4 Perspektivet til nærværende sag

EU-Domstolen bekræftede i C-520/18 Ordre des Barreaux, m.fl., hvad EU-Domstolen allerede havde fastlagt i Tele 2/Watson og Digital Rights Ireland, nuancerede enkelte problemstillinger og kom med forholdsvis aktivistiske løsninger på, hvordan medlemsstaterne rent faktisk kan fortsætte med en begrænset form for logning.

EU-Domstolen bekræftede endnu engang, at:

> *"national lovgivning, der foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, overskrider det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1 (jf. i denne retning dom af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 107)."* jf. præmis 141.

Logningsbekendtgørelsen, der netop baserer sig på generel og udifferentieret lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, er således i strid EU chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, som også fastslået i Tele2/Watson.

Sagsøgte kan ikke troværdigt eller med grundlag i gældende praksis fastholde, at Sagsøgte ikke kan udlede, i hvilket omfang Logningsbekendtgørelsen er i strid med EU-Domstolens praksis.

I generaladvokatens udtalelse til C-520/18 Ordre des Barreaux, m.fl. blev det gjort gældende, at medlemsstater "*vanskeligt*" kan indrette lovgivningen på en måde der respekterer borgernes rettigheder. I sit udkast til afgørelse afviste generaladvokaten at lægge den påstand til grund, jf. præmis 151-154. Logningsbekendtgørelsen er fuldt ud i strid med EU-Domstolens praksis. Sagsøgtes kategorisering af Logningsbekendtgørelsen som et begrænset indgreb i EU Chartrets og EMRK's grundlæggende rettigheder er gentagne gange understreget af EU-Domstolens praksis som en forkert fortolkning.

Sagsøgte har ikke handlet "hurtigst muligt" ved at bringe retstilstanden i overensstemmelse med gældende ret, som fastlagt gentagne gange af EU-Domstolen.

EU-Domstolen understregede endvidere konsekvensen af EU rettens forrangsvirkning for de nationale domstole ved at anføre konkret:

- *"Ifølge princippet om EU-rettens forrang har EU-retten en fortrinsstilling i forhold til medlemsstaternes nationale ret. Dette princip medfører derfor en forpligtelse for alle instanser i medlemsstaterne til at sikre, at de forskellige EU-retlige regler gennemføres fuldt ud, idet medlemsstaternes nationale ret ikke kan ændre den virkning, som disse forskellige regler tillægges på disse staters område (dom af 15.7.1964, Costa, 6/64, EU:C:1964:66, s. 1159 og 1160, og af 19.11.2019, A.K. m.fl. (Den øverste domstols disciplinærafdelings uafhængighed), C-585/18, C-624/18 og C-625/18, EU:C:2019:982, præmis 157 og 158 og den deri nævnte retspraksis)."* jf. præmis 214.

- *"Den nationale ret, der inden for sit kompetenceområde skal anvende EU-retlige bestemmelser, har i henhold til princippet om forrang pligt til – såfremt det ikke er muligt at anlægge en fortolkning af national lovgivning, der er i overensstemmelse med de EU-retlige krav – at sikre disse bestemmelsers fulde virkning, idet den om fornødent af egen drift skal undlade at anvende enhver modstående bestemmelse i national lovgivning, endog en senere national bestemmelse, uden at den behøver at anmode om eller afvente en forudgående ophævelse af denne bestemmelse ad lovgivningsvejen eller ved noget andet forfatningsmæssigt middel."* jf. præmis 215.

- *"Domstolen fastslog imidlertid i en sag, der omhandlede spørgsmålet om, hvorvidt foranstaltninger, der var vedtaget i strid med den forpligtelse, som er fastsat i EU-retten, til at foretage en forudgående vurdering af et projekts indvirkning på miljøet og på en beskyttet lokalitet, at en national domstol, hvis dens nationale ret tillader det, undtagelsesvis kan opretholde virkningerne af sådanne foranstaltninger, hvis denne opretholdelse er begrundet ved tvingende hensyn knyttet til nødvendigheden af at fjerne en reel og alvorlig trussel om afbrydelse af forsyningen med elektricitet i den pågældende medlemsstat, som ikke kan imødegås med andre midler og alternativer, herunder navnlig inden for rammerne af det indre marked, idet den nævnte opretholdelse kun kan omfatte den tidsperiode, som er strengt nødvendig for at afhjælpe denne ulovlighed."* jf. præmis 218.

- *"En tilsidesættelse af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, kan i modsætning til tilsidesættelsen af en proceduremæssig forpligtelse, såsom den forudgående vurdering af virkningerne af et projekt inden for det særlige område for miljøbeskyttelse, imidlertid ikke afhjælpes ved en procedure, der kan sammenlignes med den procedure, som er nævnt i den foregående præmis. Opretholdelsen af virkningerne af en national lovgivning som den i hovedsagen omhandlede ville nemlig indebære, at denne lovgivning fortsat ville pålægge udbydere af elektroniske kommunikationstjenester forpligtelser, der er i strid med EU-retten, og som ville medføre alvorlige indgreb i de grundlæggende rettigheder, der tilkommer de personer, hvis oplysninger er blevet lagret."* jf. præmis 219

- *"Den forelæggende ret kan derfor ikke anvende en bestemmelse i den nationale lovgivning, der giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til den i hovedsagen omhandlede nationale lovgivning."* jf. præmis 220

Logningsbekendtgørelsen er i strid med EU retten ved EU chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, som også fastslået i Tele2/Watson. Retten skal i medfør af forrangsprincippet følge EU-Domstolens vurdering i den forbindelse og kan ikke anlægge en selvstændig vurdering heraf. Retten kan ikke opretholde Logningsbekendtgørelsen som en "midlertidig" retsstilling, indtil Sagsøgte er kommet frem til et "passende" alternativ.

EU-Domstolen udviste endvidere forståelse for medlemsstaternes udfordringer med at balancere effektiv trusselsbekæmpelse med grundlæggende rettigheder ved at anvise mulige løsninger på, hvordan Danmark kunne regulere logning og ramme den balance. Det er imidlertid ikke et tema i nærværende sag, selvom Sagsøgte i sit svarskrift angiver netop den udfordring som et anbringende for den fortsatte opretholdelse af den ulovlige Logningsbekendtgørelse. EU-domstolen har således helt undtagelsesvist anvist en vej for medlemsstaterne for fortsat logning i begrænset og kontrolleret omfang. Det er derfor ikke korrekt, når Sagsøgte i sit svarskrift anfører, at en øjeblikkelig standsning vil få uoverstigelige konsekvenser. Sagsøgte kunne udvise rettidig omhu ved ikke at opretholde ugyldig lovgivning og evt. begynde at forberede ny lovgivning "hurtigst muligt."

EU-Domstolen fastlægger endvidere, at der er tale om så væsentligt et brud på rettighederne i EU Chartret, at de pågældende ulovligt indhentede oplysninger alene kan anvendes som bevis i straffesager under iagttagelse af særlige garantier, jf. bl.a. præmis

227. Dette er heller ikke et tema i nærværende sag, men bestyrker vurderingen af EU-Domstolens vurdering af væsentligheden i den belgiske og den franske stats overtrædelse af EU-retten ved fortsat at opretholde EU-stridige logningsregler. Tilsvarende hvad den danske stat ved Sagsøgte gør.

3.2 Logningsbekendtgørelsen opretholdes og håndhæves fortsat af Sagsøgte

Sagsøgte har ikke taget nogle effektive tiltag til ophævelse, revision eller manglende håndhævelse af Logningsbekendtgørelsen, men tværtimod forsøgt at udvide logningsadgangen.

Logningsbekendtgørelsen opretholdes og håndhæves fortsat af Sagsøgte, og der lagres stadig ulovligt oplysninger om danske borgere, der stadig ulovligt udleveres til politiet.

3.2.1 § 13 i Lovforslag nr. 42 af 8. oktober 2020 om udvidelse af politiets adgang til lagrede data efter Logningsbekendtgørelsen

Lov nr. 128 af 7. februar 2014 som løbende ændret om elektroniske kommunikationsnet og tjenester, ("Teleloven") er netop blevet gennemgående revideret den 21. december 2020 ved implementering af direktiv 2018/1972 om en europæisk kodeks for elektronisk kommunikation.

Logningsbekendtgørelsen er hjemlet i Retsplejelovens § 786, stk. 4 og 7 og ikke direkte i Teleloven. Telelovens §§ 8-10 indeholder dog regler om persondatasikkerhed for eksempelvis loggede oplysninger under Logningsbekendtgørelsen og pligt til indretning af udstyr, så der kan ske indgreb i meddelelseshemmeligheden i form af aflytning eller adgang til oplysninger lagret i medfør af Logningsbekendtgørelsen. Det ville derfor have været nærliggende at revidere Logningsbekendtgørelsen eller reguleringen der omkring i forbindelse med den gennemgribende regulering af Teleloven i efteråret 2020.

Regeringens 1. behandlede lovforslag nr. 42, som fremsat den 8. oktober 2020, indeholdt da også følgende ændring af § 13:

> *"§ 13. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal på begæring af politiet som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester, herunder oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt."*

Følgende følger af lovforslagets bemærkninger (side 33):

> *"§13 giver politiet adgang, uden kendelse, til oplysninger om en slutbrugers adgang til kommunikationsnet og –tjenester, herunder IP-adresser og mailadresser. Bestemmelsen omfatter oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger."*
>
> *"Med den foreslåede bestemmelse i telelovens § 13 udvides bestemmelsen ved, at det tydeligt vil blive angivet, at IMI nummer [er en mobiltelefons unikke identifikationsnummer, og kan sammenlignes med et serienummer, som kan benyttes til at identificere enhver mobiltelefon] er omfattet af bestemmelsen. Desuden vil det*

blive præciseret, at politiet kun indhenter IMEI-oplysning for en afgrænset periode og at denne periode er så kort som muligt. Endelig vil bestemmelsen blive indskrænket i forhold til gældende ret, idet der vi blive indsat krav om, at bestemmelsen kun kan anvendes i forbindelse med efterforskning af alvorlig kriminalitet."

Regeringen fremsatte således så sent som i efteråret 2020 et lovforslag om at tilføje øget adgang for politiet til at indhente data, de såkaldte IMEI nr. der er lagret i medfør af Logningsbekendtgørelsen. Dette endda uden retskendelse eller nogle af de øvrige retslige garantier, der er fastlagt i Tele 2/Watson og igen 2 dage forinden i medfør af C-520/18 Ordre des Barreaux, m.fl.

Dette blev heller ikke vel modtaget af de øvrige ordførere i fremsættelsesdebatten, hvoraf der nedenfor er angivet et uddrag.

Kristian Hegaard (RV) kommenterede:

"Tak for det. For 2 uger siden kom der en ny EU-afgørelse, som slår fast, at de generelle og udifferentierede danske logningsregler – den måde, vi håndterer det på – fortsat er i strid med EU-retten. Det har jeg selvfølgelig forståelse for at man på det tidspunkt, hvor louforslaget blev fremsat, ikke har kunnet nå at tage højde for og iagttage. Men mener ordføreren ikke, at det lige er en postgang for tidligt at ændre telelovens § 13, sådan at politiet kan indhente IMEI-numre uden retskendelse? Det er jo kun noget, som teleselskaberne er forpligtet til at opbevare som følge af de nuværende logningsregler, som der på baggrund af den nye EU-afgørelse kan sås tvivl om hvorvidt overhovedet er tilladt – altså hvorvidt det overhovedet er tilladt at indsamle logning på den måde. Skulle man ikke lige tænke sig en ekstra gang om og så vente med at ændre telelovens § 13, sådan som der er lagt op til her?"

Christoffer Aagaard Melson (V) kommenterede tilsvarende:

"Der er i høringssvarene også kritik af, at det i forslaget om telelov indskrives, at politiet giver adgang til logning af oplysninger vedrørende IMEI-oplysninger. Det er en bestemmelse, der efter branchens opfattelse rettelig hører til i retsplejeloven. Begrundelsen for, at man placerer det her i telelovgivningen i stedet for i retsplejeloven, vil vi gerne spørge ind til. Derudover vil vi selvfølgelig også gerne spørge ind til, hvordan det hænger sammen i forhold til den dom, der lige netop er afsagt i EU. Det er jo ikke det samme, som at jeg her siger, at vi eventuelt ikke kan stemme for. Men der er i hvert fald nogle ting, som vi har brug for at stille nogle spørgsmål til."

Ruben Kidde (RV) kommenterede:

"Men der er et vigtigt opmærksomhedspunkt, specifikt vedrørende den foreslåede § 13, som både IT-politisk Forening, PROSA og Teleindustrien er stærkt kritiske over for i deres høringssvar. Teleindustrien har bl.a. anført, at man finder udkastet til ændringen af telelovens § 13 og det tilhørende udkast til lovbemærkninger for uhensigtsmæssige, og at lovudkastet efter Teleindustriens opfattelse ikke skaber den ønskede klare hjemmel til, at politiet får adgang til IMEI-oplysninger uden rettens godkendelsen.

De opfordrer desuden til, at den nye regel om udlevering af IMEI-oplysninger placeres under retsplejelovens kapitel 71 og ikke i teleloven, idet IMEI-

oplysninger efter deres opfattelse er logningspligtige data, dvs. data, som teleselskaberne udelukkende registrerer som følge af kravet herom i logningsreglerne.

Den her del specifikt om § 13 vil jeg med afsæt i ovenstående bemærkninger foreslå bliver pillet helt ud af indeværende lovforslag for i stedet for at blive behandlet i regi af retsplejeloven, som jo er sat på lovprogrammet i februar. Alternativt kunne man dele lovforslaget op, og det har jeg så også haft en dialog med ministeren om. Men der er ingen tvivl om, at IMEI-oplysninger er vigtige efterforskningsværktøjer, men efter Radikale Venstres opfattelse bør det så betyde, at man får en retskendelse, ligesom det gælder for alle andre efterforskningsværktøjer, hvilket jo passer godt ind, i forhold til at man så behandler det i retsplejeloven.

Så med de bemærkninger – overordnet positive omkring direktivimplementeringen, men meget, meget kritiske over for lige præcis paragraf 13 – ser vi frem til den videre udvalgsbehandling af lovforslaget."

Signe Munk (SF):

"I SF har vi dog et stort problem med § 13 og mener derfor på linje med Det Radikale Venstre, at forslaget bør splittes op, for det er ret afgørende for SF's støtte til lovforslaget."

Eva Flyvholm (EL):

" Fra Enhedslistens side synes vi, det er meget problematisk, at der lige har sneget sig lidt for meget ind i det her lovforslag. § 13, der handler om logning, kommer ikke fra direktivet, det kommer ikke af den aftale, vi lavede på teleområdet, det er noget, der ligesom er blevet smidt ind fra højre, som man kunne blive fristet til at sige. Jeg synes, det er dybt problematisk, det ligger her, for det giver en øget mulighed for logning også uden en dommerkendelse, som vi ser det, og det er virkelig problematisk i forhold til retssikkerheden. Derfor ønsker vi ligesom Radikale og SF, at den her del bliver pillet ud af loven, for ellers har jeg også meget svært ved at se, at vi skulle kunne støtte det her forslag. Så det håber jeg vi kan komme i mål med undervejs i lovarbejdet, og jeg synes, det ville være helt uansvarligt at lade det blive hængende her på den måde."

Ole Birk Olesen (LA):

"Tak for det. Det er et omfattende lovforslag, hvor jeg kan sige at Liberal Alliance støtter det meste. Vi er skeptiske over for § 13 om logning og har behov for at dykke yderligere ned i det. Det kan godt ende sådan, at vi synes, at det er så problematisk, at vi må stemme nej til hele lovforslaget, men det kan også være, at ministeren kunne være åben over for at skille det ud – det får vi se. Som sagt er det et udmærket lovforslag med en enkelt knast, som kan gøre, at vi må stemme imod."

Dan Jørgensen, Minister:

"Jeg har i forbindelse med bemærkningerne her i dag og også tidligere kontakt med flere af jer bemærket, at der er foreslået ændringer af § 13, hvor det enten ønskes, at man opdeler lovforslaget i to, eller at man lader hele den del udgå. Det vil jeg se på, og mit ministerie vil meget gerne være behjælpelig med at lave ændringsforslag af den ene eller den anden karakter i den henseende, så lad os tage

en nærmere drøftelse af det i forbindelse med jeres udvalgsbehandling og den dialog, vi har med ministeriet."

I forbindelse med lovforslagets fremsættelse var vedlagt høringssvar, der for de fleste var stærkt kritiske overfor at introducere en udvidelse af logningsreglerne efter § 13, blandt andet med henvisning til manglende lovhjemmel og ageren i strid med EU-retten, jf. Høringssvarene vedrørende § 13 er vedlagt som Bilag 12.

I 2. behandlingen af lovforslag nr. 42, blev ændringen af § 13 dog trods alt også taget ud.

3.2.2 Sagsøgte har ikke iværksat nogle tiltag som reaktion på C-520/18 Ordre des Barreaux, m.fl.

Siden EU-Domstolens afgørelse den 6. oktober 2020 har Justitsministeriet den 19. november 2020 orienteret Folketingets Retsudvalg og Europaudvalg om C-520/18 Ordre des Barreaux, m.fl. og angivet:

"Justitsministeriet studerer nu dommen med henblik på at vurdere, i hvilket omfang Danmark vil kunne opretholde de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Det sker med henblik på at kunne præsentere et udkast til revision af de danske regler på området." jf. Bilag 13.

Dommen fastlægger meget klart, at Logningsbekendtgørelsen er i strid med EU-retten. Dette vil Sagsøgte fortsat ikke erkende, men alene *vurdere* om de nuværende regler vil kunne opretholdes eller skulle revideres.

Sagsøger bekendt er der ikke fremsat noget forslag siden den 19. november 2020.

Revision af retsplejeloven (Revision af reglerne om registrering og opbevaring af oplysninger om tele- og internettrafik (logning)) fremgår af Folketingets lovprogram for 2020/2021. Det har det imidlertid gjort de sidste mange år, idet det dog hvert år er blevet udskudt til næste år, som også gennemgået udførligt af Sagsøgte i svarskriftet.

Sagsøger har anmodet om aktindsigt den 14. december 2020 i det forberedende arbejde frem til dommen C 520/18 Ordre des Barreaux, m.fl. samt om arbejdet med revision af Logningsbekendtgørelsen. Sagsøger har endnu ikke modtaget nogen dokumentation i medfør af sin aktindsigt.

Sagsøger kan ikke anse Sagsøgtes ageren på anden måde end som udtryk for, at Sagsøgte ikke kommer til at tage nogle effektive tiltag til at ophæve eller ændre Logningsbekendtgørelsen, uden af Retten i medfør af nærværende sag underkender Logningsbekendtgørelsen.

3.3 Teledataskandalerne er eksempler på risikoen for misbrug af data lagret i medfør af Logningsbekendtgørelsen

3.3.1 Risiko for misbrug af adgang til lagrede data er en af EU-Domstolens væsentligste bekymringspunkter ved at indsamle, lagre og give adgang til sådanne data.

Et af hovedelementerne i EU-Domstolens vurdering af logningens uoverensstemmelse med Chartret og EMRK er misbrugsrisikoen ved at tiltro udbyderne og de udleverede myndigheder adgang til de lagrede data.

EU-Domstolen anførte eksempelvis i C-520/18 Ordre des Barreaux, m.fl.:

> *"For det andet bemærkes, at henset til den store mængde trafikdata og lokaliseringsdata, der løbende kan lagres ved hjælp af en generel og udifferentieret lagringsforanstaltning, og den følsomme karakter af de oplysninger, som disse data kan give adgang til, medfører alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, en risiko for misbrug og ulovlig adgang."* jf. præmis 119.
>
> *"For at opfylde kravet om proportionalitet skal en lovgivning fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug."* jf. præmis 132 og 168, samme Tele 2/Watson præmis 109 og Digital Rights Ireland præmis 54.

- *"Et påbud om at foretage forebyggende lagring af data, der vedrører alle brugere af elektroniske kommunikationsmidler, skal ikke desto mindre tidsmæssigt begrænses til det strengt nødvendige. Selv om det ikke kan udelukkes, at et påbud, der udstedes til udbyderne af elektroniske kommunikationstjenester, om at foretage lagring af data, kan forlænges som følge af, at en sådan trussel fortsat består, må varigheden af hvert enkelt påbud ikke overstige et forudseeligt tidsrum. Desuden skal en sådan lagring af data være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug. Denne lagring må således ikke have en systematisk karakter."* jf. præmis 138.

EU-Domstolen anførte endvidere i Tele 2/Watson:

- *"Rækkevidden af bestemmelserne i artikel 5 og 6 samt artikel 9, stk. 1, i direktiv 2002/58, der har til formål at sikre, at kommunikationen og de dermed forbundne data er hemmelige, og at minimere risikoen for misbrug, skal desuden bedømmes i lyset af 30. betragtning til direktivet, hvoraf det fremgår, at »[s]ystemer til levering af elektroniske kommunikationsnet og kommunikationstjenester bør konstrueres, så de begrænser mængden af nødvendige personoplysninger til et absolut minimum«."* jf. præmis 87.

- *"Hvad angår reglerne om sikkerheden vedrørende og beskyttelsen af de data, der lagres af udbydere af elektroniske kommunikationstjenester, bemærkes, at artikel 15, stk. 1, i direktiv 2002/58 ikke gør det muligt for medlemsstaterne at fravige direktivets artikel 4, stk. 1 eller stk. 1a. De sidstnævnte bestemmelser opstiller et krav om, at disse udbydere træffer passende tekniske og organisatoriske*

foranstaltninger, der gør det muligt at sikre en effektiv beskyttelse af de lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til disse data" jf. præmis 122.

3.3.2 De danske teledataskandaler er stærkt bekymrende eksempler på, hvordan sådanne fejl/misbrug kan opstå

De danske såkaldte "teledataskandaler" dækker over eksempler på en flerhed af fejl med indsamling, udlevering og politiets håndtering af data, der er lagret i henhold til Logningsbekendtgørelsen og udleveret til politiet efter retskendelse og den derved relaterede retslige prøvelse.

Det kom frem i efteråret 2018, at Telenor havde udleveret data til politiet, som slet ikke var omfattet af Logningsbekendtgørelsen, eller som Telenor ikke måtte udlevere efter de relaterede editionsregler. Der var tale om såkaldte signaleringsdata, indhold af SMS'er og B-numre (modtagers nummer). I den forbindelse blev der iværksat en undersøgelse af Rigspolitiet, der afdækkede yderligere problemer med yderligere data, ligesom der blev fundet fejl i datasæt fra andre udbydere.

Rigspolitiet oplyste endvidere i juni 2019, at der var fejl i det it-system, som politiet anvendte til at konvertere mastedata fra udbyderne, hvilket betød, at de lokaliseringsdata, der var anvendt i straffesager, var forkerte.

Teledataskandalerne vidner ikke om ondsindet misbrug men om de systemiske fejl, som kan forekomme, og hvordan det kan få indgribende konsekvenser for de berørte registrerede. Som EU-Domstolen anfører,

> *"Alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, udgør en risiko for misbrug og ulovlig adgang."* jf. præmis 119 i C-520 m.fl.

Teleskandalerne er eksempler på de risici, der er forbundet med at have lagret og adgang til omfattende metadata, hvor selv en tilsyneladende effektiv proces omkring krav om retskendelse ikke udgør tilstrækkelige garantier til at sikre de berørte personers personoplysninger mod risiko for misbrug, jf. C-520/18 Ordre des Barreaux, m.fl. Præmis 132 og 168, samme Tele 2/Watson præmis 109 og Digital Rights Ireland præmis 54.

Uddrag fra teledataskandalerne er angivet nedenfor.

3.3.2.1 Telenor-sagen

Justitsministeriet anmodede den 30. januar 2020 Rigspolitiet om en redegørelse for politiets håndtering af Telenor-sagen.

Den 17. april 2020 forelå Rigspolitiets Redegørelse om teledatasagen, jf. Bilag 14.

Rigspolitiet konkluderede i den forbindelse, at udover forholdene med Telenor, var der også andre udbydere, der havde udleveret flere og andre data end påkrævet.

Rigspolitiet konkluderede i sin Redegørelse, at der ikke var tale om data, som var omfattet af politiets retskendelse, eller som politiet havde bedt om. Det var således Telenor selv, der af egen drift havde udleveret de pågældende data. Der var tale om en systemisk fejl hos Telenor.

Telenor havde siden september 2018 til april 2019 systematisk udleveret signaleringsdata til politiet i forbindelse med udlevering af mastedata.

Forskellen på signaleringsdata og masterdata, hvoraf kun sidstnævnte er omfattet af Logningsbekendtgørelsen, er beskrevet i Rigspolitiets Redegørelse om teledatasagen, jf. Bilag 14, pkt. 2.3.1, således:

> *"Signaleringsdata adskiller sig bl.a. fra almindelige masteoplysninger ved, at signaleringsdata også viser, når telefonen kommunikerer/signalerer til mobilnetværket, selv om den person, der er i besiddelse af telefonen, ikke aktivt anvender telefonen på det pågældende tidspunkt."*

Konkret betyder det, at telefonens placering registreres langt oftere. Det gør det muligt at følge en borgers bevægelser med høj præcision, uanset om der sendes eller modtages sms'er og opkald. Det er således langt mere indgribende.

Signaleringsdata kan godt registreres i en kortere periode til anvendelse for fejlretning i netværket, men må ikke tilsvarende data lagret under Logningsbekendtgørelsen registreres til andre formål, opbevares i 1 år eller udleveres til politiet.

Telenor havde ved samme udlevering også inkluderet det såkaldte B nummer (modtagers nummer), hvilket de heller ikke i samme ombæring måtte udlevere ved kendelser om edition efter Retsplejelovens kapitel 74.

Det viste sig endvidere, at Telenor også ved fejl havde indleverede SMS-indhold til Politiet helt frem til juni 2019.

Kommunikationsindhold, såsom SMS-beskeder, må slet ikke registreres af udbyderne i medfør af Logningsbekendtgørelsen.

Rigspolitiet fandt i sin redegørelse også, at der gik for lang tid fra at Rigspolitiet blev opmærksom på problemet i efteråret 2018 til, at Rigspolitiet endeligt rettede henvendelse til Telenor og fik problemet løst, i hvilken periode overtrædelserne fortsatte, uden de berørte registrerede personer var vidende om det.

3.3.2.2 Øvrige teleselskaber havde også fejl i udlevering af teledata til politiet

På baggrund af sagen med Telenor iværksatte Rigspolitiet en stikprøve-analyse af modtaget logningspligtig mastedata fra de øvrige teleselskaber, jf. Bilag 14. Rigspolitiet fandt i den forbindelse følgende:

Telia

Før stikprøverne blev igangsat, opdagede man i forbindelse med Telenor-sagen, at også Telia havde udleveret ikke-logningspligtig data: af tre tilfældigt udvalgte datasæt, der alle var indhentet i forbindelse med editionskendelser, forekom der i to af dem modpartsnumre (B-numre).

I forbindelse med de efterfølgende stikprøver af samtlige teleudbyderes indleverede data kunne det konstateres, at der fandtes modpartsoplysninger (B-numre) i 10 datasæt fra Telia i perioden efter den 29. januar 2019. Disse 10 datasæt indgik i 29 datasæt indhentet hos Telia og Hi3G. Der blev ikke fundet SMS-indhold i Telias data, men der

blev dog fundet information om, hvor mange tegn, der var blevet sendt i de enkelte SMS-beskeder.

Hi3G

Der blev ikke fundet modpartsoplysninger (B-numre) i Hi3G's data i ovennævnte stikprøve på samlet set 29 datasæt (fordelt mellem Telia og Hi3G). Dog fandt politiet i februar 2020, at Hi3G registrerede aktivitet i hele timer, hvilket indikerede at Hi3G indleverede for meget data. Det kunne dog ikke konkluderes med sikkerhed.

TDC

Hos TDC blev der også afdækket fejl, hvoraf fire indberetninger fra TDC til Erhvervsstyrelsen nævnes i Rigspolitiets redegørelse. Tre af indberetningerne omfatter udlevering af data for længere tidsrum end anmodet om. Den fjerde indberetning omfatter udlevering af data for et forkert tidspunkt i forhold til tidspunktet angivet i kendelsen.

Der er i TDC's tilfælde tale om enkeltstående fejl og ikke systematiske brister, som det f.eks. var tilfældet for Telenor.

3.3.2.3 Systemfejl i Rigspolitiets eget it-program til håndtering af udleveret trafikdata

Efter teledataskandalerne i forbindelse med Telenor-sagen opstod der allerede i juni 2019 endnu en såkaldt teledataskandale.

Rigsadvokaten orienterede i juni 2019 Advokatsamfundet, Landsforeningen af Forsvarsadvokater og Domstolsstyrelsen om, at Rigspolitiet havde afdækket systemfejl i det it-program, som politiet brugte til konvertering af den rådata, de modtog fra teleselskaberne.

Rigspolitiet havde identificeret fejl i forbindelse med konverteringen af mastedata fra udbyderne, hvorefter de geografiske koordinater for telemasters placering var blevet upræcise.

Justitsministeriet anmodede Rigspolitiet om en redegørelse, som Rigspolitiet udgav den 28. september 2019, jf. Bilag 15.

Det fremgik af Rigspolitiets redegørelse, at Rigspolitiets Telecenter i august 2019 havde gennemgået mastepositionerne i samtlige datasæt, som Telecentret på dette tidspunkt havde identificeret som potentielt fejlbehæftede. I disse datasæt afveg mastepositionerne i den konverterede data fra rådataen med 100-220 meter, jf. Bilag 15.

På baggrund af fejlen suspenderede Rigsadvokaten midlertidigt brugen af teledata som bevismateriale, og der blev efterfølgende identificeret 10.700 straffesager i perioden fra 2012 til 2019, hvor mulig ukorrekt data havde været anvendt som bevismateriale, og som derfor skulle gennemgås.

Regeringen har nedsat en kulegravningsgruppe, der blandt andet skal fastsætte retningslinjer for myndighedernes gennemgang af de mange sager. Den skal blandt andet afgøre, om det er politiet eller en uvildig tredjepart, der skal foretage den indledende screening af sagerne, og hvordan sagen skal vurderes, hvis der ikke længere kan skaffes korrekte mastedata.

Rigspolitiet har i øvrigt erkendt at have kendt til problemstillingen allerede fra februar 2019, selvom Rigspolitiet først orienterede landets forsvarsadvokater og domstolsstyrelsen om forholdet efter folketingsvalget i juni 2019. I mellemtiden blev mastedata løbende anvendt som bevis i straffesager for domstolene.

4. BESVARELSE AF UDVALGTE FORHOLD FRA SAGSØGTES SVARSKRIFT

4.1 EMRK art. 8 (Retten til privatliv)

Sagsøgte anfører i sit svarskrift, at der ikke er grundlag for, at Logningsbekendtgørelsen skulle være i strid med EMRK art. 8 (Retten til privatliv), og at Sagsøger ikke har redegjort herfor.

Dette er Sagsøger uenig i.

Sagsøger kan gentage sin bemærkning i stævningens punkt 3.6.1. Baggrunden for, at EU-domstolen ikke specifikt nævner EMRK art. 8 i domskonklusionen men i øvrigt generelt henviser til EMRK i sammenhæng med Chartrets art. 7 er, at primært den Europæiske Menneskerettighedsdomstol har kompetencen til at fortolke EMRK. EU-domstolen henviser generelt til EMRK i dommen, men i sin domskonklusion henvises alene til Chartret, der er EU-domstolens jurisdiktion. EU-domstolen skriver konkret om samme i Tele2/Watson:

> "*Indledningsvist bemærkes, at selv om de grundlæggende rettigheder, som er anerkendt ved EMRK, udgør generelle principper i EU-retten, således som det bekræftes af artikel 6, stk. 3 TEU, udgør EMRK ikke et retligt instrument, der er formelt registreret i Unionens retsorden, så længe Unionen ikke har tiltrådt den. Den i det foreliggende tilfælde omhandlende fortolkning af direktiv 2002/58 skal således alene anlægges i lyset af de grundlæggende rettigheder, der er sikret ved Chartret."* jf. præmis 127 og 128.

Sagsøger skal endvidere udbygge med, at EU-Domstolen også forholder sig konkret til spørgsmålet i C-520/18 Ordre des Barreaux, m.fl.:

> *"Det skal endvidere bemærkes, at chartrets artikel 52, stk. 3, har til formål at sikre den nødvendige sammenhæng mellem de i chartret indeholdte rettigheder og de tilsvarende ved EMRK sikrede rettigheder, uden at dette berører EU-rettens og Den Europæiske Unions Domstols autonomi. Der skal derfor ved fortolkningen af chartret tages hensyn til de tilsvarende rettigheder i EMRK som tærskel for minimumsbeskyttelse (jf. i denne retning dom af 12.2.2019, TC, C-492/18 PPU, EU:C:2019:108, præmis 57, og af 21.5.2019, Kommissionen mod Ungarn (Brugsrettigheder over landbrugsarealer), C-235/17,EU:C:2019:432, præmis 72 og den deri nævnte retspraksis)."* jf. præmis 124.

Spørgsmålet om logning og aflytning har endnu været genstand for meget begrænset afprøvelse ved EMD. Relevante sager er Ben Faiza v. France (31446/12), Malone v. the UK (8691/79) og Zakharov v. Russia (47143/06).

De pågældende sager berører væsentlige principper af relevans for sagen, herunder at indgreb i metadata skal betragtes som lige så væsentlig som indgreb i kommunikationens indhold og bør overholde samme retslige garantier.

Overordnet kan Sagsøgte ikke bestride, at logning af teleoplysninger er et indgreb i privatlivet, som beskyttet af EMRK art. 8. Et sådant indgreb kan kun ske i

overensstemmelse med national ret, hvilket blandt andet understøttes af Menneskerettighedsdomstolen afgørelse i Big Brother Watch and Others v. the UK (58170/13 & 24960/15). Her tog EMD stilling til et tilfælde, hvor national ret stred imod EU-retten. Grundet EU-rettens forrang for national ret lagdes det til grund, at indgrebet derfor ikke opfyldte legalitetskravet i EMRK, jf. præmis 465-466.

Der drages klare paralleller til indeværende sag, hvor national ret ikke er i overensstemmelse med EU-retten, hvorfor indgreb efter denne nationale ret ikke kan gennemføres.

Det er således Sagsøgers klare konklusion, at Logningsbekendtgørelsens er i strid med EMRK art. 8 om retten til privatliv.

4.2 EU Chartrets art. 7 (retten til respekt for privatliv og familieliv, hjem og kommunikation) og EMRK art. 10 (Retten til ytrings- og informationsfrihed)

Sagsøgte bestrider, at Logningsbekendtgørelsen strider mod presse eller ytringsfriheden.

Forholdet er reguleret af EU Chartrets art. 7 (enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation) og EMRK art. 10 (Retten til ytrings- og informationsfrihed).

Sagsøger henviser til stævningens punkt. 3.6.2.

Sagsøger skal endvidere udbygge med, at EU-Domstolen også forholder sig konkret til spørgsmålet i C-520/18 Ordre des Barreaux, m.fl.:

> *"For det første bemærkes, at lagring af trafikdata og lokaliseringsdata med henblik på politimæssige formål i sig selv kan medføre et indgreb i retten til respekt for kommunikation, der er sikret ved chartrets artikel 7, og have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved dette charters artikel 11 (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 28, og af 21.12.2016, Tele2, C- 203/15 og C-698/15, EU:C:2016:970, præmis 101)."* jf. præmis 118.

> *"En national lovgivning, der gør det muligt at foretage en sådan automatiseret analyse af trafikdata og lokaliseringsdata, indebærer imidlertid en fravigelse fra den principielle forpligtelse, der er fastsat i artikel 5 i direktiv 2002/58, til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data. En sådan lovgivning udgør endvidere et indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, uanset hvilken brug der efterfølgende gøres af disse data. Endelig kan den nævnte lovgivning i overensstemmelse med den retspraksis, der er nævnt i denne doms præmis 118, have afskrækkende virkning på udøvelsen af ytringsfriheden, som er sikret ved chartrets artikel 11."* jf. præmis 173

Den afskrækkende virkning kan konkret betyde, at whistleblowers ikke tør kontakte journalister. EMRK art. 10 beskytter pressefriheden, herunder retten til hemmelige kilder, se Goodwin v. UK (1996), især afsnit 39. Logningsbekendtgørelsen, og Retsplejelovens regler om edition tager ikke stilling til denne særlige beskyttelse. Der findes

således ingen garanti imod udlevering med formålet at afsløre kilder. Se desuden ovenfor om teledataskandalerne for risikoen for misbrug.

4.3 Underretning af berørte personer

Sagsøger bestrider Sagsøgtes udlægning af, at der sker underretning af de berørte personer.

Sagsøgte redegør for reglerne i Retsplejeloven § 788, stk. 1 om, at der efter afslutning af et indgreb i meddelelseshemmeligheden skal ske underretning til de berørte personer. Sagsøgte henviser også til, at Retsplejeloven § 788, stk. 4 angiver, at sådan underretning undtagelsesvist ikke sker, hvis det vil være til skade for efterforskningen.

Sagsøgte har ikke dokumenteret, at hovedreglen er underretning efter stk. 1, i stedet for en praksis om undtagelse efter stk. 4. Sagsøgte overser § 788, stk. 5, hvorefter der ikke skal gives underretning ved indhentning af "udvidet teleoplysning", hvilket vil sige identifikation af personer i et givent område, eksempelvis hvor der indhentes lister over deltagerne i et politisk møde eller optog.

Forløbet omkring Telenor-sagen, hvor parterne skulle kontakte de berørte personer viste sig da heller ikke at kunne gennemføres, på trods af, at der var tale om et ulovligt indgreb, jf. Rigspolitiels beretning herom i Bilag 14.

Uanset ovenstående, er den manglende eller utilstrækkelige underretning af de berørte personer alene et enkelt af flere kumulative krav til en begrænset logning, som EU-Domstolen anfører, hvoraf Logningsbekendtgørelsen ikke overholder langt de fleste krav og allerede af den grund er ulovlig.

København, 7. januar 2021

Julie Bak-Larsen, Partner

KAMMERADVOKATEN

25. FEBRUAR 2021

4000587 RHO / PEAH

Duplik

Til

Østre Landsret

I sagsnr. BS-19085/2018-KBH: Foreningen imod Ulovlig Logning
(Advokat Martin von Haller)

mod

Justitsminister Nick Hækkerup
Justitsministeriet
(Advokat Rass Holdgaard)

KØBENHAVN
VESTER FARIMAGSGADE 23
DK-1606 KØBENHAVN V

AARHUS
ÅBOULEVARDEN 49
DK-8000 AARHUS C

T +45 33 15 20 10
@ MAIL@KAMMERADVOKATEN.DK
W WWW.KAMMERADVOKATEN.DK

Indhold

1. INDLEDNING

EU-Domstolens dom af 6. oktober 2020 i *La Quadrature du Net m.fl.* (forenede sager C-511/18, C-512/18 og C-520/18, ECLI:EU:C:2020:791) (herefter "La Quadrature-dommen") indeholder en række nye elementer, som Domstolen ikke har konstateret før, og som er af væsentlig betydning for denne sag. Dommen viser, at det var korrekt og velbegrundet, at landsretten valgte at sætte denne sag i bero i afventning af Domstolens dom.

Det er således ikke korrekt, når sagsøgeren hævder, at Domstolen blot "*stadfæstede, hvad der allerede var blevet afgjort*" i Tele2-dommen og Digital Rights-dommen (replikken, side 3), eller at Domstolen alene "*nuancerede enkelte problemstillinger*" (replikken, side 10).

Domstolen fastslog for første gang i La Quadrature-dommen, at det under visse omstændigheder *er* muligt at opretholde generel og udifferentieret logning af hensyn til den nationale sikkerhed. Hverken Tele2-dommen eller Digital Rights-dommen tog stilling til, i hvilket omfang hensyn til den nationale sikkerhed kunne begrunde regler om logning af teleoplysninger.

En generel og udifferentieret logning forudsætter ifølge La Quadrature-dommen bl.a., at medlemsstaten står over for en alvorlig trussel mod den nationale sikkerhed.

La Quadrature-dommen betyder på den ene side, at de danske regler om logning og brug af loggede teleoplysninger nu skal ændres. På den anden side betyder dommen, at den nugældende logningsforpligtelse for teleselskaberne i vidt omfang kan opretholdes, hvilket ikke var klart efter Tele2-dommen. Det skyldes, som uddybet i det følgende, at Danmark aktuelt står over for en sådan alvorlig trussel mod den nationale sikkerhed, som kan begrunde en generel og udifferentieret logning i en begrænset periode, som kan forlænges, hvis truslen fortsat består.

Justitsministeriet har to hovedanbringender til støtte for den nedlagte frifindelsespåstand.

For det første betyder princippet om EU-rettens forrang ikke, at nationale bestemmelser, hvis anvendelse kan stride mod EU-retten, skal erklæres ugyldige. Princippet betyder alene, at sådanne nationale bestemmelser ikke kan anvendes i den nationale retsorden i det omfang, dette ville stride mod EU-retlige regler med direkte virkning og forrang. Justitsministeren har i overensstemmelse hermed allerede tilkendegivet, at teleselskaberne, indtil nye logningsregler er på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke i de gældende danske regler sondres mellem, til hvilke formål oplysningerne logges som forudsat i La Quadrature-dommen.

For det andet giver La Quadrature-dommen mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed. Det betyder, at kun visse dele af logningsbekendtgørelsen skal ændres i lyset af dommen, herunder navnlig dennes § 1, som bestemmer, at oplysningerne skal kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold uden hensyn til, om der er tale om almindelig kriminalitet, grov kriminalitet eller aktiviteter, der truer den nationale sikkerhed. Det skyldes, at Danmark på nuværende tidspunkt står over for en sådan alvorlig trussel mod den nationale sikkerhed, som den, der er nævnt i La Quadrature-dommen, og som må anses for at være reel og aktuel eller forudsigelig. Selv hvis princippet om EU-rettens forrang kunne føre til, at nationale bestemmelser tilsidesættes som ugyldige, så giver La Quadrature-dommen ikke belæg for, at hele logningsbekendtgørelsen er ugyldig, således som sagsøgeren påstår.

De nødvendige ændringer af logningsreguleringen skal ifølge EU-Domstolens praksis gennemføres hurtigst muligt. Eftersom La Quadrature-dommen grundlæggende ændrer de EU-retlige rammer for logning af teleoplysninger, handler den danske stat fortsat hurtigst muligt ved at have iværksat de tiltag, som blev præsenteret på åbent samråd i Folketingets Retsudvalg den 14. januar 2021 med justitsministeren.

2. SUPPLERENDE SAGSFREMSTILLING

2.1 Forløbet siden afgivelse af svarskrift og frem til La Quadrature-dommen

Justitsministeriet orienterede ved notat af 1. oktober 2019 Retsudvalget om, at ministeren ville fremsætte lovforslag i december II om udskydelse af revisionen af logningsreglerne. Notatet fremlægges som **bilag B**. I notatet anføres det bl.a.:

> *"…*
>
> *EU-Domstolen behandler i øjeblikket to sager fra henholdsvis Belgien og Frankrig, der kan give EU-Domstolen anledning til at genoverveje den retstilstand, som Tele2-dommen har medført.*
>
> *De pågældende sager blev mundtligt forhandlet ved EU-Domstolen den 9.- 10. september 2019, hvor en lang række medlemsstater, inklusiv Danmark, afgav indlæg med henblik på, at EU-Domstolen trækker nogle af indskrænkningerne fra Tele2-dommen tilbage. EU-Domstolens afgørelse i sagerne fra Belgien og Frankrig forventes at blive afsagt omkring maj 2020.*

> *Med henblik på at afvente EU-Domstolens kommende dom, hvor Domstolen forhåbentlig genovervejer den retstilstand, som Tele2-dommen har medført, vil jeg i december II fremsætte et lovforslag om udskydelse af revision af logningsreglerne til folketingsåret 2020-21.*
>
> *3. Jeg skal for god ordens skyld oplyse, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen fortsat opretholdes, indtil revisionen af logningsreglerne er gennemført."*

Ved notat af 14. februar 2020 orienterede ministeriet Retsudvalget om regeringens afgivelse af indlæg i EU-Domstolens forenede sager C-793/19 og C-794/19, SpaceNet m.fl. Notatet fremlægges som **bilag C**.

Om de faktiske omstændigheder i sagen fremgår det bl.a.:

> "**2. Sagernes faktiske omstændigheder**
> …
>
> *Forbundsforvaltningsdomstolen anser det ikke for udelukket, at de tyske regler er i overensstemmelse med EU-retten. I den forbindelse har domstolen påpeget, at de tyske regler på området ikke foreskriver lagring af samtlige telekommunikationstrafikdata for alle abonnenter og registrerede brugere, idet eksempelvis kommunikationsindhold, besøgte hjemmesider, data fra e-mailtjenester og data, som er baseret på forbindelser til eller fra bestemte personer, som i henhold til tysk lovgivning er pålagt tavshedspligt, herunder advokater, læger eller journalister, er undtaget fra kravet om logning. Endvidere påpeger domstolen, at lagringsperioden under den tyske lovgivning på henholdsvis fire og ti uger er væsentlig kortere end i Tele2-sagen, hvor lagringsperioden var på seks måneder efter de svenske regler. Domstolen anfører ligeledes, at de tyske regler, som fastsætter pligt til generel lagring af trafikdata, ikke uden videre kan anses for uforenelig med Charteret henset til behovet for at etablere en balance mellem på den ene side medlemsstatens forpligtelse til at sikre den personlige og nationale sikkerhed og på den anden side overholdelsen af de grundlæggende rettigheder."*

Om den danske interesse i sagen anføres det bl.a.:

*"**3. Den danske interesse i sagen***

Det er regeringens opfattelse, at regeringen bør afgive indlæg i disse sager, idet sagerne vedrører EU-medlemsstaternes muligheder for at pålægge teleudbydere at gemme og opbevare oplysninger om tele- og internettrafik (logning) til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

De danske regler om logning skal som konsekvens af EU-Domstolens afgørelse i Tele2-sagen revideres.

Tele2-dommen efterlader imidlertid væsentlig fortolkningstvivl i forhold til, hvordan nationale bestemmelser om logning kan indrettes i overensstemmelse med EU-retten. Der har således siden foråret 2017 løbende været drøftelser i EU-regi om, hvordan medlemsstaterne kan indrette nationale logningsregler i lyset af dommen. Kommissionen tilkendegav, som følge af Tele2-dommen, at Kommissionen ville udarbejde retningslinjer til medlemsstaterne om indretning af logningsregler. Disse retningslinjer er endnu ikke udarbejdet.

Der verserer for tiden en række præjudicielle sager fra andre EU-medlemsstater for EU-Domstolen, som kan få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler.

Danmark og 16 andre EU/EØS-medlemsstater har afgivet indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18 om de franske logningsregler samt i sag C-520/18 om de belgiske logningsregler. I begge sager gjorde regeringen gældende, at Domstolen bør genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen.

Det forventes, at EU-Domstolen vil afsige domme i sagerne i løbet af sommerhalvåret 2020.

…"

Ved notat af 5. august 2020 orienterede ministeriet Retsudvalget om afgivelse af indlæg i endnu en præjudiciel sag om logning af teleoplysninger, nemlig EU-Domstolens sag C-140/20, The Commissioner of the Garda Síochána m.fl. Notatet fremlægges som **bilag D**.

I notatet fremgår det bl.a. om sagens faktiske omstændigheder:

*"**2. Sagens faktiske omstændigheder***

…

Af anmodningen fremgår blandt andet, at formålet er at få præciseret de EU-retlige krav vedrørende lagring af data med henblik på bekæmpelse af grov kriminalitet og de nødvendige sikkerhedsforanstaltninger ved adgang til disse data, henset til en medlemsstats kompetence på det strafferetlige område. I den forbindelse anføres det, at det ikke er muligt at få adgang til data, der ikke er blevet lagret, og at hvis universel lagring af metadata fra telekommunikation ikke var tilladt, uanset hvor robust ordningen for adgang hertil er, ville mange alvorlige forbrydelser ikke blive opklaret eller føre til retsforfølgning.

Sagsøger har bl.a. henvist til dommen i Tele2-sagen (sag C-203/15 og C-698/15). I dommen fastslog EU-Domstolen, at de svenske regler om logning var i strid med direktiv 2002/58, sammenholdt med de grundlæggende rettigheder i EU-Chartret. EU-retten var således til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en pligt til generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation."

Under afsnittet om den danske interesse i sagen gentages det bl.a., at de danske regler om logning som konsekvens af EU-Domstolens afgørelse i Tele2-sagen skal revideres, men at dommen efterlader væsentlig fortolkningstvivl i forhold til, hvordan nationale bestemmelser om logning kan indrettes i overensstemmelse med EU-retten. Om prognoserne for Domstolens dom forlyder det dog nu, at man forventer, at EU-Domstolen vil afsige domme i sagerne i løbet af 2020/2021.

Om regeringens synspunkter i sagen anføres bl.a.:

*"**Regeringens synspunkter i sagen***
Det er overordnet regeringens opfattelse, at EU-Domstolen skal opfordres til at genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen. Der skal i den forbindelse henvises til, at loggede oplysninger udgør et centralt og effektivt redskab for politiet og politiets efterretningstjeneste, som i forhold til efterforskning og strafforfølgning af alvorlig kriminalitet og terror er af afgørende betydning, således som også påpeget af den irske højesteret i forelæggelseskendelsen.

…"

2.2 La Quadrature-dommen

EU-Domstolen afsagde den 6. oktober 2020 dom i *La Quadrature du Net m.fl.* (forenede sager C-511/18, C-512/18 og C-520/18, ECLI:EU:C:2020:791).

EU-Domstolen fastslår i dommen, at national lovgivning, der påbyder teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet, falder ind under anvendelsesområdet for Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (herefter e-data-beskyttelsesdirektivet). Nationale logningsregler skal således være i overensstemmelse med artikel 15, stk. 1, i e-data-beskyttelsesdirektivet sammenholdt med artikel 7 om respekt for privatlivet, artikel 8 om beskyttelse af personoplysninger og artikel 11 om ytringsfrihed i EU's Charter om Grundlæggende Rettigheder (herefter Chartret).

Herefter fastlægger Domstolen for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed (præmis 134ff).

Hensynet til den nationale sikkerhed adskiller sig ifølge Domstolen fra hensynet til bl.a. den offentlige sikkerhed og hensynet til bekæmpelse af grov kriminalitet. Domstolen udtaler i den forbindelse, at det fremgår af artikel 4, stk. 2, TEU, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar. Dette ansvar svarer til den primære interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed, jf. dommens præmis 135.

Hensynet til den nationale sikkerhed vejer ifølge Domstolen tungere end hensynet til bl.a. den offentlige sikkerhed, som også dækker over andre former for alvorlig kriminalitet, såsom narko-, bande- og våbenkriminalitet. Derfor kan hensynet til den nationale sikkerhed også begrunde indgreb i de grundlæggende rettigheder, som er mere alvorlige end dem, som bl.a. hensynet til den offentlige sikkerhed mv. kan begrunde, jf. præmis 136.

Domstolen fastslår herefter i præmis 137 – som noget nyt og centralt for denne sag – at artikel 15 i e-data-beskyttelsesdirektivet sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, *ikke* er til hinder for generel og udifferentieret logning af teleoplysninger, når det sker af hensyn til den nationale sikkerhed. Dette forudsætter, at den berørte medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

Et påbud til teleudbyderne om generel og udifferentieret lagring af teleoplysninger skal tidsmæssigt begrænses til det strengt nødvendige. Forpligtelsen til at foretage generel og udifferentieret logning vil ifølge EU-Domstolen principielt kunne forlænges, hvis truslen mod den nationale sikkerhed fortsat

består. Hver enkelt påbud må ikke overstige et forudseeligt tidsrum. Desuden skal logningen være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug. Logningen må ikke have en systematisk karakter.

2.3 Justitsministeriets opfølgning på dommen

Den 21. oktober 2020 stillede Folketingets Retsudvalg efter ønske fra Rosa Lund spørgsmål til justitsministeren om, hvorvidt det var ministerens opfattelse, at teleselskaber i Danmark var juridisk forpligtet til at logge teledata. Spørgsmålet fremlægges som **bilag E**.

Den 13. november 2020 stillede Folketingets Retsudvalg efter ønske fra Karina Lorentzen Dehnhardt følgende tre spørgsmål til drøftelse i åbent samråd:

> *"Samrådsspørgsmål J*
> *Vil ministeren redegøre for, hvorfor man ikke straks ophører den ulovlige masselogning af danskernes teledata, når EU-Domstolens afgørelse af 6. oktober 2020 præciserer, at reglerne er i strid med EU-retten og ikke kan opretholdes midlertidigt, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?"*

> *"Samrådsspørgsmål K*
> *Vil ministeren redegøre for teleselskabernes retsstilling i forhold til afgørelsen, herunder hvordan ministeren forventer selskaberne kan agere, efter det er fastslået og præciseret, at deres praksis – også midlertidigt – er i strid med EU-retten, men den danske stat pålægger dem at fortsætte denne praksis, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?"*

> *"Samrådsspørgsmål L*
> *Vil ministeren redegøre for, hvorvidt regeringen med det lovforslag, som ifølge ministeren fremsættes i februar 2021, planlægger at ændre reglerne, således at de vil være i overensstemmelse med EU-retten og regler om retten til privatliv, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?"*

De tre samrådsspørgsmål fremlægges som **bilag F-H**.

Den 17. november 2020 stillede Folketingets Retsudvalg efter ønske fra Karina Lorentzen Dehnhardt yderligere fem spørgsmål til skriftlig besvarelse. Spørgsmålene fremlægges som **bilag I-M**.

Den 20. november 2020 oversendte Justitsministeriet et orienteringsnotat vedrørende La Quadrature-dommen fra 6. oktober til Retsudvalget. Samtidig oversendte Justitsministeriet svar på spørgsmål 140.

Af orienteringsnotatet, der fremlægges som **bilag N**, fremgår bl.a.:

> *"4. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.*
>
> *5. Justitsministeriet studerer nu dommen med henblik på at vurdere, i hvilket omfang Danmark vil kunne opretholde de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Det sker med henblik på at kunne præsentere et udkast til revision af de danske regler på området.*
>
> *Det er vigtigt for mig som justitsminister, at politiet og PET har de nødvendige værktøjer for at kunne efterforske og retsforfølge alvorlig kriminalitet og beskytte vores nationale sikkerhed. Her er loggede oplysninger af afgørende betydning."*

I besvarelsen af spørgsmål 140, der fremlægges som **bilag O**, fremgår det bl.a.:

> *"EU-Domstolen afsagde den 6. oktober 2020 dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen vedrører det EUretlige grundlag for at kunne pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet.*
>
> *Justitsministeriet er i øjeblikket i gang med at studere dommen og vurdere dens nærmere konsekvenser for de danske logningsregler.*
>
> *Det bemærkes, at EU-Domstolens dom ikke betyder, at de gældende danske logningsregler sættes ud af kraft. Derfor skal teleudbydere fortsat logge og udlevere oplysninger i overensstemmelse med gældende regler, indtil ny lovgivning måtte være vedtaget og trådt i kraft."*

Den 5. januar 2021 oversendte Justitsministeriet skriftlig besvarelse af spørgsmål 219-223. Besvarelserne med bilag fremlægges som **bilag P-T**. Vedlagt som bilag til besvarelsen af spørgsmål 219 var Justitsministeriets korrespondance med Teleindustrien om La Quadrature-dommen af 6. oktober 2020.

Af besvarelsen af spørgsmål 223, vedrørende hvilke lande, der som konsekvens af EU-Domstolens afgørelser havde tilpasset deres nationale logningsregler, fremgår følgende:

> *"Sverige vedtog på baggrund af Tele2-dommen (EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl.) en ændring af de svenske logningsregler, som trådte i kraft den 1. oktober 2019. De svenske logningsregler indebærer bl.a. en begrænset og differentieret forpligtelse til logning af oplysninger afhængig af typen af data.*
>
> *Justitsministeriet kan herudover henvise til de tidligere svar af lignende spørgsmål i besvarelserne af 19. juni 2018 på spørgsmål nr. 623 og 625 (Alm. del) fra Folketingets Retsudvalg, som uddyber, hvordan en række af de øvrige EU-lande havde indrettet sig efter Tele2-dommen.*
>
> *Justitsministeriet vil til brug for revisionen af de danske logningsregler indhente oplysninger om relevante landes opfølgning på EU-Domstolens dom af 6. oktober 2020 om de franske og belgiske logningsregler (de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.), herunder oplysninger om, i hvilket omfang dommen forventes at føre til ændringer af de pågældende landes logningsregler. Justitsministeriet er påbegyndt en indledende dialog med relevante lande herom.*
>
> *En række medlemsstater har oplyst, at de er ved at studere dommen af 6. oktober 2020 med henblik på at vurdere, i hvilket omfang nationale regler skal tilpasses."*

Den 14. januar 2021 kl. 10.15 afholdtes åbent samråd i Folketingets Retsudvalg om logningsbekendtgørelsen. Justitsministerens talepapir fra samrådet fremlægges som **bilag U**. Under besvarelsen af samrådsspørgsmål L om planerne for at ændre reglerne fremgår bl.a. følgende:

> *"Som sagt skal vi finde den rette balance mellem de forskellige hensyn. Og finde den rette løsning. Det tager tid.*
>
> *Regeringen forventer derfor først at kunne fremsætte et lovforslag, der materielt ændrer logningsreglerne, i åbningsugen i den kommende folketingssamling.*
>
> *Det lovforslag, der vil blive fremsat i indeværende samling, vil altså være et forslag om at udskyde revisionen.*

> *Men det betyder på ingen måde, at regeringen bare vil læne sig tilbage indtil næste folketingsår.*
>
> *Samtidig med fremsættelsen af lovforslaget om udskydelse af revisionen vil jeg fremlægge en skitse til det kommende lovforslag om den materielle ændring af reglerne.*
>
> *Det gør jeg for at lægge op til en åben drøftelse med bl.a. Folketingets partier, telebranchen og andre interessenter.*
>
> *Jeg vil gerne tage debatten åbent og på et tidligt stadie. Så vi finder den rette løsning og sikrer, at politiet fortsat kan bruge loggede oplysninger i videst muligt omfang."*

Under det åbne samråd spurgte Karina Lorentzen Dehnhardt bl.a. fra ca. kl. 10:33:20 og frem, hvad grundlaget var for at opretholde logningen midlertidigt frem til vedtagelsen af reviderede regler:

> *"Jeg vil rigtig gerne høre – fordi sådan som jeg forstår dommen og læser dommen og også – der er flere, der har hjulpet mig med at læse dommen – så siger den faktisk, at vi kan ikke opretholde logningen – heller ikke midlertidigt. Ministeren siger, at det er ikke i strid med EU-retten at fortsætte til efteråret, men er det ikke korrekt forstået, at man kan faktisk ikke opretholde logning midlertidigt? Og som jeg lytter mig frem til det, ministeren siger, så er der faktisk heller ikke en hjemmel til at pålægge teleselskaberne at fortsætte med logningen. Så hvis de vælger at sige, "i morgen ophører vi, fordi nu er den her dom faldet", så kan vi sådan set ikke pålægge dem det? Og det synes jeg jo er lidt i strid med den melding, som ministeren tidligere har givet til selskaberne om, at de skal fortsætte med det her. Men kan ministeren bekræfte, at der er sådan set ikke en hjemmel i lovgivningen til at sige, at de skal fortsætte med det her? Så hvis de vælger at ophøre, så kan vi sådan set ikke gøre noget ved det."*

Justitsministeren besvarede dette spørgsmål fra ca. kl. 10:39:50 og frem:

> *"Så var der det konkrete spørgsmål, om man kan opretholde logningen midlertidigt. Hvordan er teleselskabernes retsstilling egentlig. EU-Domstolens dom – det var også det, jeg prøvede på at sige med at implementere det hurtigst muligt – EU-Domstolens dom betyder ikke, at de gældende danske logningsregler sættes ud af kraft. Og det som jeg også sagde i talen, det var, at jeg håber på teleselskabernes forståelse for, at politiet og politiets efterretningstjeneste har behov for adgang til loggede oplysninger til at bekæmpe grov kriminalitet og til at beskytte den nationale sikkerhed, som jo er det, der ligger inden for rammerne i dommen.*

> *Men også jo, som jeg også sagde, at visse dele af de danske logningsregler strider mod EU-retten […] mod EU-Charteret, sådan som det fortolkes af EU-Domstolen. Og derfor kan det ikke håndhæves over for teleudbyderne. Altså de dele, som strider mod EU-retten – de dele af den danske lovgivning, som strider mod EU-retten, kan vi ikke håndhæve over for teleudbyderne. Og derfor vil teleudbyderne heller ikke kunne straffes, hvis de undlader at logge teleoplysninger."*

Den 21. januar 2021 stillede Karina Lorentzen Dehnhardt yderligere fem spørgsmål til skriftlig besvarelse vedrørende logningsreglerne. Spørgsmålene fremlægges som **bilag V-Z**.

Den 29. januar 2021 oversendte Justitsministeriet til Retsudvalgets orientering et udkast til lovforslag om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af revisionsbestemmelse). Udkastet til lovforslag fremlægges som **bilag Æ**. Udkastet blev samme dag sendt i høring hos en række myndigheder og organisationer.

I de almindelige bemærkninger i lovforslaget fremgår bl.a. følgende:

> *"EU-Domstolen har den 6. oktober 2020 afsagt dom i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af grov kriminalitet og terror. Der henvises til notat af 19. november 2020, som er sendt til Folketingets Retsudvalg og Folketingets Europaudvalg (EUU Alm. del – bilag 101).*
>
> *I dommen af 6. oktober 2020 indgår en række nye elementer. Selvom EU-Domstolen gentager udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse, så fastslår EU-Domstolen samtidig under hvilke betingelser og i hvilke situationer, udgangspunktet kan fraviges. Det gælder bl.a. logning med henblik på beskyttelse af den nationale sikkerhed.*
>
> *Det er Justitsministeriets vurdering, at der på baggrund af dommen af 6. oktober 2020 er behov for at ændre i de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Endvidere vurderes det nødvendigt at ændre reglerne om adgang til loggede oplysninger, herunder retsplejelovens bestemmelser om edition, indgreb i meddelelseshemmeligheden mv.*

Det er fortsat Justitsministeriets vurdering, at udformningen af de nye logningsregler bør ske på et fuldt oplyst grundlag, og at rækkevidden af dommen af 6. oktober 2020 bør fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Dette vil sikre, at de nye regler holdes inden for EU-rettens rammer. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen i Danmark ikke pålægges unødige byrder. Justitsministeriet er derfor i tæt dialog med de øvrige medlemsstater, om hvordan dommen skal fortolkes. Regeringen forventer at kunne præsentere en skitse til revision af de danske regler på området i løbet af foråret 2021. Som følge heraf foreslås det at udskyde revisionen af logningsreglerne til folketingsåret 2021-22."

Den 17. februar 2021 oversendte Justitsministeriet besvarelsen af de fem spørgsmål stillet af Karina Lorentzen Denhardt den 21. januar 2021. Besvarelserne fremlægges som **bilag Ø-AC**.

I svaret på spørgsmål 562 angående håndhævelsen af logningsbekendtgørelsen og princippet om EU-rettens forrang fremgår bl.a.:

*"**3.** EU-Domstolens dom af 6. oktober 2020 indebærer ikke, at de gældende danske logningsregler sættes ud af kraft eller bliver umiddelbart ugyldige.*

Det er imidlertid Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter dommen af 6. oktober 2020 ikke vil kunne begrundes af hensyn til bekæmpelsen af almindelig kriminalitet.

Da de gældende logningsregler pålægger teleselskaberne at registrere og opbevare oplysninger om teletrafik til brug for efterforskning af alle strafbare forhold, er det således Justitsministeriets opfattelse, at teleselskaberne, indtil nye logningsregler er på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke i de gældende danske regler sondres mellem, til hvilke formål oplysningerne logges.

Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og beskytte den nationale sikkerhed, skal ses i dette lys.

…

2.4 Vurdering af terrortruslen mod Danmark

Center for Terroranalyse (CTA) offentliggør i udgangspunktet hvert år en vurdering af terrortruslen mod Danmark. CTA er et fusionscenter, hvis medarbejdere stammer fra Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste, Udenrigsministeriet, Beredskabsstyrelsen og Rigspolitiets Nationale Efterforskningscenter.

CTA's vurdering af terrortruslen mod Danmark fra 1. marts 2020 fremlægges som **bilag AD**.

Som det fremgår af vurderingens side 5, vurderer CTA, at terrortruslen mod Danmark fortsat er "*alvorlig*", dvs. det næsthøjeste niveau af fem niveauer. Det betyder i henhold til CTA's definitioner, at der er en erkendt trussel, og der er kapacitet, hensigt og planlægning.

Den væsentligste trussel er militante islamister og udgår fra sympatisører af Islamisk Stat (IS). Truslen har generelt været faldende siden 2017, hvilket også afspejler sig i angrebsstatistikken, som er tæt på niveauet før IS' etablering af "kalifatet" i Syrien og Irak. Trods den generelle forbedring er det dog fortsat CTA's vurdering, at der er personer i Danmark og i udlandet, herunder i Danmarks nabolande, der har sympati for militant islamisme, og som kan udgøre en terrortrussel mod Danmark. Truslen er derfor fortsat i sig selv "*alvorlig*". Det illustreres ifølge vurderingen bl.a. af den koordinerede anholdelsesaktion, som PET i samarbejde med relevante politikredse gennemførte den 11. december 2019, og som førte til varetægtsfængsling af syv personer for mistanke om overtrædelse af straffelovens § 114.

Ud over truslen fra militante islamister, der altså vurderes som "alvorlig", er terrortruslen fra højreekstremister hævet fra "*begrænset*" til "*generel*", hvilket betyder, at der er kapacitet og/eller hensigt og mulig planlægning. Denne trussel ses ifølge vurderingen bl.a. ved, at der siden foråret 2019 har været en række højreekstremistiske terrorangreb i Vesten udført af soloaktører, hvis radikaliseringsproces primært er foregået på online-fora, herunder et omfattende angreb i marts 2019 i Christchurch, New Zealand, der bidrog til at inspirere til efterfølgende højreekstremistiske angreb udført af soloaktører i bl.a. USA, Norge og Tyskland.

Justitsministeren har senest den 11. februar 2021 udtalt, at terrortruslen mod Danmark fortsat er alvorlig, bl.a. på baggrund af en større antiterroraktion i Holbæk mv. med i alt 13 anholdte.

Materialet fra svarskriftet fremlægges som **bilag AE-AK**.

3. ANBRINGENDER

3.1 La Quadrature-dommen er ikke en stadfæstelse af Tele2-dommen

Der er på ingen måde tale om, at Domstolen i La Quadrature-dommen blot "*stadfæstede, hvad der allerede var blevet afgjort*" i Tele2-dommen og Digital Rights-dommen, som anført af sagsøgeren på side 3 i replikken, eller at Domstolen alene "*nuancerede enkelte problemstillinger*", som det anføres på side 10.

I forhold til det spørgsmål, som er helt centralt for denne sag, nemlig muligheden for at opretholde eller indføre en generel og udifferentieret forpligtelse til at logge teleoplysninger, indebærer La Quadrature-dommen en markant og relevant videreudvikling af Tele2-dommen.

Dommen fastslår for første gang, at det under visse omstændigheder *er* muligt at opretholde generel og udifferentieret logning af hensyn til den nationale sikkerhed i en tidsbegrænset periode. Hverken Tele2-dommen eller Digital Rights-dommen tog stilling til, i hvilket omfang hensyn til den nationale sikkerhed kunne begrunde regler om logning af teleoplysninger.

Hensynet til den nationale sikkerhed vejer ifølge Domstolen tungere end hensynet til bl.a. den offentlige sikkerhed, som også dækker over andre former for alvorlig kriminalitet, såsom narko-, bande- og våbenkriminalitet. Derfor kan hensynet til den nationale sikkerhed også begrunde indgreb i de grundlæggende rettigheder, som er mere alvorlige end dem, som bl.a. hensynet til den offentlige sikkerhed mv. kan begrunde, jf. præmis 136.

Det betyder konkret, at hensynet til den nationale sikkerhed principielt *kan* begrunde et indgreb i form af generel og udifferentieret logning af teleoplysninger.

Dommen nødvendiggør ændringer af de danske bestemmelser om logning af teleoplysninger, idet teleoplysninger bl.a. efter gældende ret skal logges, så de kan anvendes til brug for efterforskning af al kriminalitet, herunder almindelig kriminalitet. Disse ændringer er dog væsentligt anderledes end den målretning af logningsforpligtelsen, som størstedelen af udredningsarbejdet efter Tele2-dommen har handlet om.

3.2 Princippet om EU-rettens forrang fører ikke til, at logningsbekendtgørelsen er hverken helt eller delvist ugyldig

Sagsøgerens påstand går ud på, at logningsbekendtgørelsen skal tilsidesættes som ugyldig. Påstanden støttes på, at bekendtgørelsen strider mod artikel 15, stk. 1, i e-data-beskyttelsesdirektivet sammenholdt med artikel 7, 8 og 11 i Chartret.

Det bestrides, at en eventuel modstrid mellem bekendtgørelsen og EU-retten kan føre til, at bekendtgørelsen som helhed er ugyldig, således som sagsøgeren påstår.

Princippet om EU-rettens forrang betyder, at nationale domstole og retsanvendende myndigheder skal *undlade at anvende* enhver bestemmelse i national lov, der strider mod EU-retten, jf. bl.a. Domstolens dom af 24. juni 2019 i *Popławski* (sag C-573/17, ECLI:EU:C:2019:530), præmis 58, dom af 9. marts 1978 i *Simmenthal* (sag C-106/77, ECLI:EU:C:1978:49), præmis 21 og 24, og dom af 4. juni 1992 i *Debus* (sag C-13/91, ECLI:EU:C:1992:247), præmis 31-33.

Princippet betyder derimod *ikke*, at en modstridende national regel bliver ugyldig eller i det hele ikke længere kan anses for at eksistere, jf. Domstolens dom af 22. oktober 1998 i *IN.CO.GE 90* (forenede sager C-10/97 - C-22/97, ECLI:EU:C:1998:498), præmis 21 og dom af 3. maj 2005 i *Berlusconi* (forenede sager C-387/02, C-391/02 og C-403/02, ECLI:EU:C:2005:270), præmis 72, Alan Dashwood og Derrick Wyatts "*European Union Law*", 6. udgave (2011), s. 270-271, Paul Craig og Gráinne de Búrcas "*EU Law Text, cases, and materials*", 6. udgave (2015), s. 272-273, og Birgitte Egelund Olsen i "*EU-retten i Danmark*", 1. udgave (2018), side 405.

I en situation, hvor anvendelsen af en national bestemmelse kan føre til uoverensstemmelser med EU-retten, påhviler det de retsanvendende myndigheder at vurdere i hver enkelt konkrete situation, om en sådan uoverensstemmelse vil foreligge. Hvis der konstateres en uoverensstemmelse, skal de retsanvendende myndigheder undlade at anvende den nationale bestemmelse i det konkrete tilfælde, og kun i det omfang det er nødvendigt for at fjerne uoverensstemmelsen med EU-retten, jf. Domstolens dom af 24. oktober 1996 i *Kraaijeveld* (sag C-72/95, ECLI:EU:C:1996:404).

Kraaijeveld-dommen vedrørte en nederlandsk lov og tilhørende bekendtgørelse, som indebar en fritagelse for krav om forudgående miljøvurdering for projekter angående bygning af diger på mindre end 5 kilometer i længden og med en tværprofil på mindre end 250 m^2. Virksomheden Kraaijeveld havde anfægtet en dispositionsplan vedtaget af kommunalbestyrelsen i Sliedrecht og godkendt af Zuid-Hollands provinsregering. De ved dispositionsplanen vedtagne ombygninger af diget ved Merwede betød bl.a., at Kraaijeveld ikke længere ville have adgang til sejlbare vandveje, hvilket skadede dens virksomhed. Under sagen opstod der bl.a. spørgsmål om, hvorvidt det var berettiget, at der ikke var gennemført en undersøgelse af projektets indvirkning på miljøet forud for vedtagelsen af planen.

I henhold til artikel 2 i det dagældende direktiv 85/337/EØF af 27. juni 1985 om vurdering af visse offentlige og private projekters indvirkning på miljøet skulle medlemsstaterne træffe de nødvendige foranstaltninger med henblik på, at projekter, der bl.a. på grund af deres art, dimensioner eller placering kunne få væsentlig indvirkning på miljøet, blev undergivet en vurdering af denne indvirkning, inden der blev givet

tilladelse til projekterne. Ifølge direktivets artikel 4, stk. 2, kunne medlemsstaterne fastsætte kriterier og/eller grænseværdier for bestemte typer af projekter – herunder bl.a. "Anlæg til regulering af vandløb", jf. direktivets bilag II, pkt. e) – for at afgøre, om de skulle undergives en miljøvurdering efter direktivet.

Et af spørgsmålene for Domstolen var, om de føromtalte fastsatte grænseværdier for bygning af diger var i overensstemmelse med direktivets artikel 2 og artikel 4, stk. 2, og hvad konsekvenserne af en eventuel uoverensstemmelse ville være.

Domstolen udtalte i præmis 43-53 bl.a., at bestemmelsen i direktivets artikel 4, stk. 2, sammenholdt med artikel 2, overlod medlemsstaterne et vist skøn, og at Nederlandene havde ret til at fastsætte kriterier for digernes størrelse til brug for afgørelsen af, hvilke projekter vedrørende diger, der skulle være genstand for en undersøgelse af indvirkningerne på miljøet. Spørgsmålet om, hvorvidt Nederlandene ved at fastsætte disse kriterier havde overskredet grænserne for sit skøn, kunne ikke afgøres på grundlag af et enkelt projekts kendetegn. Det måtte i stedet afhænge af en samlet bedømmelse af kendetegnene ved de projekter af denne art, der kunne imødeses på medlemsstatens område.

I præmis 54-61 tog Domstolen stilling til betydningen af en eventuel tilsidesættelse af direktivet i konkrete sager. Domstolen udtalte, at det påhvilede den nationale domstol at undersøge inden for rammerne af sin kompetence, om medlemsstatens lovgivende eller udøvende myndigheder havde holdt sig inden for grænserne af det skøn, der er fastsat i direktivets artikel 2, stk. 1, og artikel 4, stk. 2, og at tage hensyn hertil under behandlingen af annullationssøgsmålet. Hvis grænserne for skønnet var overskredet, således at et projekt var blevet undtaget for miljøvurdering i strid med direktivet, måtte der ses bort fra den nationale undtagelsesbestemmelse, og myndighederne måtte herefter inden for deres kompetence træffe alle de almindelige eller særlige foranstaltninger, der er nødvendige for at projekterne undersøges med henblik på at fastslå, om de kan få væsentlig indvirkning på miljøet, og i bekræftende fald, at deres indvirkninger undersøges.

Kraaijeveld-dommen vedrørte på samme måde som denne sag en national lovgivning, hvis anvendelse i visse tilfælde kunne stride mod EU-retten. Dommen viser, at konsekvensen af en sådan potentiel modstrid ikke er, at hele loven eller konkrete nationale retsregler tilsidesættes som ugyldig. Konsekvensen er i stedet, at nationale domstole og myndigheder skal se bort fra den nationale lovgivning og undlade at anvende den, hvis en sådan anvendelse konkret vil føre til konsekvenser, der er uforenelige med EU-retten.

Denne konsekvens af en konflikt mellem en EU-retsregel, der har direkte virkning og forrang, og en national retsregel er almindeligt anerkendt, jf. også EU-institutionernes egen opsummering af forrangsprincippet på EUR-Lex: EUR-Lex - l14548 - EN - EUR-Lex (europa.eu):

> *"Hvis en national lovregel er i modstrid med en EU-bestemmelse, skal medlemsstaternes myndigheder altså anvende EU-bestemmelsen. Den nationale ret er hverken annulleret eller afskaffet, men dens forpligtende kraft er ophævet."* (Understreget her)

I overensstemmelse hermed tilkendegav justitsministeren på åbent samråd med Folketingets Retsudvalg den 14. januar 2020, at teleudbyderne som følge af dommen ikke ville kunne straffes for manglende overholdelse af logningsbekendtgørelsen. Ministeren har med denne erklæring om de manglende muligheder for at håndhæve dele af logningsreglerne gjort det klart, at logningsbekendtgørelsens bestemmelser ikke vil blive anvendt på en måde, der kan stride mod EU-retten. Dermed har ministeriet bidraget til at overholde de EU-retlige forpligtelser, der kan udledes af EU-Domstolens retspraksis. Principperne om EU-rettens forrang og direkte virkninger kræver ikke derudover, at danske retsanvendende myndigheder erklærer nationale retsregler, der strider mod EU-retlige regler, ugyldige eller ophæver sådanne retsregler. Allerede af denne grund skal Justitsministeriet frifindes for sagsøgerens påstand.

Sammenfattende gøres det gældende, at sagsøgerne ikke kan få medhold i deres påstand på grundlag af princippet om EU-rettens forrang.

3.3 Justitsministeriet handler fortsat hurtigst muligt for at bringe dansk ret i overensstemmelse med EU-retten

Som også anført i svarskriftet følger det af EU-Domstolens praksis, at en ændring af nationale regler for at bringe disse i overensstemmelse med EU-retten, som fortolket af EU-Domstolen, skal ske så hurtigt som muligt, jf. EU-Domstolens dom af 21. juni 2007 i *Jonkman* (forenede sager C-231/06 - C-233/06, ECLI:EU:C:2007:373). Der kan også henvises til Højesterets dom af 19. januar 2017 i sag 42/2016 (UfR 2017.1243 H). Det vil i lyset heraf afhænge af den enkelte sags omstændigheder, hvor hurtigt en tilpasning skal foretages. Der vil i den forbindelse bl.a. kunne tages hensyn til, hvor teknisk vanskelige ændringer der er tale om, og hvor store økonomiske konsekvenser, ændringerne vil kunne medføre for de virksomheder, der skal indrette sig efter de tilrettede regler.

Det gøres gældende, at Justitsministeriet har iagttaget – og fortsat iagttager – alle relevante forpligtelser, der følger af konstateringen af, at logningsbekendtgørelsen skal revideres i lyset af EU-Domstolens retspraksis.

Justitsministeriet har handlet – og handler fortsat – så hurtigt som muligt i lyset af de væsentlige udfordringer forbundet med revisionen for at bringe logningsbekendtgørelsen i overensstemmelse med EU-retten. Ændringerne af logningsreglerne kræver grundige juridiske og tekniske overvejelser. Der er tale om teknisk vanskelige ændringer, som alt afhængig af udformning kan medføre store økonomiske konsekvenser for teleudbyderne mv. Endvidere bør rækkevidden af dommen af 6. oktober 2020, der som nævnt

ovenfor indeholder nye elementer, efter Justitsministeriets opfattelse så vidt muligt fastlægges i fællesskab med de øvrige EU-lande og Kommissionen.

Det er ikke korrekt som anført af sagsøgeren i pkt. 3.2.2 i replikken, at Justitsministeriet ikke har iværksat tiltag som reaktion på La Quadrature-dommen.

Som anført af justitsministeren på åbent samråd den 14. januar 2021, og som det fremgår af udkast til lovforslag om revision af retsplejeloven m.m. sendt i høring den 29. januar 2021, har Justitsministeriet igangsat en proces for revision af logningsreglerne, der skal munde ud i fremsættelsen af et lovforslag til oktober 2021. For at fremskynde forhandlingerne om lovforslaget forventer regeringen desuden ekstraordinært at præsentere en skitse til lovforslaget allerede i foråret 2021. Samtidig arbejder Justitsministeriet tæt sammen med Kommissionen og de øvrige EU-medlemslande for i fællesskab at fastlægge rækkevidden af Domstolens dom af 6. oktober 2020 med henblik på at sikre, at de kommende regler implementerer dommen korrekt.

Forpligtelsen til hurtigst muligt at bringe national ret i overensstemmelse med EU-retten skal ses i lyset af, hvor klar EU-retten er, og hvor vanskeligt det er at tilpasse national ret.

I denne sag har der i en længere periode været betydelig uklarhed om rækkevidden af de EU-retlige forpligtelser, ligesom der har været betydelige vanskeligheder med at tilpasse national ret til Domstolens retspraksis.

Dette bekræftes navnlig af en række præjudicielle forelæggelser om retsstillingen og af, at La Quadrature-dommen blev afsagt efter et ekstraordinært forløb, hvor bl.a. 15 medlemsstater afgav indlæg og samstemmende – og det gjaldt også Kommissionen – anmodede Domstolen om at genoverveje sin praksis, jf. afsnit 2.1 ovenfor. Dommen har bl.a. ført til væsentlige modifikationer af den hidtidige retspraksis, herunder Tele2-dommen.

Eftersom La Quadrature-dommen væsentligt præciserer Tele2-dommen og faktisk tillader generel og udifferentieret logning under visse betingelser, har ministeriet for det første ikke overtrådt nogen handlepligt forud for domsafsigelsen i La Quadrature-dommen, hvor der helt åbenbart var et behov for, at EU-Domstolen yderligere afklarede retsstillingen, inden Tele 2-dommen kunne implementeres fuldt ud.

For det andet har ministeriet ikke overtrådt nogen handlepligt i perioden fra den 6. oktober 2020, hvor Domstolen afsagde dom i La Quadrature-sagen. Efter dommen står det klart, at det er nødvendigt at afklare både hvordan, logning kan målrettes, og i hvilket omfang en generel logningsforpligtelse kan opretholdes. Det gælder så meget desto mere, eftersom Danmark aktuelt befinder sig i en situation med

en alvorlig trussel mod den nationale sikkerhed, der potentielt kan begrunde en opretholdelse af en forpligtelse til generel og udifferentieret logning, jf. nærmere nedenfor.

I den forbindelse gøres der opmærksom på, at ingen af de 15 medlemsstater, der afgav indlæg i La Quadrature-dommen, har ændret deres nationale regler som følge af dommen. Det gælder også Frankrig og Belgien, som dommen af 6. oktober 2020 retter sig mod. Disse lande har således senest i februar 2021 oplyst til Justitsministeriet, at de hverken har suspenderet deres gældende regler eller fremsat forslag til revision af deres gældende regler.

Endelig gøres det gældende, at en tilsidesættelse af forpligtelsen til at handle hurtigst muligt under alle omstændigheder alligevel ikke ville føre til, at de pågældende nationale regler mistede deres gyldighed og skulle ophæves, sådan som sagsøgerne påstår. En tilsidesættelse af denne forpligtelse vil i stedet kunne medføre, at Danmark risikerer at blive dømt i en traktatbrudssag, eller at danske myndigheder ifalder et erstatningsansvar som følge af brud på EU-retten, jf. den førnævnte dom i UfR 2017.1243 H. Sagsøgeren kan derimod ikke få medhold i den nedlagte påstand om ugyldighed, selv hvis det kunne påvises, at forpligtelsen ikke var iagttaget.

3.4 Danmark står over for en alvorlig trussel mod den nationale sikkerhed, der muliggør generel og udifferentieret logning efter La Quadrature-dommen, ligesom det vil være muligt at fortsætte logning af IP-adresser med henblik på bekæmpelse af grov kriminalitet mv.

Som omtalt ovenfor har Justitsministeriet besluttet at indstille håndhævelsen af logningsforpligtelsen over for teleudbyderne. Teleudbyderne vil således ikke kunne straffes for manglende overholdelse af logningsbekendtgørelsen. Det fastholdes som anført ovenfor i afsnit 3.2, at Justitsministeriet herved fuldt ud respekterer princippet om EU-rettens forrang, idet man helt har afstået fra at håndhæve selv de dele af forpligtelsen, som principielt kunne opretholdes, uden at det ville være i strid med EU-retten.

Hvis landsretten på trods af det anførte i afsnit 3.2 måtte finde, at EU-rettens forrang i den danske retsorden principielt kan føre til logningsbekendtgørelsens ugyldighed, gøres det gældende, at gyldigheden skal bedømmes i lyset af, at Danmark faktisk aktuelt befinder sig i en situation, hvor en generel og udifferentieret logning i overensstemmelse med logningsbekendtgørelsens kapitel 2 principielt kunne opretholdes under visse betingelser.

Den omstændighed, at visse dele af bekendtgørelsen skal ændres for at leve op til La Quadrature-dommen, betyder ikke, at hele bekendtgørelsen kan tilsidesættes som ugyldig.

De nødvendige tilpasninger vil bl.a. angå bekendtgørelsens § 1, som bestemmer, at oplysningerne skal kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold uden hensyn til, om der er tale om almindelig kriminalitet, grov kriminalitet eller aktiviteter, der truer den nationale sikkerhed. Derudover vil forpligtelsen skulle tidsbegrænses i overensstemmelse med La Quadrature-dommens præmis 138.

Dommen giver dog intet belæg for at antage, at bestemmelserne i bekendtgørelsens kapitel 2 på nuværende tidspunkt ikke kan opretholdes – tværtimod.

Det gøres gældende, at der aktuelt består en trussel mod den nationale sikkerhed i Danmark, der kan betegnes som alvorlig, reel og aktuel, og som dermed kan begrunde opretholdelsen af en forpligtelse til generel og udifferentieret lagring af teleoplysninger i overensstemmelse med La Quadrature-dommens præmis 137.

Ifølge CTA's vurdering af terrortruslen mod Danmark fra marts 2020 er den overordnede terrortrussel netop "*alvorlig*", hvilket betyder, at truslen er erkendt, og at der er både kapacitet, hensigt og aktuel planlægning. Der er intet grundlag for at tilsidesætte denne vurdering. Dette opfylder kriterierne i præmis 137.

Det gøres videre gældende, at de nugældende regler principielt opfylder kravene i dommens præmis 138 om strenge garantier, der gør det muligt effektivt at beskytte de berørte personers personoplysninger mod risikoen for misbrug. Adgangen til teleoplysninger er bl.a. efter retsplejelovens kapitel 74 sammenholdt med kapitel 71 underlagt et proportionalitetskriterie samt krav om dommerkendelse.

Endelig bemærkes, at logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelsen nr. 660 af 19. juni 2014, som bl.a. bestemmer, at en udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere den tildelte brugeridentitet (herunder IP-adresser) samt navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet, kan opretholdes inden for rammerne af La Quadrature-dommen.

En generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse,, er ifølge dommens præmis 155 principielt ikke i strid med artikel 15 i e-databeskyttelsesdirektivet sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, under forudsætning af, at denne mulighed er betinget af en streng overholdelse af de materielle og proceduremæssige betingelser, der skal gælde for brugen af disse data. Et sådan indgreb vil efter dommens præmis 156 kunne begrundes med henblik på bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed (i lighed med beskyttelsen af den nationale sikkerhed). Domstolen opstiller i den forbindelse ikke – på

samme måde som ved national sikkerhed – kriterier for, hvornår der foreligger en sådan situation med grov kriminalitet mv., at en generel og udifferentieret logning kan begrundes. Det afgørende må derfor være, at den tilstrækkelige begrundelse for indgrebet sikres ved opstilling af materielle betingelser for politiets *adgang* til loggede oplysninger om IP-adresser. Den gældende bestemmelse i logningsbekendtgørelsen § 5, stk. 1, må derfor antages at kunne opretholdes inden for rammerne af La Quadrature-dommen.

Justitsministeriet gør derfor sammenfattende gældende, at der ikke aktuelt er noget konkret grundlag for at tilsidesætte logningsbekendtgørelsen som ugyldig i sin helhed, selv hvis dette principielt i dansk ret kunne være en konsekvens af, at en EU-retlig regel med direkte virkning og forrang strider mod dansk ret.

3.5 Øvrige forhold

Sagsøgerne omtaler i afsnit 3.2.1 i replikken, at det ville have været nærliggende at revidere logningsbekendtgørelsen i forbindelse med revisionen af teleloven (lovbekendtgørelse nr. 128 af 7. februar 2014) i efteråret 2020.

Det fremgår ikke, hvilken betydning dette synspunkt ifølge sagsøgeren konkret skulle have for gyldigheden af logningsbekendtgørelsen. Under alle omstændigheder bemærkes det, at forpligtelsen for teleudbydere til på begæring af politiet at udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester, som indgik i § 13 i lovforslaget, ikke begrænses af La Quadrature-dommen.

Disse identifikationsoplysninger består af såkaldte International Mobile Equipment Identity-numre (IMEI-numre) og bruges udelukkende til at identificere en sammenhæng mellem en fysisk person og en kommunikationsenhed. Oplysningerne, der ville kunne udleveres efter den foreslåede § 13 i lovforslaget, identificerer ikke, hvornår, med hvem, hvor længe eller hvordan en slutbruger har kommunikeret, eller hvor slutbrugeren har befundet sig på et givet tidspunkt.

EU-Domstolen har udtalt i dom af 2. oktober 2018 i *Ministerio Fiscal* (sag C-207/16, ECLI:EU:C:2018:788), at adgangen til sådanne data alene ikke i sig selv kan karakteriseres som et "alvorligt" indgreb i de grundlæggende rettigheder, der er fastslået i Chartrets artikel 7 og 8, og at denne adgang derfor ikke er underlagt samme kriterier som fastslået i bl.a. Tele2-sagen. Det betyder, at adgangen til disse oplysninger ikke er begrænset til efterforskning mv. af grov kriminalitet, men også gælder for almindelig kriminalitet. Det bekræftes ligeledes af Domstolen i La Quadrature-dommens præmisser 157-159 vedrørende oplysninger om identiteten på brugere af elektroniske kommunikationsmidler.

Sagsøgeren redegør endelig i afsnit 3.3 for det, man betegner som "teleskandalerne", og anfører, at disse er *"eksempler på de risici, der er forbundet med at have lagret og adgang til omfattende metadata, hvor selv en tilsyneladende effektiv proces omkring krav om retskendelse ikke udgør tilstrækkelige garantier til at sikre de berørte personers personoplysninger mod risiko for misbrug."*

Det bestrides, at "Telenor-sagen" på nogen måde er et relevant eksempel på noget problematisk i selve forpligtelsen til at logge oplysningerne.

Den risiko for "*misbrug*", som Domstolen omtaler i Tele2-dommen og La Quadrature-dommen, har intet at gøre med en risiko for, at oplysningerne er fejlbehæftede. Domstolen beskæftiger sig udelukkende med risikoen for uretmæssig adgang til oplysningerne og brug af dem til fordækte formål såsom profilering, politisk undertrykkelse og personforfølgelse, jf. Tele2-dommens præmis 99 sammenholdt med pkt. 257-260 i Generaladvokatens forslag til afgørelse i samme sag, hvoraf fremgår:

> *"257. Lad os for det første antage, at en person med adgang til de lagrede data har til hensigt at identificere alle de personer i en medlemsstats befolkning, der lider af psykiske vanskeligheder. En analyse af indholdet af al kommunikation foretaget på det nationale område med dette formål ville kræve betydelige ressourcer. Udnyttelsen af databaser vedrørende kommunikation ville derimod gøre det muligt straks at identificere alle de personer, som har kontaktet en psykolog inden for datalagringsperioden. Det tilføjes, at denne teknik kan udstrækkes til at omfatte ethvert lægeligt specialområde, der er registreret i en medlemsstat.*
>
> *258. Lad os for det andet antage, at samme person ønsker at identificere alle de personer, der er imod den siddende regerings politik. Igen ville en analyse af indholdet af al kommunikation foretaget på det nationale område med dette formål kræve betydelige ressourcer. Udnyttelsen af databaser vedrørende kommunikation ville derimod gøre det muligt straks at identificere alle de personer, som har tilmeldt sig mailinglister, der er kritiske over for regeringens politik. Disse data ville desuden også gøre det muligt at identificere de personer, som deltager i offentlige demonstrationer mod regeringen.*
>
> *259. Jeg ønsker at fremhæve, at de risici, der er forbundet med adgangen til kommunikationsdata (eller »metadata«), kan være tilsvarende, eller endog større end, de risici, der følger af adgangen til disse kommunikationers indhold, således som Open Rights Group, Privacy International og Law Society of England and Wales samt en nylig rapport fra FN's Højkommissariat for Menneskerettigheder (86) har fremhævet. Som ovennævnte eksempler viser, gør »metadata« det navnlig muligt nærmest øjeblikkeligt at katalogisere en*

befolkning i sin helhed, hvilket ikke er muligt på baggrund af kommunikationernes indhold.

260. *Det skal hertil tilføjes, at risikoen for ulovlig adgang til lagrede data eller misbrug heraf absolut ikke er af teoretisk art. Dels skal risikoen for, at de kompetente myndigheder misbruger adgangen, sættes i forhold til det enorme antal adgangsanmodninger, som er blevet nævnt i de indlæg, der er indgivet for Domstolen. Hvad angår den svenske ordning har Tele2 Sverige oplyst, at selskabet modtager ca. 10 000 adgangsanmodninger om måneden, og dette antal omfatter ikke de anmodninger, der modtages af andre udbydere på det svenske område. Hvad angår Det Forenede Kongeriges ordning har Tom Watson gengivet tal fra en officiel rapport, som nævner 517 236 tilladelser og 55 346 mundtlige hastetilladelser alene for 2014. Dels udgør risikoen for personers ulovlige adgang en uadskillelig bestanddel af selve eksistensen af en database for lagrede data på databærende medier."*

Der er ingen støtte for, at eventuelle fejl i oplysningerne kan indgå som et relevant moment, når det skal vurderes, om selve forpligtelsen til at lagre teleoplysninger er i overensstemmelse med EU-retten.

4. DOKUMENTER, SOM FREMLÆGGES

Bilag B Orientering om udskydelse af ændring af logningsregler af 1. oktober 2019

Bilag C Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivende af indlæg i SpaceNet af 14 . februar 2020

Bilag D Orienteringsnotat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i The Commissioner of the Garda Siochana af 5. august 2020

Bilag E Spørgsmål nr. 140 fra Rosa Lund til Justitsministeren af 21. oktober 2020

Bilag F Spørgsmål J fra Karina Lorentzen Dehnhardt til Justitsministeren af 13. november 2020

Bilag G Spørgsmål K fra Karina Lorentzen Dehnhardt af 13. november 2020

Bilag H Spørgsmål L fra Karina Lorentzen Dehnhardt til Justitsministeren af 13. november 2020

Bilag I Spørgsmål 219 fra Karina Lorentzen Dehnhardt til Justitsministeren af 17. november 2020

Bilag J Spørgsmål 220 fra Karina Lorentzen Dehnhardt til Justitsministeren af 17. november 2020

Bilag K	Spørgsmål 221 fra Karina Lorentzen Dehnhardt til Justitsministeren af 17. november 2020
Bilag L	Spørgsmål 222 fra Karina Lorentzen Dehnhardt til Justitsministeren af 17. november 2020
Bilag M	Spørgsmål 223 fra Karina Lorentzen Dehnhardt til Justitsministeren af 17. november 2020
Bilag N	Notat til Folketingets Retsudvalg og Europaudvalg om Domstolens afgørelse i Quadrature du Net af 19. november 2020
Bilag O	Justitsministerens svar på spørgsmål 140 af 20. november 2020
Bilag P	Justitsministerens svar på spørgsmål 219 af 5. januar 2021
Bilag Q	Justitsministerens svar på spørgsmål 220 af 5. januar 2021
Bilag R	Justitsministerens svar på spørgsmål 221 af 5. januar 2021
Bilag S	Justitsministerens svar på spørgsmål 222 af 5. januar 2021
Bilag T	Justitsministerens svar på spørgsmål 223 af 5. januar 2021
Bilag U	Justitsministerens udkast til talepapir 12. januar 2021
Bilag V	Spørgsmål 562 fra Karina Lorentzen Dehnhardt til Justitsministeren af 21. januar 2021
Bilag W	Spørgsmål 563 fra Karina Lorentzen Dehnhardt til Justitsministeren af 21. januar 2021
Bilag X	Spørgsmål 564 fra Karina Lorentzen Dehnhardt til Justitsministeren af 21. januar 2021
Bilag Y	Spørgsmål 565 fra Karina Lorentzen Dehnhardt til Justitsministeren af 21. januar 2021
Bilag Z	Spørgsmål 563 fra Karina Lorentzen Dehnhardt til Justitsministeren af 21. januar 2021
Bilag Æ	Forslag til lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbruger-forhold på telemarkedet mv. af 29. januar 2021
Bilag Ø	Justitsministerens svar på spørgsmål 562 af 17. februar 2021
Bilag Å	Justitsministerens svar på spørgsmål 563 af 17. februar 2021
Bilag AA	Justitsministerens svar på spørgsmål 564 af 17. februar 2021

Bilag AB Justitsministerens svar på spørgsmål 565 af 17. februar 2021

Bilag AC Justitsministerens svar på spørgsmål 566 af 17. februar 2021

Bilag AD CTA's terrortrusselsvurdering af 1. marts 2020

Bilag AE Forslag til lov om ændring af straffeloven, retsplejeloven og forskellige andre love af 31. marts 2016 (uddrag)

Bilag AF Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarket mv. af 24. marts 2010

Bilag AG Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet mv. af 14. december 2011

Bilag AH Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet mv. af 6. februar 2013

Bilag AI Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet mv. af 29. april 2015

Bilag AJ Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet mv. af 26. april 2017

Bilag AK Forslag til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet mv. af 11. april 2018

København, den 25. februar 2021

Rass Holdgaard
Partner, Advokat (H)

Bird & Bird
Advokatpartnerselskab
Sundkrogsgade 21
2100 København Ø
Danmark

Tlf +45 72 24 12 12

twobirds.com

Sag BS-36799/2018-OLR
Østre Landsret
14. Afdeling
Bredgade 59
1260 København K.

PROCESSKRIFT I

Sagsøger	Foreningen imod Ulovlig Logning CVR-nr. 39 30 93 86 Birkegade 15, 5. tv. 2200 København N v./advokat Martin Von Haller ("Sagsøger")
mod	
Sagsøgte	Justitsminister Nick Hækkerup Justitsministeriet Slotholmsgade 10 1216 København K v./advokat Rass Holdgaard ("Sagsøgte")

1. PÅSTAND

Sagsøger nedlægger følgende *sideordnede* anerkendelsespåstande:

1) bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik er ugyldig;

2) Sagsøgte har ikke sikret, at den ugyldige retstilstand fra bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnet og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger blev bragt til ophør hurtigst muligt.

2. INDLEDENDE BEMÆRKNINGER

Sagsøger fastholder, at EU-Domstolens dom af 6. oktober 2020 i La Quadrature du Net m.fl.[1] (”**La Quadrature-dommen**”) er et udtryk for en stadfæstelse af Tele2/Sverige og Watson[2] (”**Tele2-dommen**”) og Digital Rights Ireland og Seitlinger m.fl[3] (”**Digital Rights-dommen**”).

Sagsøger anerkender – i tråd med sin Replik af 7. januar 2021 – at La Quadrature-dommen rummer en række nuanceringer og konkrete krav til, hvordan medlemsstater under særlige omstændigheder kan logge. EU-Domstolen udtaler således, at der *undtagelsesvis* kan ske *midlertidig generel og udifferentieret* logning af trafik-og lokaliseringsdata, dog alene såfremt yderligere betingelser og retsgarantier er iagttaget.

Det er således forkert, når Sagsøgte påstår, at *”La Quadrature-dommen grundlæggende ændrer de EU-retlige rammer for logning[4]*”. Det er ligeledes misvisende, når Sagsøgte hævder, at den blotte tilstedeværelse af en *”alvorlig trussel mod den nationale sikkerhed*” åbner op for, at Sagsøgte kan videreføre Logningsbekendtgørelsen.

En sådan unuanceret, og fragmenteret læsning af La Quadrature-dommen, negligerer dommens centrale præmisser– og understreger denne sags principielle karakter.

La Quadrature-dommen fremhæver ligeledes, at en medlemsstat ikke kan opretholde en ugyldig retstilstand med midlertidige foranstaltninger.

Sagsøger nedlægger en supplerende påstand om, at Justitsministeriet har en reel og konkret handlepligt og derfor ikke blot kan ”sidde på hænderne”, indtil ministeriet på et tidspunkt udtænker en lovlig løsning. Justitsministeriet skulle have sikret, at Logningsbekendtgørelsen ikke længere var virksom, indtil en revision af reglerne var tilvejebragt.

Ministeriet har ved sin tilgang ikke handlet *”så hurtigt som muligt*”.

Der er ikke herved tale om nye forhold, idet spørgsmålet allerede har været indgående behandlet i parternes processkrifter.

---

[1] Forenede sager C-511/18, C-512/18 og C-520/18
[2] Forenede sager C-203/15 og C-698/15
[3] C-293/12
[4] Duplikken, side 4

Justitsministeriet har den 24. marts 2021 fremsat en såkaldt "lovskitse", som indeholder de overordnede principper for den forestående revision af logningsreglerne ("**Lovskitsen**"), jf. Bilag 18. Ministeriet anfører i forlængelse heraf, at Lovskitsen skal danne grundlag for drøftelser med branchen og relevante interessenter, samt at et lovforslag påtænkes fremsat ved Folketingets åbning i oktober 2021. Sagsøger skal bemærke, at Lovskitsen ikke udgør en retskraftig akt, ligesom den hverken suspenderer, ændrer eller sætter Logningsbekendtgørelsen ud af kraft. Sagsøger finder ikke, at Lovskitsen udgør en tilstrækkelig foranstaltning til, at Sagsøgte har løftet sin handlepligt i forhold til at bringe Logningsbekendtgørelsen i overensstemmelse med den retsstilling, som EU-Domstolen har fastlagt. Hvorvidt et efterfølgende lovforslag, der – angiveligt – fremsættes i oktober 2021 kunne udgøre en sådan tilstrækkelig foranstaltning er ikke til pådømmelse i denne sag.

For nuværende er status, at Logningsbekendtgørelsen fortsat er i kraft – i henhold til ministeriet med de kvalifikationer, som ministeren afgav på et samråd den 14. januar 2021, hvorved Justitsministeriet har anerkendt, at dele af bekendtgørelsen ikke kan håndhæves.

3. BEMÆRKNINGER TIL UDVALGTE FORHOLD

3.1 National sikkerhed – en snæver undtagelse

EU-Domstolen har ved La Quadrature-dommen bekræftet, at EU-retten som det klare udgangspunkt er til hinder for national lovgivning, der foreskriver generel og udifferentieret logning af trafik- og lokaliseringsdata.

EU-Domstolen udtaler imidlertid, at der – af hensyn til national sikkerhed – undtagelsesvis kan ske en midlertidig generel og udifferentieret logning af trafik- og lokaliseringsdata. Denne mulighed er dog underlagt en række stringente krav.

Nedenfor gennemgås først konturerne af den undtagelse, som EU-Domstolen opridser ved La Quadrature-dommen (afsnit 3.1.1). Herefter gennemgås, med afsæt i dommens præmis 137-139, de betingelser og retsgarantier, som benyttelsen af denne undtagelse betinges af (afsnit 3.1.2). Endeligt anføres det med afsæt i en ordlydsfortolkning af præmis 138-139, at bekendtgørelsesformatet ikke er egnet til at etablere en lovlig praksis på logningsområdet (afsnit 3.1.3).

3.1.1 Kvalificerende omstændigheder

Med afsigelsen af La Quadrature-dommen, har EU-Domstolen anerkendt, at hensynet til en *kvalificeret trussel mod national sikkerhed* i visse – afgrænsede – tilfælde kan begrunde et generelt og udifferentieret logningspåbud.

Domstolen udtaler, at følgende omstændigheder skal være til stede, før der er tale om en kvalificeret trussel mod den nationale sikkerhed:

1. Der er tilstrækkelige og konkrete omstændigheder, som indikerer, at
2. en medlemsstat står overfor en alvorlig fare, og
3. denne fare er reel, aktuel eller forudsigelig.

Når disse kvalificerende omstændigheder foreligger, aktualiseres *muligheden for* at pålægge udbydere en pligt til at foretage en generel og udifferentieret logning.

Som det vil fremgå af afsnit 3.1.2, er det således ikke i sig selv tilstrækkeligt, at en medlemsstat kan påvise, at der er en kvalificeret trussel mod den nationale sikkerhed.

3.1.2 Betingelser og retsgarantier

EU-Domstolen opstiller fem kumulative krav, som skal være opfyldt førend en medlemsstat, kan begrunde et generelt og udifferentieret logningspåbud i hensynet til national sikkerhed. Disse har til formål at sikre den rette balance mellem på den ene side beskyttelsen af den nationale sikkerhed og på den anden side Charterets artikel 7, 8 og 11 samt artikel 52, stk. 1.

For det første udtaler Domstolen, at ethvert påbud om at foretage forebyggende logning skal "*tidsmæssigt begrænses til det strengt nødvendige*[5]".

For det andet forudser Domstolen, at kravet om tidsbegrænsning vil kunne udhules, ved periodiske og gentagende forlængelser af logningspåbuddet. EU-Domstolen foregriber dette ved at betone, at varigheden af hvert enkelt påbud ikke må "*overstige et forudsigeligt tidsrum*" og at lagringen under alle omstændigheder ikke må have "*systematisk karakter*". Domstolen opstiller således klare parametre for *(i)* lovligheden af det enkelte påbud og *(ii)* lovligheden af den samlede mængde påbud.

For det tredje angiver Domstolen, at lagring af data skal være "*omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte personers personoplysninger mod risikoen for misbrug*[6]".

For det fjerde understreger EU-Domstolen vigtigheden af at sikre, at logning "*rent faktisk begrænses til de situationer, hvor der foreligger en trussel mod den nationale sikkerhed*[7]".

For det femte udtaler EU-Domstolen, at en afgørelse, hvorved udbydere pålægges en logningsforpligtelse skal kunne gøres til genstand for "*[…] en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt*[8]" [vores fremhævelse]. Det er i den forbindelse væsentligt at foregribe, at en sådan "effektiv prøvelse" ville fordre, at en domstol reelt og meningsfyldt gives mulighed for at efterprøve, om en sådan situation foreligger.

EU-Domstolen fastlægger således klare, stringente og kumulative betingelser for lovligheden af et påbud om generel og udifferentieret logning. Det er med andre ord ikke i sig selv tilstrækkeligt, at en medlemsstat kan sandsynliggøre eller sågar påvise en kvalificeret trussel mod den nationale sikkerhed.

Justitsministeriet har i duplikken anført, at der "*[…] aktuelt består en trussel mod den nationale sikkerhed i Danmark, der kan betegnes som alvorlig, reel og aktuel, og som dermed kan begrunde opretholdelsen af en forpligtelse til generel udifferentieret*

[5] La Quadrature-dommen, præmis 137
[6] Ibid. Præmis 138
[7] Ibid. Præmis 139
[8] Ibid. Præmis 139

lagring af teleoplysninger i overensstemmelse med La Quadrature-dommens præmis 137."

Ministeriet støtter dette anbringende på en vurdering foretaget af Center for Terror Analyse ("CTA"), som henhører under PET.

Sagsøger har hverken grundlag eller mulighed for at anfægte CTA's vurdering af trusselsniveauet. Det er dog afgørende at understrege, at en sådan vurdering ikke automatisk eller *i sig selv* kan begrunde en udifferentieret lagring af teleoplysninger, som fejlagtigt påstået af Sagsøgte. Derudover har Sagsøger svært ved at se, hvordan logning begrundet i national sikkerhed også kan begrunde logning til efterforskning af berigelses- eller voldsforbrydelser, der ikke har nogen relation til terror eller andre kvalificerede trusler mod national sikkerhed.

En sådan vurdering fra CTA vil således kunne indgå som et moment i et forestående pålæg om logning, men den kan ikke i sig selv udgøre et grundlag for at indføre generel og uddifferentieret logning – alene med henvisning til, at Danmark er genstand for en kvalificeret trussel mod national sikkerhed.

Det gøres i forlængelse heraf gældende, at Justitsministeriets læsning af dommen – som fremført i duplikken – fremstår fragmenteret, idet ministeriet i det hele undgår at forholde sig til de fem kumulative betingelser og retsgarantier, som EU-Domstolen opstiller i La Quadrature-dommens præmis 137-139.

Sådanne garantier er ikke tilsikret indenfor rammerne af den nuværende Logningsbekendtgørelse, der giver adgang til en generel, udifferentieret og ikke tidsmæssigt begrænset logningspraksis.

Det gøres på den baggrund gældende, at Logningsbekendtgørelsen strider imod EU-retten, allerede fordi den ikke lever op til de supplerende betingelser og retsgarantier, som La Quadrature-dommen opstiller.

3.1.3 Særligt hvad angår bekendtgørelsesformatets tilstrækkelighed

Det fremgår af Justitsministeriets duplik, at ministeriet agter at tilpasse den eksisterende Logningsbekendtgørelse i kølvandet på La Quadrature-dommen.

Det fremstår umiddelbart uklart, om Justitsministeriets vurdering er, at EU-Domstolens anvisninger kan efterleves indenfor rammerne af en bekendtgørelse. I sin Lovskitse anfører Justitsministeriet følgende[9]:

> *"[...] Det foreslås på den baggrund, at der indføres en ordning, hvorefter justitsministeren kan fastsætte en forpligtelse for teleudbydere mv. i op til 1 år."*

Denne formulering kunne tyde på, at Justitsministeriet agter at udmønte logningsforpligtelsen ved et generelt 1-årigt påbud, udstedt ved en årlig bekendtgørelse.

Det gøres supplerende gældende, at etableringen af en lovlig logningspraksis næppe vil kunne udmøntes ved bekendtgørelse alene, jf. La Quadrature-dommens præmis 138-139.

[9] Lovskitsen, side 24

Af dommens præmis 138 fremgår:

> *"Et påbud om at foretage forebyggende lagring af data, der vedrører alle brugere af elektroniske kommunikationsmidler, skal ikke desto mindre tidsmæssigt begrænses til det strengt nødvendige. Selv om det ikke kan udelukkes, at et påbud, der udstedes til udbyderne af elektroniske kommunikationstjenester, om at foretage lagring af data, kan forlænges som følge af, at en sådan trussel fortsat består, må varigheden af hvert enkelt påbud ikke overstige et forudseeligt tidsrum."* [vores fremhævelse]

Af dommens præmis 139 følger endvidere, at:

> *"[…] Det er i denne henseende væsentligt, at en afgørelse, hvorved udbyderne af elektroniske kommunikationstjenester pålægges at foretage en sådan lagring af data, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt."* [vores fremhævelse]

Dommens franskprogede version opererer med ordene "injonction" og "décision" mens den engelsksprogede version anvender "instruction" og "decision".

En traditionel dansk forvaltningsretlig forståelse af ordet "afgørelse" fordrer, at en sådan skal bygge på en konkret og individuel vurdering og ligeledes skal indeholde alle relevante og aktuelle hensyn i sagen. Det er herudover en forudsætning, at der inden afgørelsen er indhentet eventuelle nye og relevante oplysninger. Dette taler imod en statisk ordning, hvorved forpligtelsen pålægges for ét år ad gangen, og således mangler den dynamiske, konkrete og aktuelle karakter, som kendetegner en afgørelse.

Sammenfattende gøres det gældende, at La Quadrature-dommens præmis 138-139 bestyrker Sagsøgers påstand om nødvendigheden af at tilsidesætte Logningsbekendtgørelsen som ugyldig – allerede fordi bekendtgørelsesformatet er uegnet til at etablere en lovlig praksis på området.

3.2 Justitsministeriets ageren i sagen har været materielt og tidsmæssigt utilstrækkelig

Sagsøgers anden påstand vedrører Justitsministeriets ageren i sagen, som i Sagsøgers optik ikke har levet op til det EU-retlige krav om, at en tilpasning af national ret bør ske "*så hurtigt som muligt*".

Ved vurderingen af dette forhold opstår følgende tre underspørgsmål, som behandles særskilt i det følgende:

1. Hvornår aktualiseres medlemsstatens handlepligt (afsnit 3.2.1)
2. Hvor hurtigt herefter skal medlemsstaten agere (afsnit 3.2.2)?
3. Hvilke tiltag har frigørende virkning (afsnit 3.2.3)?

3.2.1 Hvornår aktualiseres medlemsstatens handlepligt?

Allerede ved EU-Domstolens afsigelse af Digital Rights-dommen i 2014 blev der skabt en formodning for, at de danske logningsregler ikke var i overensstemmelse med EU-

retten, idet dommen erklærede dét direktiv, som de danske regler er modelleret over, ugyldigt.

Ved afsigelsen af Tele2-dommen i 2016 blev enhver rest af tvivl endegyldigt fjernet. Herved stadfæstede EU-Domstolen, at nationale regler, der foreskriver en generel og udifferentieret logning, er i strid med EU-retten.

Justitsministeriet har under denne sags forløb vedvarende påstået, at retstilstanden selv efter Tele2-dommen var "uklar", hvorfor ministeriet har set sig nødsaget til at afvente EU-Domstolens afgørelse i Le Quadrature-dommen. Af samme årsag, har Justitsministeriet i denne sag gjort en dyd ud af at udlægge La Quadrature-dommen som et nybrud.

Det fremgår imidlertid af justitsministerens talepapir fra et samråd i Retsudvalget den 2. marts 2017, at Justitsministeriet allerede på daværende tidspunkt havde vurderet følgende:

> *"Jeg skal starte med at understrege, at vi ikke er færdige med at analysere konsekvenserne af dommen i Tele2- sagen for de danske logningsregler. Der er dog to centrale konklusioner i EU-domstolens dom, **som ligger fast allerede på nuværende tidspunkt**.*
>
> *For det første: Ifølge dommen er EU-retten til hinder for en såkaldt "generel og udifferentieret" logning af alle oplysninger. Det vil med andre ord sige, at regler om logning ikke må omfatte alle teleselskabernes kunder til enhver tid.*
>
> *For det andet: Ifølge dommen er EU-retten ikke til hinder for såkaldt "målrettet" logning af oplysninger med henblik på bekæmpelse af grov kriminalitet eller en fare mod den offentlige sikkerhed[10]."* [vores fremhævelse]

Denne erkendelse blev ligeledes afspejlet i den efterfølgende udsættelseslov[11], som blev fremsat den 26. april 2017, hvoraf følger:

> *"De danske logningsregler indebærer, at teleudbyderne skal foretage logning af en række oplysninger om alle deres kunder, på alle tidspunkter og i hele landet, jf. nærmere herom pkt. 2.3. Det må derfor forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.4 ovenfor, vil skulle foretages nogle tilpasninger af de danske logningsregler, således at reglerne målrettes. EU-Domstolen har ikke taget stilling til, hvordan målrettede logningsregler nærmere kan udfærdiges."*

Af den juridiske litteratur fremgår følgende:

> *"Højesterets praksis i CO-industri kan udlægges til, at lovgiver efter at være bibragt et fyldestgørende grundlag skal reagere hurtigt, dermed sprogvalget om "legitim" forsinkelse. Det kan overvejes, om det samme gælder i det øjeblik, hvor den ansvarlige minister er bibragt en retlig vurdering af overtrædelsen. Om det i så fald vil være nødvendigt at fremsætte en midlertidig lov indtil et endeligt fyldestgørende beslutningsgrundlag er tilvejebragt[12]."* [vores fremhævelse]

Det gøres bl.a. på ovenstående baggrund gældende, at Justitsministeriet *senest* primo maj 2017 havde tilvejebragt et tilpas fyldestgørende grundlag til fastlæggelse af, at en

[10] Bilag 7
[11] Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige, afsnit 3 i de almindelige bemærkninger
[12] Klinge, EU-direktiver og Grundrettigheder i horisontale retsforhold, side 286

generel og udifferentieret logning ikke kunne opretholdes efter EU-retten. Dette lå – med ministeriets egne ord – fast allerede på daværende tidspunkt.

At Tele2-dommen, i Justitsministeriets optik, rummer andre uklarheder og ikke leverer en alternativ løsning, som Justitsministeriet kan sætte i stedet kan ikke begrunde, at ministeriet i det hele undlader at reagere. En sådan manglende tilpasning kan heller ikke – uanset om ministeriet på et tidspunkt skulle dokumentere dette – begrundes i at "oplysningerne er for vigtige" eller at de indgår i "politiets daglige arbejde med at bekæmpe alvorlig kriminalitet[13]", som antydet i ministerens talepapir til brug for ovennævnte samråd i Retsudvalget.

Det gøres således gældende, at Justitsministeriets handlepligt senest aktualiseres i forbindelse med Tele2-dommens udredning primo 2017, og at dén omstændighed, at der – i ministeriets optik – var en række uklarheder eller politiske uhensigtsmæssigheder ikke kan begrunde en manglende tilpasning eller en forlænget stand-still periode.

3.2.2 Hvor hurtigt skal medlemsstaten agere?

I forlængelse af ovenstående spørgsmål er det naturligt at analysere, hvor lang reaktionstid lovgiver ydes efter aktualiseringen af en sådan handlepligt. Stævningens afsnit 3.8.2-3.8.3 behandler dette forhold indgående.

I forlængelse heraf skal det supplerende bemærkes, at Justitsministeriet i skrivende stund har brugt over 4 år på at tilpasse de danske logningsregler – hvis Tele2-dommen bruges som målestok, jf. afsnit 3.2.1.

I den juridiske litteratur er det – i en erstatningssammenhæng, og med afsæt i CO-industri dommen samt EU-Domstolens praksis vedrørende TEUF artikel 260, stk. 2 – vurderet, at en varighed på over 2 år i sig selv vil være erstatningspådragende:

> "[...] *I forhold til anvendelsen af en billedlig figur med trafiklys om de konstaterede varigheder, er det min vurdering, at en varighed af overtrædelse på under 12 måneder vil befinde sig i den "grønne zone" (jf. CO-industri-dommen) og varigheder mellem 12-24 måneder i den "gule zone" (jf. bødesagerne), mens jeg vurderer, at varigheder over 24 måneder i sig selv vil være ansvarspådragende (medmindre helt ekstraordinære hensyn gør sig gældende, som f.eks. Kommissionens medvirkende til retsvildfarelsen eller manglende ændring af EU-retlige regler fra EU-lovgiver). [...] Denne opdeling i perioder harmonerer også med andre EU-retlige omstillingsperioder som f.eks. implementeringsfristen efter vedtagelsen af et EU-direktiv[14].* " [vores fremhævelse]

Det fastholdes i tråd hermed, at en reaktionstid på mere end 4 år ikke lever op til "så hurtigt som muligt" tærsklen.

Det skal i den forbindelse supplerende bemærkes, at begge parter har henvist til Højesterets afgørelse i CO-industri sagen til støtte for deres påstande. En væsentlig pointe, som hidtil ikke har genkaldt sig megen opmærksomhed er, at Sagsøger *ikke* i nærværende sag har nedlagt en erstatningspåstand, som tilfældet var i CO-industri sagen.

[13] Bilag 7, side 7
[14] Klinge, EU-direktiver og Grundrettigheder i horisontale retsforhold, side 285

Det gøres supplerende gældende, at tærsklen som anvist af Højesteret i CO-sagen udgør den *absolutte øvre grænse* for varigheden af uoverensstemmelser mellem national ret og EU-retten. Det er således Sagsøgers påstand, at ministeriets handlepligt indtræder på et langt tidligere tidspunkt end dér, hvor varigheden rent faktisk udløser et erstatningsansvar.

Det gøres derfor gældende, at Justitsministeriets manglende konsekvensændring af logningsreglerne mere end 4 år efter tilvejebringelsen af et fyldestgørende beslutningsgrundlag ikke lever op til "så hurtigt som muligt" tærsklen som anvist i Jonkman.

Endeligt skal det bemærkes, at Justitsministeriet – ved fremlæggelsen af en Lovskitse – har angivet, at ministeriet forventer, at ny lovgivning på området vil kunne træde i kraft den 1. januar 2022. Sagsøger skal for en god ordens skyld bemærke, at dette ikke giver anledning til at korrigere ovenstående, allerede fordi en manglende effektuering på fjerde år ville være i strid med Jonkman-tærsklen.

For det tilfælde, at landsretten måtte finde, at Justitsministeriets handlepligt først aktualiseres ved afsigelsen af La Quadrature-dommen, skal Sagsøger først og fremmest henlede opmærksomheden mod ovennævnte betragtninger, hvorved der skal tages bestik af, at omdrejningspunktet for denne sag ikke er den erstatningsudløsende undladelse. Det gøres herudover gældende, at et så langstrakt forløb som det nuværende, ville forudsætte, at ministeriets effektuering af dommen sker endog *meget hurtigt* efter aktualiseringen af en handlepligt. Det bemærkes til støtte herfor, at Justitsministeriet over de seneste 10 år har afgivet talrige indlæg for EU-Domstolen, forestået ekstensivt lovgivningsarbejde med henblik på at udsætte en revision, besvaret utallige Folketingsspørgsmål og forberedt adskillige samråd. Der er således næppe – på nuværende tidspunkt – tale om et uforudsigeligt nybrud, som vil kunne begrunde en lang betænkningstid.

3.2.3 Hvilke tiltag har frigørende virkning?

Fokus i parternes processkrifter har hidtil været rettet mod hastigheden, hvormed Justitsministeriet skulle have ageret til brug for tilpasningen af dansk ret. Det gøres supplerende gældende, at ikke alle tiltag kan have frigørende virkning.

EU-Domstolen udtalte allerede ved Jonkman[15], at det:

> *"[...] påhviler den pågældende medlemsstats myndigheder at træffe de almindelige eller særlige foranstaltninger, der er egnede til at sikre overholdelsen af fællesskabsretten, idet de navnlig skal påse, at national ret så hurtigt som muligt bringes i overensstemmelse med fællesskabsretten, og at borgernes rettigheder i henhold til fællesskabsretten gennemføres fuldt ud[16]."* [vores fremhævelse]

Som nærmere beskrevet i afsnit 3.3 nedenfor, bliver dette udgangspunkt gentaget ved La Quadrature-dommens præmis 214, idet Domstolen udtaler, at alle instanser skal sikre, at EU-retlige regler "*gennemføres fuldt ud*".

Efter retspraksis fordrer en gennemførelse således reelle, materielle og autoritative lovændringer af en vis intensitet.

---

[15] De forenede sager C-231/06-C-233/06 Jonkman
[16] Jonkman, præmis 41

Denne læsning understøttes af den juridiske litteratur, der angiver følgende[17]:

> *"Det kan sammenfattende konkluderes, at lovgivers samlede reaktionstid kan indledes i følgende delperioder: Periode **A**, der udgør lovforberedende arbejde og den retlige vurdering af EU-domme, periode **B** det efterfølgende parlamentariske arbejde med fremsættelsen i Folketinget og tre behandlinger, der afsluttes med en vedtagelse af ændringsloven, og periode **C** det tidsrum, som fremgår af ikrafttrædelsesbestemmelsen, som kan indeholde bestemmelser om tilbagevirkende kraft […]. Først ved ikrafttrædelsen er den EU-stridige retstilstand bragt til ende."* [vores fremhævelse]

Sådanne materielle lovændringer er, som bekendt, ikke indført. At Justitsministeriet har deltaget i diverse arbejdsgrupper og drøftelser i EU-regi, er ikke et tiltag af en sådan autoritativ styrke og kvalitet, som kan begrunde en overholdelse af handlepligten.

Justitsministeriet har herudover forklaret sit "bidrag" til overholdelsen af EU-retten ved at henvise til, at logningsreglerne ikke vil blive håndhævet[18]:

> *"Ministeren har med denne erklæring om de manglende muligheder for at håndhæve dele af logningsreglerne gjort det klart, at logningsbekendtgørelsens bestemmelser ikke vil blive anvendt på en måde, der kan stride mod EU-retten. Dermed har ministeriet bidraget til at overholde de EU-retlige forpligtelser, der kan udledes af EU-Domstolens retspraksis."* [vores fremhævelse]

Det gøres gældende, at udtalelser om "manglende intention" om at håndhæve regler i strid med EU-retten ikke udgør relevante momenter i vurderingen af, om ministeriet har iværksat passende foranstaltninger. En sådan manglende håndhævelsesmulighed følger langt hen ad vejen allerede af EU-rettens forrangs princip, hvorfor ministeriets udtalelse herom ikke dækker over et selvstændigt bidrag.

Justitsministeriet har senest også fremlagt en Lovskitse, som redegør for ministeriets "overordnede overvejelser" vedrørende ny lovgivning på området. Det fremgår af Lovskitsen, side 75, at:

> *"[…] Samlet set er det således Justitsministeriet vurdering, at der ikke forud for indførelsen af ny lovgivning […] er behov for en suspension af anvendelsen af loggede oplysninger, der er opnået ved en generel og udifferentieret lagring af trafik- og lokaliseringsdata."*

Ministeriet har således endnu engang afvist at suspendere en bekendtgørelse, som ministeriet i over 4 år har erkendt er EU-retsstridig. Al den stund Lovskitsen ikke er ledsaget af en reel suspension af Logningsbekendtgørelsen, vil ovenstående betragtninger gøre sig gældende med samme styrke og intensitet. Det gøres således gældende, at heller ikke Lovskitsen er et tiltag af en sådan autoritativ karakter og styrke, som kan begrunde, at Justitsministeriet har løftet sin handlepligt.

Det gøres opsamlende gældende, at Justitsministeriet ikke før ikrafttrædelsen af en revideret lovpakke kan siges at have opfyldt sin EU-retlige handlepligt.

3.2.4 Afsluttende bemærkninger

Det gøres således opsamlende gældende:

[17] Klinge, EU-direktiver og Grundrettigheder i horisontale retsforhold, side 285
[18] Duplikken, side 19

1) at Justitsministeriets handlepligt senest aktualiseres i forbindelse med Tele2-dommens udredning primo 2017, og at dén omstændighed, at der – i ministeriets optik – var en række uklarheder eller politiske uhensigtsmæssigheder ikke i sig selv kan begrunde en manglende tilpasning eller en forlænget stand-still periode;

2) at Justitsministeriets manglende konsekvensændring af de danske logningsregler 4 år efter aktualiseringen af denne handlepligt ikke lever op til "*så hurtigt som muligt*" tærsklen, jf. Jonkman;

3) at Justitsministeriet først har løftet sin handlepligt ved ikrafttrædelsen af en materiel revision af de danske logningsregler.

3.3 En midlertidig opretholdelse af status quo kan ikke konkret begrundes

Som skitseret ovenfor har Justitsministeriet siden Tele2-dommen anerkendt, at en revision af de danske logningsregler er nødvendig (afsnit 3.2.1). Som også beskrevet ovenfor, har Justitsministeriet gentagende gange og senest ved Lovskitsen afvist at suspendere Logningsbekendtgørelsen i den mellemliggende periode (afsnit 0). Justitsministeren har sågar personligt indskærpet fastholdelsen af logningsreglerne overfor teleselskaberne (Bilag 10), og sidenhen tyet til at "opfordre" teleselskaberne til at fortsætte en praksis, som ministeriet selv har erkendt, er EU-retsstridig (Bilag 21).

Det er i forlængelse heraf væsentligt at overveje, om en sådan fastholdelse af de danske logningsregler ville være berettiget med henvisning til reglernes "midlertidige" karakter eller omstændighederne i øvrigt.

Det er Sagsøgers påstand, at La Quadrature-dommen endegyldigt fastlægger, at Justitsministeriets fastholdelsen af status-quo i en mellemliggende periode ikke har været berettiget.

Justitsministeriet har i et notat til Folketingets Europa Udvalg af 29. november 2018 anerkendt, at EU-Domstolens besvarelse af det fjerne spørgsmål i La Quadrature-dommen vil have en væsentlig indflydelse på nærværende sag[19]:

> *"[...] Endvidere er spørgsmålet fra den belgiske forfatningsdomstol, der vedrører muligheden for midlertidig opretholdelse af logningsregler i strid med EU-retten, af væsentlig dansk interesse, idet der er anlagt et civilt søgsmål mod Justitsministeriet, hvor et centralt spørgsmål forventes at blive, om Danmark har brugt for lang tid på at revidere logningsreglerne i lyset af Tele2-dommen."*

I La Quadrature-dommen har EU-Domstolen, med henvisning til EU-rettens forrang, besvaret dette centrale spørgsmål benægtende.

I præmis 214 uddyber Domstolen, hvilke forpligtelser EU-rettens forrang pålægger "alle instanser" – herved også at forstå den lovgivende magt:

> *"Dette princip medfører derfor en forpligtelse for alle instanser i medlemsstaterne til at sikre, at de forskellige EU-retlige regler gennemføres fuldt ud, idet medlemsstaternes nationale ret ikke kan ændre den virkning, som disse forskellige regler tillægges på disse staters område."* [vores fremhævelse]

[19] Bilag 22, side 3

I præmis 215 gentager Domstolen de krav, som EU-rettens forrang afstedkommer for de nationale domstole:

> *"Den nationale ret, der inden for sit kompetenceområde skal anvende EU-retlige bestemmelser, har i henhold til princippet om forrang pligt til – såfremt det ikke er muligt at anlægge en fortolkning af national lovgivning, der er i overensstemmelse med de EU-retlige krav – at sikre disse bestemmelsers fulde virkning, idet den om fornødent af egen drift skal undlade at anvende enhver modstående bestemmelse i national lovgivning, endog en senere national bestemmelse, uden at den behøver at anmode om eller afvente en forudgående ophævelse af denne bestemmelse ad lovgivningsvejen eller ved noget andet forfatningsmæssigt middel."* [vores fremhævelse]

Domstolen uddyber i forlængelse heraf, at kun EU-Domstolen kan træffe afgørelse om en midlertidig udsættelse, og overvejer da også, om dette konkret er aktuelt for så vidt angår logningsreglerne. Domstolen vurderer imidlertid ikke, at der foreligger sådanne "tvingende hensyn", som kan begrunde en midlertidig opretholdelse af EU-retsstridige logningsregler med følgende begrundelse:

> *"[...] Opretholdelsen af virkningerne af en national lovgivning som den i hovedsagen omhandlende ville nemlig indebære, at denne lovgivning fortsat ville pålægge udbydere af elektroniske kommunikationstjenester forpligtelser, der er i strid med EU-retten, og som vil medføre **alvorlige indgreb i de grundlæggende rettigheder**, der tilkommer de personer, hvis oplysninger er blevet lagret."* [vores fremhævelse]

EU-Domstolen forholder sig således både abstrakt og konkret til, om en midlertidig opretholdelse af status-quo kan rummes indenfor rammerne af EU-retten. Domstolen afviser dette med henvisning til EU-rettens forrang sammenholdt med alvoren af de indgreb, som en sådan opretholdelse konkret ville afstedkomme.

Det gøres i tråd hermed gældende, at Justitsministeriets hovedargument for den fortsatte opretholdelse af de danske logningsregler er endegyldigt og konkret udhulet med afsigelsen af La Quadrature-dommen, der netop tager stilling til spørgsmålet om lovligheden af en midlertidig opretholdelse af EU-retsstridige logningsregler.

3.4 Justitsministerens opfordring til fortsat logning og forholdet til øvrige regelsæt

Nærværende sag rummer en klar snitflade til det databeskyttelsesretlige regelsæt, som ikke hidtil har indgået med stor styrke i parternes processkrifter.

Nedenstående bemærkninger skal ses i lyset af, at Justitsministeriets seneste tiltag har været at opfordre teleselskaberne til at fortsætte den ulovlige logning. Som det vil fremgå af afsnit 3.4.2-3.4.3 nedenfor er denne henstilling forbundet med uhensigtsmæssige og betænkelige risici.

3.4.1 Justitsministeriets brev af 29. januar 2021

Teleindustrien rettede den 15. januar 2021 henvendelse til Justitsministeriet med henblik på en afklaring af retsgrundlaget for teleselskabernes fortsatte logning i kølvandet på La Quadrature-dommen (Bilag 20).

Justitsmisteriet besvarede denne henvendelse ved brev af 29. januar 2021 (Bilag 21). Ved dette brev erkender Justitsministeriet, at store dele af de danske logningsregler strider mod EU-retten, men fastholder desuagtet, at logningsreglerne er gyldige og kan

opretholdes i deres helhed. Ministeriet udtaler imidlertid, at logningsreglerne ikke længere kan håndhæves, og at teleselskaberne ikke vil kunne straffes, hvis de undlader at logge.

Justitsministeriet opfordrer ligeledes teleselskaberne til at efterleve logningsreglerne af egen drift:

> "*Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og terror, skal således ses i dette lys.*"

Justitsministeriet mener således *på den ene side*, at reglerne ikke kan håndhæves og *på den anden side* at regelsættet fortsat er i fuld kraft. Disse to udmeldinger synes indbyrdes modstridende, juridisk uholdbare og retssikkerhedsmæssigt betænkelige[20].

Problematikken skærpes yderligere af følgende to momenter:

- at teleselskabernes efterlevelse af justitsministerens opfordring til at fortsætte en EU-retsstridig logningspraksis formodentligt vil resultere i et selvstændigt brud på databeskyttelsesretten (afsnit 3.4.2);

- at sådanne brud vil kunne være genstand for særskilt håndhævelse (afsnit 3.4.3).

3.4.2 Teleselskaberne har ikke længere behandlingshjemmel

Det følger af databeskyttelsesforordningens[21] artikel 5, stk. 1, lit. a, at personoplysninger skal behandles på lovlig, rimelig og gennemsigtig vis. En lovlig behandling forudsætter derudover, at den dataansvarlige kan påvise en behandlingshjemmel, jf. forordningens artikel 6, stk. 1, lit. a-f.

Det følger af forordningens artikel 6, stk. 1, lit. c, at behandlingen kan ske, når:

> "*Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.*" [vores fremhævelse]

Det følger endvidere af præambelbetragtning 45, at:

> "*Hvis behandling foretages i overensstemmelse med en retlig forpligtelse, som påhviler den dataansvarlige […], bør behandlingen have retsgrundlag i EU-retten eller medlemsstaternes nationale ret.*" [vores fremhævelse]

Logningsreglerne ville – under normale omstændigheder – udgøre en sådan retlig forpligtelse, som artikel 6, stk. 1, lit. c, henviser til, ligesom der ville være tale om en lovlig behandling i medfør af artikel 5, stk. 1, lit. a.

Det er med afsigelsen af La Quadrature-dommen endegyldigt klarlagt, at et nationalt regelsæt, der bygger på en forudsætning om generel og udifferentieret logning ikke kan opretholdes – end ikke i en overgangsperiode. Idet Logningsbekendtgørelsen netop bygger på en sådan generel og udifferentieret logning, aktualiserer La Quadrature-

[20] Jf. i samme retning Bilag 17, side 18
[21] Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27/4 2016

dommen spørgsmålet om, hvorvidt teleselskaberne kan basere deres indsamling af personoplysninger på en national "retlig forpligtelse", som strider mod EU-retten.

Af samme årsag, spurgte Teleindustrien i sit brev, om det ville være i overensstemmelse med databeskyttelsesreglerne, hvis teleselskaberne fortsætter med at logge som hidtil.

Justitsministeriet besvarede dette spørgsmål på følgende vis[22]:

> *"[...] I det omfang teleselskabernes behandling af loggede teleoplysninger er i overensstemmelse med dansk ret eller EU-retten som fortolket af EU-Domstolen, vil GDPR ikke være til hinder for teleselskabernes fortsatte behandling af loggede teleoplysninger i overensstemmelse med logningsbekendtgørelsens bestemmelser. Som anført ovenfor er det Justitsministeriets vurdering, at dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed og en målrettet logningsforpligtelse med henblik på bekæmpelse af grov kriminalitet under nærmere betingelser. Trafik- og lokaliseringsdata vil således efter GDPR fortsat kunne logges som hidtil med henblik på beskyttelse af **national sikkerhed** og bekæmpelse af **grov kriminalitet**."* [vores fremhævelse]

Justitsministeriet anerkender således, at logning kun er i overensstemmelse med det databeskyttelsesretlige regelsæt, når logningen sker til to specifikke formål: national sikkerhed og grov kriminalitet.

Overholdelsen af det databeskyttelsesretlige regelsæt forudsætter således, med ministeriets egne ord, at der logges på en anden måde end det er forudsat i den nugældende Logningsbekendtgørelse.

3.4.3 Håndhævelsesforanstaltninger

Et selvstændigt brud på det databeskyttelsesretlige regelsæt, som det i afsnit 3.4.2 skitserede vil kunne foranledige en sag ved Datatilsynet. En sådan sag kan potentielt initieres af Datatilsynet som en "egen driftssag", eller blive foranlediget af en klage fra en af de mange borgere, hvis oplysninger dagligt er genstand for generel og udifferentieret logning.

Det følger af Databeskyttelseslovens § 27, stk. 1, at Datatilsynet udøver sine funktioner i fuld uafhængighed. Den gældende ordning udgør en videreførelse af persondatalovens § 56. Af databeskyttelseslovens almindelige bemærkninger, afsnit 2.7.3.1, fremgår følgende:

> *"Justitsministeriet forholdt sig således til tilsynsmyndighedernes uafhængighed i et svar af 17. december 2012 på spørgsmål nr. 284 (Alm. del) af 19. november 2012 fra Folketingets Retsudvalg. Det fremgår af besvarelsen, at det af persondatalovens § 56 følger, at Datatilsynet udøver sine funktioner i fuld uafhængighed. Dette indebærer bl.a., at hverken Justitsministeriet eller andre ministerier kan give instruktioner eller føre tilsyn med Datatilsynet."* [vores fremhævelse]

Det gøres i tråd hermed gældende, at Justitsministeriet ikke meningsfyldt kan forsikre udbydere om, at en efterlevelse af ministeriets opfordring om fastholdelse af den nuværende ulovlige logningspraksis ikke vil afstedkomme håndhævelsesforanstaltninger ved Datatilsynet.

[22] Bilag 21, side 3

Sådanne sager kan potentielt have alvorlige økonomiske implikationer for udbydere, idet bødeniveauet kan udstrække sig til 4 % af selskabets samlede globale årlige omsætning i det foregående regnskabsår, jf. Databeskyttelsesforordningens artikel 83, stk. 5.

Det gøres på ovenstående baggrund gældende, at Justitsministerens formelle opretholdelse af en EU-retsstridig Logningsbekendtgørelse sammenholdt med ministeriets konkrete opfordring til fastholdelse af en generel og udifferentieret logningspraksis kan føre til et selvstændigt brud på de databeskyttelsesretlige regler. Det gøres i forlængelse heraf gældende, at et sådant selvstændigt brud vil kunne afstedkomme håndhævelsesforanstaltninger ved Datatilsynet, som potentielt kan have alvorlige økonomiske implikationer for de berørte udbydere.

Det gøres sammenfattende gældende, at denne uhensigtsmæssige afsmittende effekt bestyrker Sagsøgers påstand om, at Logningsbekendtgørelsen skal kendes ugyldig.

3.5 Øvrige forhold

I sin Duplik af 25. februar 2021 kommenterer Sagsøgte på spørgsmålet om, hvorvidt EU-rettens forrang kan begrunde, at et modstridende nationalt regelsæt bliver ugyldigt.

Sagsøger skal uddybende oplyse, at dennes påstand ikke går på, at EU-rettens forrang *generelt* skulle føre til, at en modstridende national retsakt straks efter afsigelsen af en EU-retlig dom bliver umiddelbart ugyldig. Når det i denne sag er gjort gældende, at Logningsbekendtgørelsen er "umiddelbart ugyldig", skyldes det de særlige omstændigheder, som gør sig gældende for nærværende sagsforløb.

Sagsøger minder i den forbindelse om, at EU-Domstolen med La Quadrature-dommen for tredje gang har stadfæstet, at en generel og udifferentieret logningspraksis ikke kan opretholdes. Justitsministeriet har – som beskrevet i afsnit 3.2.1 – de seneste 4 år anerkendt, at en generel og udifferentieret logning *ikke* lovligt kan opretholdes, men desuagtet nægtet at agere herpå.

Sagsøger skal i den forbindelse understrege, at argumentet om, at en bekendtgørelse, der på så umiddelbar, erkendt og eklatant vis strider mod en højere retsnorm, er umiddelbart ugyldig (en nullitet) ingenlunde er en nyskabelse i dansk forvaltningsret:

> "*En ugyldig forvaltningsakt kan være en nullitet, eller den kan være anfægtelig. Nullitet er den stærkeste ugyldighed og indebærer, at forvaltningsakten uden videre kan ignoreres af enhver offentlig myndighed og enhver borger. Nullitet forekommer hvor forvaltningsakten er åbenbart eller groft ulovlig*[23].

[23] Garde, m.fl., Forvaltningsret almindelige emner, side 427

København, den 25. marts 2021

Julie Bak-Larsen

Partner, advokat

BILAG

Bilag 18: Justitsministeriets Skitse for revision af logningsreglerne mv.

Bilag 19: Justitia: Analyse, Ulovlig logning – tid til en revision

Bilag 20: Brev af 15. januar 2021 fra Tele Industrien

Bilag 21: Brev af 29. januar 2021 fra Justitsministeriet

Bilag 22: Notat af 29. november 2018 til Folketingets Europaudvalg og Retsudvalget

Processkrift A

Til

Østre Landsret

I sagsnr. BS-19085/2018-KBH: Foreningen imod Ulovlig Logning
(Advokat Julie Bak-Larsen)

mod

Justitsminister Nick Hækkerup
Justitsministeriet
(Advokat Rass Holdgaard)

KØBENHAVN
VESTER FARIMAGSGADE 23
DK-1606 KØBENHAVN V

AARHUS
ÅBOULEVARDEN 49
DK-8000 AARHUS C

T +45 33 15 20 10
@ MAIL@KAMMERADVOKATEN.DK
W WWW.KAMMERADVOKATEN.DK

1. INDLEDNING

Sagsøgeren har i processkrift I af 25. marts 2021 nedlagt en ny påstand, som går ud på, at Justitsministeriet skal anerkende ikke at have sikret, at den ugyldige retstilstand fra logningsbekendtgørelsen blev bragt til ophør hurtigst muligt.

Det er ikke helt klart, hvordan en dom efter denne påstand vil påvirke sagsøgerens retsstilling. Påstanden synes umiddelbart at angå en konstatering af et faktisk forhold, jf. tilsvarende U.2005.2134H. Det er således ikke oplagt, at påstanden er egnet til at indgå i en domskonklusion. Derudover synes påstanden – som sagen er tilskåret af sagsøgeren – fortsat at være et anbringende til støtte for den første påstand, jf. bl.a. sagsøgerens bemærkninger under afsnit 3.5 i processkrift I.

Efter omstændighederne vil Justitsministeriet dog ikke i denne konkrete sag nedlægge påstand om afvisning. Justitsministeriet påstår **frifindelse** overfor denne nye påstand og gør til støtte herfor de samme anbringender gældende som hidtil er fremført. Det bemærkes dog for god ordens skyld, at domstolene efter fast praksis kan afvise påstande ex officio.

Justitsministeriet fastholder overordnet, at logningsbekendtgørelsen ikke kan erklæres generelt ugyldig eller uden virkning som følge af hverken hel eller delvis modstrid med EU-retlige regler. Princippet om EU-rettens forrang betyder alene, at modstridende regler ikke kan anvendes. Sagsøgerens bemærkninger om, at noget andet skulle gælde i denne sag på grund af de påståede særlige omstændigheder, har ingen støtte i hverken dansk ret eller EU-retten.

2. SUPPLERENDE SAGSFREMSTILLING

2.1 Vurdering af terrortruslen mod Danmark 2021

Center for Terroranalyse (CTA) har den 31. marts 2021 offentliggjort en ny og ajourført vurdering af terrortruslen mod Danmark. Vurderingen fremlægges som **bilag AL**.

Det fremgår af vurderingens side 8, at CTA fortsat vurderer, at terrortruslen mod Danmark er alvorlig. Den største trussel er fortsat fra militante islamister. Herom hedder det bl.a. følgende i vurderingen:

> *"Der er personer i Danmark og i udlandet med sympati for militant islamisme, som udgør en terrortrussel mod Danmark. CTA vurderer, at truslen udgår fra personer, der sympatiserer med og inspireres af udenlandske militant islamistiske terrorgrupper, særligt Islamisk Stat (IS) og al-Qaida (AQ). Det illustreres bl.a. af anholdelsen den 30. april 2020 af en dansk*

statsborger, mistænkt for at planlægge et terrorangreb på egen hånd med et eller flere skydevåben, og af anholdelserne den 06. februar 2021 af to syriske statsborgere i Danmark, mistænkt for at planlægge et terrorangreb i Danmark eller udlandet med brug af skydevåben og hjemmelavede bomber. I begge sager er der indikationer på, at de mistænkte var blevet inspireret af militant islamistisk propaganda.

I 2020 har hændelser i Danmark og udlandet, der er blevet opfattet som krænkelser af islam, vist, at krænkelsessager fortsat har et betydeligt potentiale som drivkraft for militante islamister. Reaktioner på krænkelsessager i udlandet og særligt i Frankrig har været med til at sætte fokus på både historiske og aktuelle krænkelsessager i Danmark. Både AQ og IS har i det seneste år omtalt Danmark i deres udgivelser, ligesom den AQ-affilierede gruppe al-Qaida på Den Arabiske Halvø (AQAP) i en propagandaudgivelse har opfordret til at angribe navngivne danske "krænkere". Et øget fokus på krænkelsessager generelt kan skærpe terrortruslen mod Danmark og danske interesser i udlandet. Eventuelle reaktioner vil kunne komme på kort sigt, men vil også kunne finde sted med en betydelig forsinkelse."

Vurderingens kapitel 2 indeholder en detaljeret redegørelse for truslen, som udgår fra militante islamister. Særlige begivenheder, som vurderes at have haft betydning for trusselsbilledet, er bl.a. en række Stram Kurs-demonstrationer med skænding af koraner samt genoptrykningen af de danske muhammedtegninger fra 2005 i et fransk satiremagasin. Det fremgår derudover, at IS som noget nyt siden september 2020 har haft fokus på opfattede krænkelser af islam i sin officielle propaganda, og at denne propaganda deles i danske virtuelle fællesskaber.

2.2 Cybertruslen mod Danmark

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, som er særskilt reguleret ved CFCS-loven, jf. lovbekendtgørelse nr. 836 af 7. august 2019. Centeret har ifølge lovens § 1 til formål at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Center for Cybersikkerhed udgiver årligt en vurdering af cybertruslen mod Danmark. Den seneste vurdering fra juni 2020 fremlægges som **bilag AM**.

Det fremgår bl.a. af denne trusselsvurdering, at cybertruslen er en alvorlig trussel mod Danmark. Truslen fra cyberkriminalitet og cyberspionage vurderes at være "meget høj". Om sidstnævnte anføres bl.a. følgende i vurderingen på side 6:

"Nogle stater, især Rusland og Kina, bruger cyberspionage meget aktivt og der er ingen tegn på, at truslen fra disse stater vil aftage. Der har i de seneste år været en stigning i antallet af lande, især i Asien, der bruger cyberspionage. Destruktive cyberangreb er med enkelte undtagelser forblevet et regionalt fænomen med særlig tilknytning til konflikten i Ukraine og rivaliseringen mellem Iran og Saudi Arabien. Angrebene kan imidlertid sprede sig og ramme Danmark, som det var tilfældet under NotPetya-angrebet i 2017."

På side 6-7 oplistes en række kendte større internationale cyberangreb gennem de sidste 10 år, herunder f.eks. angreb på Demokraternes Nationale Komité i USA i 2016, WannaCry-angrebet på en række hospitaler i Storbritannien i 2017 og et forsøg fra russiske efterretningsagenter på at skaffe sig adgang til organisationen OPCW, som er en organisation, der arbejder for afskaffelsen af kemiske våben.

På side 10-11 anføres bl.a. følgende om cyberangreb mod samfundsvigtige funktioner:

"Målrettede cyberangreb som disse kan få alvorlige konsekvenser for samfundsvigtige funktioner. Det har f.eks. været tilfældet i forbindelse med ransomware-angreb mod sundhedssektoren i bl.a. USA og Storbritannien, hvor nedetid i administrative systemer medførte, at patientaftaler måtte aflyses.

Et vellykket målrettet ransomware-angreb på leverandører af samfundsvigtige ydelser under en krise, som f.eks. mod sundhedssektoren i Danmark under COVID-19 krisen, vil kunne øge det pres, som sektoren allerede oplever pga. krisen.

Angrebet mod Amgros, der er leverandør til danske sygehusapoteker, er et eksempel på et ransomwareangreb mod sundhedssektoren i Danmark under krisen. Angrebet betød bl.a. at Amgros i nogle dage ikke kunne købe og sælge lægemidler via deres forretningssystem Naviline. Angrebet førte dog ikke til mangel på lægemidler på de offentlige hospitaler."

Endvidere anføres det om cyberspionage på side 15f, at der "ses kontinuerlige forsøg på cyberspionage mod danske myndigheder, samt at truslen især er rettet mod myndigheder og personer, der arbejder med udenrigs- og sikkerhedspolitik". Cyberspionage bl.a. kan udnyttes til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres, ligesom det kan skade dansk konkurrenceevne og økonomi.

Derved kan cybertruslen mod Danmark udgøre en trussel mod den nationale sikkerhed, der f.eks. kan påvirke grundlæggende politiske og økonomiske strukturer.

2.3 Justitsministeriets lovskitse af 24. marts 2021

Den 23. marts 2021 offentliggjorde Justitsministeriet en skitse for revision af logningsbestemmelserne i retsplejeloven (REU, Alm. del, Bilag 262, fremlagt i sagen som bilag 18).

Lovskitsen indeholder en udførlig gennemgang af forholdet mellem de gældende logningsregler og EU-Domstolens domme i navnlig Digital Rights-sagen, Tele2-sagen, Ministerio Fiscal-sagen og La Quadrature-sagen. Under afsnit 3.3 tages der bl.a. stilling til muligheden for under nærmere betingelser at opretholde en generel og udifferentieret logning af hensyn til den nationale sikkerhed i lyset af sidstnævnte dom.

Om grundlaget for vurderingen af trusselsniveauet hedder det bl.a. følgende i afsnit 3.3.1:

> *"Det er Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark bygger på tilstrækkeligt konkrete omstændigheder, herunder konkrete efterforskninger og straffesager i Danmark, der gør det muligt at vurdere og sandsynliggøre, om der er en alvorlig trussel mod den nationale sikkerhed, hvor f.eks. aktiviteter alvorligt kan destabilisere Danmarks grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed. Endvidere er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark ud fra dens analytiske kvalitet, systematik og metodik kan sandsynliggøre, at en sådan trussel er reel og aktuel eller forudsigelig.*
>
> *Endelig er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark er tilstrækkelig dynamisk i karakter til, at logningen ikke herved vil få en systematisk karakter. Der henvises til, at der tidligere har været perioder, hvor truslen mod Danmark har været vurderet anderledes af nationale myndigheder, samt at vurderingen efter Justitsministeriets opfattelse har en kvalitet, systematik og metodik, der sandsynliggør det valgte trusselsniveau, uanset at vurderingen i en årrække har været på samme niveau."*

Det anføres videre, at Vurderingen af Terrortruslen mod Danmark ikke vil stå alene:

> *"Ud over Vurderingen af Terrortruslen mod Danmark, kan også en række andre analyseprodukter udgivet af enten Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center For Cybersikkerhed, belyse en trussel mod Danmarks sikkerhed inden for et specifikt område. Det kunne f.eks. være Center For Cybersikkerheds årlige "Trusselsvurdering 2020: Cybertruslen mod Danmark", men også andre relevante trusselsvurderinger vil kunne indgå.*

Disse analyser vil kunne indgå i en samlet vurdering af truslen mod Danmark, der vil kunne foretages regelmæssigt, så det sikres, at både nationale og internationale forhold af betydning for Danmarks nationale sikkerhed inddrages. Inddragelsen af flere af hinanden uafhængige analyseprodukter vil kunne styrke det vurderingsmæssige grundlag af det samlede trusselsbillede.

Det er således Justitsministeriets vurdering, at der bl.a. på baggrund af Vurderingen af Terrortruslen mod Danmark og øvrige analyseprodukter, kan foretages en velunderbygget vurdering af truslen mod Danmarks nationale sikkerhed med henblik på at konstatere, om der er tilstrækkelige solide grunde til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig."

Under afsnit 3.3.3 om retsgarantier og domstolsprøvelse mv. tages der bl.a. stilling til, hvordan det kan sikres, at afgørelsen, som pålægger teleselskaberne en logningsforpligtelse, kan gøres til genstand for en effektiv domstolsprøvelse. Om efterprøvelsen af grundlaget for trusselsvurderingen hedder det bl.a.:

"Som nævnt ovenfor, forventes Vurderingen af Terrortruslen mod Danmark samt andre uklassificerede efterretningsmæssige analyseprodukter at kunne udgøre grundlaget for vurderingen af, om der er en alvorlig trussel mod den nationale sikkerhed. Justitsministeriets vurdering kan gøres til genstand for en domstolsprøvelse af, om der foreligger en sådan situation, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

Det er Justitsministeriets opfattelse, at detaljeringsgraden i den uklassificerede udgave af Vurderingen af Terrortruslen mod Danmark udgør et tilstrækkeligt sikkert grundlag til, at der kan foretages en effektiv retlig prøvelse af Justitsministeriets vurdering af grundlaget for et pålæg om logning.

Ved domstolsprøvelsen er det alene Justitsministeriets vurdering, der kan efterprøves, da de efterretningsmæssige analyseprodukter i vidt omfang baserer sig på klassificeret materiale. Det kan i den forbindelse nævnes, at der vil være betydelige fordele forbundet med, at prøvelsen sker i en sædvanlig retsproces, hvor den fremlagte dokumentation – i det omfang det vurderes nødvendigt – evt. kan suppleres med vidneforklaringer fra ledende medarbejdere, der kan forklare om metodikken og tilblivelsesprocessen af de konkrete vurderinger mv."

3. ANBRINGENDER

3.1 Logningsbekendtgørelsen er ikke ugyldig (påstand 1)

Det fastholdes, at princippet om EU-rettens forrang ikke fører til, at logningsbekendtgørelsen er hverken helt eller delvist ugyldig. Uanset om eller i hvilket omfang der består en modstrid mellem logningsbekendtgørelsen og EU-retten som fortolket ved La Quadrature-dommen, kan en sådan modstrid ikke føre til, at bekendtgørelsen mister sin gyldighed. Allerede af denne grund kan sagsøgeren ikke få medhold i påstand 1. Der henvises til duplikkens afsnit 3.2.

Der er intet belæg for sagsøgerens anbringender under afsnit 3.5 i processkrift I om, at en modstrid med en EU-regel under særlige omstændigheder kan føre til, at nationale regler mister deres gyldighed. Det er ikke korrekt, at princippet om EU-rettens forrang kan medføre ugyldighed efter *lex superior*-retsgrundsætningen. Sagsøgeren har heller ikke henvist til nogen praksis fra EU-Domstolen, der understøtter dette vidtgående synspunkt.

Selv hvis landsretten måtte finde, at logningsbekendtgørelsen principielt kan være helt eller delvist ugyldig som følge af en konflikt med en EU-retlig regel, fastholdes det, at gyldigheden skal bedømmes i lyset af, at Danmark faktisk aktuelt befinder sig i en situation, hvor en generel og udifferentieret logning i overensstemmelse med logningsbekendtgørelsens kapitel 2 principielt kan opretholdes under visse betingelser.

Sagsøgerne har ikke godtgjort, at hele bekendtgørelsen strider mod EU-retten. På flere punkter er bekendtgørelsen utvivlsomt ikke i modstrid med EU-retten på nuværende tidspunkt, og af denne grund er der ikke grundlag for at tilsidesætte hele bekendtgørelsen som ugyldig i overensstemmelse med sagsøgerens påstand.

Der er intet belæg for at antage, at en bekendtgørelse skulle være et utilstrækkeligt format med den konsekvens, at hele den nuværende bekendtgørelse allerede af den grund er i modstrid med La Quadrature-dommen. Dommen indeholder ingen betragtninger om, at de i præmis 134-139 omtalte "*lovgivningsmæssige foranstaltninger*", herunder påbud, afgørelser m.v., skal have en særlig form eller være særligt individualiserede. Det påhviler de enkelte medlemsstater at tilvejebringe en retsstilling inden for rammerne af deres nationale retssystemer, som er i overensstemmelse med dommens præmisser. En bekendtgørelse udgør en helt sædvanlig lovgivningsmæssig foranstaltning i den danske retsorden og er både et naturligt og fuldt ud tilstrækkeligt middel til at gennemføre retsstillingen.

Det er i øvrigt ikke korrekt, at *"[e]n traditionel dansk forvaltningsretlig forståelse af ordet "afgørelse" fordrer, at en sådan skal bygge på en konkret og individuel vurdering".* Det er tværtimod fast antaget i

dansk forvaltningsret, at en bekendtgørelse og lignende generelle retsakter også er afgørelser i forvaltningsretlig forstand, jf. bl.a. Niels Fenger, Forvaltningsloven, 2020, side 128-129 og 154-156 med yderligere henvisninger.

Det gøres gældende, at det er dokumenteret ved navnlig Vurderingen af terrortruslen mod Danmark fra Center for Terroranalyse, som senest er udkommet i en ny udgave 31. marts 2021 (bilag AL), at der på nuværende tidspunkt består en reel og alvorlig trussel mod den nationale sikkerhed i Danmark. Denne vurdering underbygges yderligere bl.a. af Center for Cybersikkerheds Vurdering af cybertruslen mod Danmark fra juni 2020 (bilag AM). Sagsøgerne har ikke påvist, at disse vurderinger konkret er utilstrækkelige eller fejlbehæftede.

Det gøres videre gældende, at retsgarantierne opstillet i La Quadrature-dommen ikke på nuværende tidspunkt er tilsidesat. Som anført i lovskitsen (bilag 18, side 26ff.) er de nuværende regler om teleudbydernes behandling af loggede oplysninger, herunder de sektorspecifikke databeskyttelsesregler i bekendtgørelse nr. 1882 af 4. december 2020, samt krav om sikkerhedsgodkendelse mv. i bekendtgørelse nr. 1144 af 20. november 2006, tilstrækkelige til at sikre effektiv beskyttelse mod misbrug. Logningsbekendtgørelsen kan ikke anses for i sin helhed at stride mod EU-retten, blot fordi den formelt ikke er tidsbegrænset på nuværende tidspunkt, idet det afgørende er, at grundlaget for en logningsforpligtelse aktuelt er til stede. Grundlaget for logningsforpligtelsen kan endvidere domstolsprøves i overensstemmelse med anvisningerne i lovskitsens afsnit 3.3.3.

Sagsøgeren har i øvrigt fortsat ikke påvist noget grundlag for, at bekendtgørelsens § 5, stk. 1, om lagring af bl.a. IP-adresser, indebærer nogen som helst konflikt med EU-retten, jf. afsnit 3.4 i ministeriets duplik. Også af denne grund kan sagsøgeren ikke få medhold i påstanden om, at hele bekendtgørelsen er ugyldig.

Det kan i øvrigt ikke som anført af sagsøgeren tillægges betydning for muligheden for opretholdelse af en logningsforpligtelse, at bekendtgørelsen ikke aktuelt sondrer mellem logning af oplysninger til brug for efterforskning og retsforfølgning almindelig kriminalitet, grov kriminalitet eller aktiviteter, der truer den nationale sikkerhed. Så længe grundlaget for en logningsforpligtelse i form af en alvorlig trussel mod den nationale sikkerhed er til stede, og de øvrige betingelser og retsgarantier m.v. er opfyldt, kan oplysningerne logges generelt og udifferentieret. Sondringen mellem almindelig kriminalitet, grov kriminalitet og aktiviteter, der truer den nationale sikkerhed, bliver kun relevant ved en efterfølgende adgang til de loggede oplysninger, hvilket i udgangspunktet sker på baggrund af en kendelse.

Tilstrækkeligheden af Justitsministeriets påtænkte fremtidige tiltag er uden betydning for gyldigheden af den nuværende logningsbekendtgørelse. Sagsøgerens kritiske bemærkninger om indholdet i lovskitsen er derfor uden betydning for denne sag.

Det bestrides, at præmis 213-228 i La Quadrature-dommen har nogen betydning for gyldigheden af logningsbekendtgørelsen i perioden frem til national ret er bragt i fuld overensstemmelse med dommen, jf. afsnit 3.3 i sagsøgerens processkrift I. Disse præmisser vedrører spørgsmålet om, hvorvidt en national domstol er beføjet til at fortsætte med at anvende nationale regler, der strider mod EU-retten, i en midlertidig periode. De vedrører ikke spørgsmålet om, hvorvidt sådanne nationale regler mister deres gyldighed. Som beskrevet i duplikken har justitsministeren allerede tilkendegivet, at visse dele af logningsbekendtgørelsen strider mod EU-retten og ikke kan håndhæves, før reglerne er ændret. Dette er fuldt ud i overensstemmelse med præmis 213-228 i dommen.

3.2 Justitsministeriet har handlet og handler fortsat hurtigst muligt for at bringe den danske retsstilling i overensstemmelse med EU-retten (påstand 2)

Det fastholdes, at Justitsministeriet har handlet og fortsat handler hurtigst muligt for at bringe den danske retsstilling i overensstemmelse med EU-retten.

Det bestrides, at Digital Rights-dommen i sig selv udløste en forpligtelse til at tilpasse national ret hurtigst muligt. Dommen efterlod en række væsentlige spørgsmål ubesvaret, herunder navnlig spørgsmålet om, hvorvidt en generel og udifferentieret logningsforpligtelse kunne opretholdes, så længe adgangen til de loggede oplysninger var underlagt tilstrækkelige garantier – såsom et proportionalitetskriterie og krav om dommerkendelse som i dansk ret, jf. retsplejelovens kapitel 74 sammenholdt med kapitel 71.

Sagsøgerens citater fra samrådet i Retsudvalget den 2. marts 2017 og udsættelsen af revisionen af reglerne den 26. april 2017 efter Tele2-dommen illustrerer netop – modsat hvad sagsøgeren hævder – at retstilstanden på området har gennemgået en sådan udvikling, at det savner mening at hævde, at den på noget tidspunkt hidtil har været klar. Det dengang anførte om, at EU-retten var til hinder for en generel og udifferentieret logning, er nemlig ikke længere retvisende i lyset af La Quadrature-dommen.

Det skal understreges, at forløbet fra Digital Rights-dommen til La Quadrature-dommen har været helt usædvanligt. I alt 15 medlemsstater, inklusive Danmark, har afgivet indlæg i La Quadrature-sagen og sammen med Kommissionen samstemmende anmodet Domstolen om at genoverveje balancen mellem behovet for beskyttelse af de grundlæggende rettigheder efter EU-retten og behovet for loggede oplysninger til opklaring af forbrydelser mv.

Der verserer på nuværende tidspunkt stadigvæk fem sager for EU-Domstolen om uafklarede spørgsmål relateret til logning (C-339/20 og 397/20 - VD m.fl., C-140/20 - Commissioner of the Garda Síochána and Others, og C-793/19 og C-794/19 - SpaceNet m.fl.). Det bemærkes, at disse sager verserer for EU-Domstolen uagtet, at der er faldet dom i La Quadrature-sagen, idet denne dom ikke anses at have besvaret

alt vedrørende staternes pålæg til teleudbyderne om at foretage generel og udifferentieret logning. Reaktionerne på Tele2-dommen og La Quadrature-dommen i de øvrige EU-medlemslande er stærkt varierende og fragmenteret og bærer klart præg af, at der endnu ikke er fundet en gennemgående linje for, hvordan retsstillingen kan indrettes i overensstemmelse med EU-retten.

I oversigtsform er Justitsministeriet navnlig bekendt med følgende landes logningsregler og reaktioner på dommene:

- I Belgien stilles der krav om logning af teledata (trafik- og lokaliseringsdata) i 12 måneder. Efter Justitsministeriets oplysninger er reglerne ikke suspenderet efter La Quadrature-dommen, men Belgien afsøger i øjeblikket mulighederne for ny lovgivning. Der afventes ligeledes dom fra deres nationale forfatningsdomstol i sagen, der var genstand for La Quadrature-dommen.

- I Frankrig stilles der krav om logning af teledata (trafik- og lokaliseringsdata) i op til 1 år. Frankrig har oplyst til Justitsministeriet, at der efter La Quadrature-dommen ikke er sket suspension af de nationale regler, idet Frankrig anser, at en sådan suspension vil vanskeliggøre politi- og juridisk arbejde på kriminalitetsområdet. Der afventes ligeledes dom fra deres statsråd (Conseil d'État) i sagen, der var genstand for La Quadrature-dommen.

- I Nederlandene er der på nuværende tidspunkt ingen specifikke lovkrav om logning, idet de tidligere regler blev suspenderet som følge af nationale domsafsigelser efter EU-Domstolens afgørelse i Digital Rights-sagen i 2014. Efter Justitsministeriets oplysninger forbereder Nederlandene nye regler. Forberedelsen af reglerne har tidligere været indstillet som følge af EU-Domstolens domme.

- I Irland stilles der fortsat krav om logning af teledata i en periode på 2 år. Kravet gælder trafik- og lokaliseringsdata. Irland har over for Justitsministeriet oplyst, at der ikke er sket suspension af de nationale regler, og at der forventes ny lovgivning, når der er endelig dom i den irske sag, der er forelagt præjudicielt for EU-Domstolen (C-140/20 - Commissioner of the Garda Síochána and Others).

- I Sverige skete der efter Tele2-dommen en tilpasning af logningsreglerne, som trådte i kraft den 1. oktober 2019. Reglerne er baseret på en begrænset og differentieret tilgang baseret på typen af teledata, men oplysningerne logges som udgangspunkt for alle mobiltelefonbrugere. Sverige vurderer umiddelbart, at reglerne fortsat er i overensstemmelse med EU-retten efter La Quadrature-dommen, men følger med interesse også bl.a. EU-Domstolens afgørelse i SpaceNet m.fl.-sagen.

- I Tyskland blev der i 2015 vedtaget regler, der – ligesom i Sverige – er baseret på en generel og udifferentieret pligt til at logge trafik- og lokaliseringsdata, men er begrænset i tid og omfang både

med hensyn til hvilken type data, der skal logges, og hvor længe. Der verserer imidlertid en sag om foreneligheden af det tyske retsgrundlag med EU-retten, som er blevet forelagt præjudicielt for EU-Domstolen (C-793/19 og C-794/19 - SpaceNet m.fl.). På grund af de verserende tyske sager meddelte den tyske netværksstyrelse (Bundesnetzagentur) den 28. juni 2017, at man, indtil der forelå en retsgyldig afgørelse, ville suspendere håndhævelsen af reglerne og øvrige tiltag for så vidt angår logning, herunder ikke udstede bøder for manglende efterlevelse.

- I Østrig blev den tidligere lovgivning vedrørende logning underkendt af forfatningsdomstolen i 2014 som følge af Digital Rights-sagen. Den 1. juni 2018 trådte en ny lov i kraft, som indebærer målrettet hastesikring på baggrund af en indledende mistanke (såkaldt "quick freeze").

Det fastholdes på denne baggrund som anført i afsnit 6.2.2 i svarskriftet, at tilpasningen af retsstillingen har frembudt sådanne ekstraordinære faktiske og retlige vanskeligheder, at Justitsministeriet har handlet og fortsat handler hurtigst muligt. Dommen i La Quadrature-sagen understøtter, at det ikke giver reel mening at bruge Tele2-dommen som målestok for denne forpligtelse. Justitsministeriet har indtil nu iværksat alle nødvendige og tilstrækkelige tiltag som opfølgning på La Quadrature-dommen, og der kan derfor ikke på nuværende tidspunkt gives sagsøgerne medhold i påstand 2.

3.3 Øvrige forhold

Sagsøgerens bemærkninger under afsnit 3.4 er uden betydning for nærværende sag. Spørgsmålet om, hvorvidt teleselskabernes behandling af loggede oplysninger er i overensstemmelse med databeskyttelsesreglerne, er uden betydning for gyldigheden af selve logningsbekendtgørelsen (påstand 1), eller for spørgsmålet om, hvorvidt Justitsministeriet har handlet hurtigst muligt (påstand 2).

Det bemærkes dog, at Justitsministeriet fastholder, at teleselskabernes behandling af loggede teleoplysninger er i overensstemmelse med databeskyttelsesforordningen. Der henvises til bilag 21.

København, den 21. april 2021

Rass Holdgaard
Partner, Advokat (H)

EKSTRAKT – BIND II – BILAG

I sagen for

Østre Landsret, 16. afdeling

BS-36799/2018-OLR

Foreningen imod Ulovlig Logning
Birkegade 15, 5. tv.
2200 København N
advokat Julie Bak-Larsen i henhold til proceduretilladelse
(”Sagsøger”)

mod

Justitsminister Nick Hækkerup
Justitsministeriet
Slotholmsgade 10
1216 København K
advokat Rass Holdgaard
("Sagsøgte")

Sagen hovedforhandles den 5. maj 2021, kl. 9.30-15, og den 6. maj 2021, kl. 9.30-12.

INDHOLDSFORTEGNELSE

BILAG 11

Bird & Bird
Advokatpartnerselskab
Sundkrogsgade 21
2100 Copenhagen
Tel +45 72 24 12 12
Fax +45 72 24 12 13
twobirds.com

Medlemsliste for Forening imod ulovlig logning

Virksomheder og organisationer

- **Greenspeak -** CVR: 35851011
- **PROSA - Forbundet af It-profesionelle –** CVR: 39628228
- **Ordforsyningen –** CVR: 34538298
- **Nikobojs Web & Software –** CVR: 38273965
- **Rubech ApS** - CVR: 27231640
- **Amok Marketing ApS** - CVR: 33260369
- **SHH Consult** - CVR: 32181287

Privatpersoner

- **Alberte Korshagen Welikala Langebæk**
- **Alexander Welsch Carlsen**
- **Allan Greve**
- **Amalie Corvinius Jakobsen**
- **Anders Kresten Kousgaard**
- **Anders Krogh Jensen**
- **Anne-Marie Krogsbøll**
- **Bjørn Amdi Sloth**
- **Bjarne D Mathiesen**
- **Bjørn Amdi Sloth**
- **Bertram Stæhr von Undall**
- **Bjørn Hansen**

- **Bror Tao Sjørslev Bojlén**
- **Christian Holm**
- **Carsten Plith Andersen**
- **Casper Qvortrup**
- **Christian Krogh Schubert**
- **Christoffer Hare Buchholz**
- **Dennis Fris Kuhlmann**
- **Dennis Eriksen**
- **Erik Brøndum Holstborg**
- **Eiliv Haugland**
- **Eric Kenworthy**
- **Elmo Johannes Grube Due**
- **Emil Evald Johanse**
- **Flemming Leer Jakobsen**
- **Frank Andersen**
- **Gunnar Isholm Simonsen**
- **Hans-Henrik Johansen Larsson**
- **Helle Hinge**
- **Henning Wangerin**
- **Henrik Bitsch Kirk**
- **Henrik Jacobsen**
- **Henrik Olsen**
- **Inger Langhorn**
- **Inge Ørum Petersen**
- **Ivan Al-Hilali**
- **Jacob Andersen**

- **Jakob Hoffmeyer Tougård**
- **Jacob Ringmann Madsen**
- **Jan Irgens**
- **Jan Nielsen**
- **Jens Jørgen Madsen Lind**
- **Jens Vest-Jensen**
- **Jesper Andersen**
- **Jesper Rou Larsen**
- **Jesper Rubech Rasmussen**
- **Jim Bernbom Wolff**
- **Jimmie Lemvigh Jensen**
- **Johan Taarnskov Aabech**
- **Johny Woller Skovdal**
- **Jonas Bo Jalling**
- **Jonas christensen**
- **Julian Bybeck Tosev**
- **Jørgen Bonde Jensen**
- **Jørgen Brandt**
- **Jørgen Nørgaard**
- **Kim N. H. Nguyen**
- **Kim Osbøl**
- **Kim Schulz**
- **Kim Vagn Jakobsen**
- **Kirstine Askholm**
- **Knud Haugmark**
- **Kristine Frisenfeldt Horn**

- **Lama Tendar Olaf Høyer**
- **Lars Christian Remmen**
- **Lars Damgaard Petersen**
- **Lars Slouborg Bengtsson**
- **Lasse Heimann Larsen**
- **Lene Hansen**
- **Line Rosendahl Meldgaard Pedersen**
- **Line Schmidt Sørensen**
- **Lisa Jörgensen**
- **Lukas Frimer Tholander**
- **Mads Jønsson**
- **Marc Nyholm**
- **Mathias Gigas**
- **Martin Philip Topholm**
- **Mathias Nørup Hall-Andersen**
- **Michael Overlund Knudsen**
- **Mikael Barfred**
- **Mikkel Arent**
- **Mikkel Morgen Mark**
- **Morten Grue Sørensen**
- **Morten Skov Bendtsen**
- **Morten Wulff**
- **Nicki Kristensen**
- **Nicolai Zimling Fich**
- **Niels Erdman Thomsen**
- **Niels Holmgård Andersen**

- **Nils Ververs Lübke**
- **Nini Nielsen Kerckhoffs**
- **Patrick Boisen**
- **Patrick Hassing Sørensen**
- **Pelle Midjord Persson**
- **Peter Brinck Lykke Jørgensen**
- **Peter Jensen**
- **Peter Vang Johansen**
- **Philip Thinggaard**
- **Rasmus Lau Petersen**
- **Rasmus Underbjerg Pinnerup**
- **Rasmus Worup Rørbæk**
- **Rune Juhl Jacobsen**
- **Rune Schjellerup Philosof**
- **Sanne Hardis Jensen**
- **Sean Gregory Bronée**
- **Simon Kyrin Toft**
- **Simon Pagh Clausen**
- **Sofus Emil Albertsen**
- **Steen Garbers Enevoldsen**
- **Steen Theis Lund Meyer**
- **Steffen Holst Holmvard**
- **Sune Rievers Jensen**
- **Svend Erik Christensen**
- **Svend Skipper Andersen**
- **Søren Bredlund Caspersen**

- **Søren Møller-Larsson**
- **Thomas Bang Toft**
- **Thomas Bech-Thomassen**
- **Thomas Larsen**
- **Thomas Mejer**
- **Tom Tækker**
- **Tue Haulund**
- **Ulrik Borgermann**
- **William John Gauthier**
- **Yvonne Selma Mogensen**
- **Øyvind Mo**

Bilag 1

Vedtægter

Foreningen imod Ulovlig Logning

Cvr.-nr.

1. Navn og hjemsted

1.1
Foreningens navn er ” Foreningen imod Ulovlig Logning”.

1.2
Foreningens hjemsted er København.

2. Formål

2.1
Foreningens formål er at forberede, koordinere og støtte, herunder økonomisk, sagsanlæg ved danske domstole med det formål af få kendt logningsbekendtgørelsen ulovlig.

2.2
Foreningen kan, med henblik på varetagelse af foreningens formål, optræde som sagsøger i forbindelse med sagsanlæg, eller som biintervenient.

3. Medlemmer og støttemedlemmer

3.1
Som medlem af foreningen kan optages enhver fysisk eller juridisk person, herunder andre foreninger, der ønsker at medvirke til at opnå foreningens formål.

3.3
Bestyrelsen kan afvise en indmeldelse eller slette en indmeldt, hvis medlemmet ikke inden for en af bestyrelsen fastsat frist præsterer en efter bestyrelsens skøn tilfredsstillende dokumentation for opfyldelse af medlemsbetingelserne.

3.4
Bestyrelsen kan ved enstemmig beslutning ekskludere et medlem, som modarbejder Foreningens formål, eller hvis medlemskab er egnet til at forringe foreningens anseelse.

4. Kontingent

4.2
Om nødvendigt opkræves af foreningens medlemmer et årligt medlemskontingent. Dette fastsættes i så fald af generalforsamlingen for hvert kalenderår og indbetales senest 2 måneder efter påkrav fra foreningen. Finder indbetalingen ikke sted inden denne frist, ekskluderes restanten fra foreningen, med mindre bestyrelsen træffer anden bestemmelse.

5. Juridisk rådgiver

5.1
Bestyrelsen antager advokat Martin von Haller Grønbæk fra Bird & Bird Advokatpartnerselskab som juridisk rådgiver, der på foreningens vegne repræsenterer foreningen og dens medlemmer.

6. Ledelse

6.1
Foreningen ledes af en bestyrelse på 5 medlemmer.

6.2
Bestyrelsen fastsætter en forretningsorden og vælger en talsperson.

6.3
Bestyrelsesmedlemmer valgt af generalforsamlingen vælges for en periode på 2 år ad gangen. Genvalg er muligt. Det er muligt at vælge/indstille suppleanter.

6.4
Bestyrelsens beslutninger træffes ved almindelig stemmeflerhed, med mindre andet fremgår af vedtægterne.

6.5
Den juridiske rådgiver kan ikke besidde en plads i foreningens bestyrelse, men kan dog undtagelsesvist, f.eks. grundet administrative forhold eller andet, sidde i foreningens bestyrelse på kortvarigt basis.

6.6
Bestyrelsesmøder afholdes så ofte som talspersonen finder det hensigtsmæssigt. Ethvert medlem af bestyrelsen eller den juridiske rådgiver kan dog indkalde til bestyrelsesmøde. Indkaldelse til bestyrelsesmøde skal ske med mindst 7 dages varsel.

6.7
Bestyrelseshvervet er ulønnet, men foreningen dækker bestyrelsens direkte udgifter i forbindelse med hvervet.

7. Generalforsamling

7.1
Foreningens højeste myndighed er generalforsamlingen.

7.2
Indkaldelse til generalforsamling sker ved e-mail eller brev med vedlagt dagsorden til samtlige foreningens medlemmer med mindst 14 dages varsel.

7.3
Forslag, der ønskes behandlet på generalforsamlingen, skal være meddelt foreningens talsperson senest 7 dage før generalforsamlingen.

7.4
Hvert medlem har én (1) stemme på generalforsamlingen. Medlemmer, der er i kontingentrestance, har dog ikke stemmeret.

7.5
Medlemmer kan møde ved en fuldmægtig. Fuldmagten skal i så fald være skriftlig og dateret.

7.6
Beslutninger træffes ved simpelt stemmeflertal blandt de på generalforsamlingen repræsenterede medlemmer.

7.7
Forslag om ændring af foreningens vedtægter eller opløsning af foreningen kan dog alene vedtages med 2/3 flertal blandt de på generalforsamlingen repræsenterede medlemmer.

8. Ordinær generalforsamling

8.1
Der afholdes ordinær generalforsamling hvert år i marts, første gang marts 2020.

8.2
På den ordinære generalforsamling skal dagsordenen indeholde følgende punkter:

a) Valg af dirigent
b) Beretning fra bestyrelsen og den juridiske rådgiver
c) Godkendelse af regnskabet for det forløbne år
d) Behandling af indkomne forslag
e) Fastsættelse af kontingent
f) Valg af bestyrelsesmedlemmer
g) Valg af revisor
h) Eventuelt

9. Ekstraordinær generalforsamling

9.1
Der afholdes ekstraordinær generalforsamling, når dette forlanges af et medlem af foreningens bestyrelse, revisor, den juridiske rådgiver eller mindst 25 medlemmer af foreningen.

9.2
Anmodning om afholdelse af ekstraordinær generalforsamling skal være ledsaget af en begrundet angivelse af de punkter, der ønskes behandlet på den ekstraordinære generalforsamling.

9.3
Bestyrelsen skal indkalde til ekstraordinær generalforsamling senest fjorten (14) dage efter, der er fremsat berettiget krav herom.

10. Hæftelse

10.1
Foreningens medlemmer eller bestyrelse hæfter ikke for foreningens forpligtelser.

10.2
For foreningens forpligtelser hæfter alene foreningen, med dennes til enhver tid hørende formue.

11. Regnskab og revision

11.1
Foreningens regnskabsår følger kalenderåret.

11.2
Regnskabet skal revideres.

12. Tegningsregel

12.1
Foreningen tegnes af bestyrelsens talsperson i forening med et bestyrelsesmedlem eller af 3 bestyrelsesmedlemmer.

13. Opløsning

13.1
Ved foreningens opløsning uddeles dens eventuelle nettoformue til en velgørende organisation med samme formål som foreningen. Det kan være en forening som er stiftet mhp. at sagsøge stat eller anden magthaver for at beskytte borgernes rettigheder, herunder især retten til privatliv. Alternativt en forening eller organisation der på anden vis arbejder for at beskytte og udbrede kendskabet til borgernes rettigheder.

Lovforslag nr. L 35. Fremsat den 13. december 2001 af justitsministeren (Lene Espersen)

Forslag

til

Lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme mv.)

§ 1

I straffeloven, jf. lovbekendtgørelse nr. 808 af 14. september 2001, foretages følgende ændringer:

1. I *§ 27, stk. 1,* indsættes som *2. pkt.*:

»For så vidt angår straf for forsøg finder § 21, stk. 3, tilsvarende anvendelse.«.

2. I *§ 77 a* indsættes efter *1. pkt.*:

»Der kan under samme betingelser ske konfiskation af andre formuegoder, herunder penge.«.

3. I *§ 93, stk. 1, nr. 1,* indsættes som *2. pkt.*:

»2. led gælder dog ikke for juridiske personer.«.

4. *§ 114* affattes således:

»**§ 114.** For terrorisme straffes med fængsel indtil på livstid den, som med forsæt til at skræmme en befolkning i alvorlig grad, eller uretmæssigt at tvinge danske eller udenlandske offentlige myndigheder eller en international organisation til at foretage eller undlade at foretage en handling, eller at destabilisere eller ødelægge et lands eller en international organisations grundlæggende politiske, forfatningsmæssige, økonomiske eller samfundsmæssige strukturer begår en eller flere af følgende handlinger, når handlingen i kraft af dens karakter eller den sammenhæng, hvori den begås, kan tilføje et land eller en international organisation alvorlig skade:

1) Manddrab efter § 237.
2) Grov vold efter § 245 eller § 246.
3) Frihedsberøvelse efter § 261.
4) Forstyrrelse af trafiksikkerheden efter § 184, stk. 1, retsstridige forstyrrelser i driften af almindelige samfærdselsmidler mv. efter § 193, stk. 1, eller groft hærværk efter § 291, stk. 2, hvis disse overtrædelser begås på en måde, der kan bringe menneskeliv i fare eller forårsage betydelige økonomiske tab.
5) Kapring af transportmidler efter § 183 a.
6) Grove våbenlovsovertrædelser efter § 192 a eller lov om våben og eksplosivstoffer § 10, stk. 2.
7) Brandstiftelse efter § 180, sprængning, spredning af skadevoldende luftarter, oversvømmelse, skibbrud, jernbane- eller anden transportulykke efter § 183, stk. 1 og 2, sundhedsfarlig forurening af vandforsyningen efter § 186, stk. 1, sundhedsfarlig forurening af ting bestemt til almindelig udbredelse mv. efter § 187, stk. 1.

Stk. 2. På samme måde straffes den, som med det i stk. 1 nævnte forsæt transporterer våben eller eksplosivstoffer.

Justitsmin., Lovafd., j.nr. 2001-730-0466

Stk. 3. Endvidere straffes på samme måde den, der med det i stk. 1 nævnte forsæt truer med at begå en af de i stk. 1 og 2 nævnte handlinger.«.

5. Efter *§ 114* indsættes:

»**§ 114 a.** Med fængsel indtil 10 år straffes den, som

1) direkte eller indirekte yder økonomisk støtte til,
2) direkte eller indirekte tilvejebringer eller indsamler midler til, eller
3) direkte eller indirekte stiller penge, andre formuegoder, eller finansielle eller andre lignende ydelser til rådighed for

en person, en gruppe eller en sammenslutning, der begår eller har til hensigt at begå terrorhandlinger omfattet af § 114.

§ 114 b. Den, som i øvrigt ved tilskyndelse, råd eller dåd medvirker til at fremme den kriminelle virksomhed eller det fælles formål for en gruppe eller sammenslutning, som foretager en eller flere handlinger omfattet af § 114 eller § 114 a, nr. 1 eller 2, når virksomheden eller formålet indebærer, at en eller flere handlinger af denne karakter begås, straffes med fængsel indtil 6 år.

§ 114 c. Den, som, uden at forholdet omfattes af §§ 114-114 b, deltager i eller yder væsentlig økonomisk støtte eller anden væsentlig støtte til korps, gruppe eller sammenslutning, der har til hensigt ved magtanvendelse at øve indflydelse på offentlige anliggender eller fremkalde forstyrrelse af samfundsordenen, straffes med fængsel indtil 6 år.

§ 114 d. Den, som, uden at forholdet omfattes af §§ 114-114 c, deltager i en ulovlig militær organisation eller gruppe, straffes med bøde eller fængsel indtil 4 måneder eller under skærpende omstændigheder med fængsel indtil 2 år.

§ 114 e. Med fængsel indtil 6 år straffes den, der under skærpende omstændigheder i strid med lovgivningen om ikke spredning af masseødelæggelsesvåben mv.

1) udfører produkter med dobbelt anvendelse uden tilladelse,
2) til brug for myndighedernes afgørelser om produkter med dobbelt anvendelse giver urigtige eller vildledende oplysninger eller fortier oplysninger af betydning for sagens afgørelse, eller
3) handler i strid med vilkår, der er fastsat i myndighedernes afgørelser om produkter med dobbelt anvendelse.«.

6. *§ 183 a* affattes således:

»**§ 183 a.** Den, som om bord i et luftfartøj, skib samt andet kollektivt transportmiddel eller godstransportmiddel ved ulovlig tvang, jf. § 260, overtager kontrollen over fartøjet eller køretøjet eller griber ind i dettes manøvrering, straffes med fængsel indtil livstid.«.

7. I *§ 192 a* ændres »fængsel indtil 4 år« til: »fængsel indtil 6 år«.

8. I *§ 192 a* indsættes som *stk. 2.*:

»*Stk. 2.* På samme måde straffes den, der i strid med lovgivningen om våben og eksplosivstoffer udvikler eller med henblik herpå forsker i faste stoffer, væsker eller luftarter, som ved spredning virker skadevoldende, bedøvende eller irriterende.«.

9. *§ 306* affattes således:

»**§ 306.** Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i 5. kapitel for overtrædelse af denne lov.«.

§ 2

I lov om rettens pleje, jf. lovbekendtgørelse nr. 809 af 14. september 2001, foretages følgende ændringer:

1. Overskriften til kapitel 71 affattes således:
»Indgreb i meddelelseshemmeligheden, observation og dataaflæsning«.

2. I *§ 786, stk. 1,* udgår: »offentlige«.

3. I *§ 786* indsættes efter *stk. 3* som nye stykker:

»*Stk. 4.* Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med ministeren for videnskab, teknologi og udvikling nærmere regler om denne registrering og opbevaring.

Stk. 5. Justitsministeren kan efter forhandling med ministeren for videnskab, teknologi og udvikling fastsætte regler om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Stk. 6. Overtrædelse af stk. 4, 1. pkt., straffes med bøde. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 7. For overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af stk. 4, 2. pkt., og stk. 5, kan der fastsættes bestemmelser om bødestraf. Der kan endvidere fastsættes bestemmelser om at pålægge selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.«.

Stk. 4 bliver herefter stk. 8.

4. Efter *§ 791 a* indsættes:

»**§ 791 b.** Aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning) kan foretages, såfremt

1) der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3,
2) indgrebet må antages at være af afgørende betydning for efterforskningen, og
3) efterforskningen angår en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af straffelovens §§ 180, 183, stk. 1 og 2, 183 a, 186, stk. 1, 187, stk. 1, 191, 192 a eller 237.

Stk. 2. Indgreb som nævnt i stk. 1 må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.

Stk. 3. Afgørelse om dataaflæsning træffes af retten ved kendelse. I kendelsen angives det informationssystem, som indgrebet angår. I øvrigt finder reglerne i § 783, stk. 1, 3. og 4. pkt., samt stk. 2 og 3, tilsvarende anvendelse.

Stk. 4. Efterfølgende underretning om et foretaget indgreb sker efter reglerne i § 788, stk. 1, 3 og 4. Underretningen gives til den, der har rådigheden over det informationssystem, der har været aflæst efter stk. 1. I øvrigt finder reglerne i § 782, stk. 2, §§ 784-785, § 789 samt § 791 tilsvarende anvendelse.«.

5. *§ 799, stk. 1, 1. pkt.,* affattes således:

»Såfremt det er af afgørende betydning for efterforskningen, at ransagningen foretages, uden at den mistænkte eller andre gøres bekendt hermed, kan retten, hvis efterforskningen angår en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af straffelovens §§ 180, 183, stk. 1 og 2, 183 a, 186, stk. 1, 187, stk. 1, 191, 192 a eller 237, ved kendelse træffe bestemmelse herom og om, at reglerne i § 798, stk. 2, 1.-4. pkt., og stk. 3, fraviges.«.

6. I *§ 799* indsættes som stk. 3:

»*Stk. 3.* Retten kan bestemme, at der inden for det tidsrum, der efter stk. 2 fastsættes i medfør af § 783, stk. 2, kan foretages gentagne ransagninger. Retten skal i den forbindelse fastsætte antallet af ransagninger. Hvis særlige grunde taler derfor, kan retten bestemme, at der kan foretages et ubestemt antal ransagninger.«.

7. I *§ 802, stk. 2, nr. 2, § 805, stk. 3,* og *§ 807 d, stk. 2, 1. pkt.,* ændres »og § 76 a, stk. 5,« til: »§ 76 a, stk. 5, og § 77 a, 2. pkt.,«.

8. I *§ 803, stk. 1,* indsættes efter *1. pkt.:*

»Andre formuegoder, herunder penge, som en person, der ikke er mistænkt, har rådighed over, kan beslaglægges som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, hvis der er grund til at antage, at disse formuegoder bør konfiskeres.«.

9. I *§ 806, stk. 3, 1. pkt.,* indsættes efter »kan politiet træffe beslutning om beslaglæggelse«: »og om edition«.

10. I *§ 807 b, stk. 1,* og *§ 807 d, stk. 1, 1. pkt.,* ændres »§ 803, stk. 1,« til: »§ 803, stk. 1, 1. pkt.,«.

11. I *§ 807 b, stk. 2,* og *§ 807 d, stk. 2, 1.pkt.,* indsættes efter »§ 802, stk. 2,«: »og § 803, stk. 1, 2. pkt.,«.

§ 3

I lov nr. 418 af 31. maj 2000 om konkurrence- og forbrugerforhold på telemarkedet foretages følgende ændringer:

1. *§ 15, stk. 3,* ophæves.

2. I *§ 34, stk. 5,* indsættes efter »den offentlige alarmtjeneste«: »eller politiet«.

§ 4

I lov om våben og eksplosivstoffer, jf. lovbekendtgørelse nr. 67 af 26. januar 2000, som ændret ved § 23 i lov nr. 433 af 31. maj 2000, foretages følgende ændring:

1. I *§ 5, 1. pkt.,* indsættes efter »tilvirke«: »og udvikle eller med henblik herpå forske i«.

§ 5

I lov om udlevering af lovovertrædere, jf. lovbekendtgørelse nr. 110 af 18. februar 1998, som ændret ved § 4 i lov nr. 280 af 25. april 2001, foretages følgende ændringer:

1. *§ 2* affattes således:

»**§ 2.** Udlevering af en dansk statsborger til strafforfølgning i en medlemsstat i Den Europæiske Union kan ske,

1) hvis den pågældende i de sidste 2 år forud for den strafbare handling har haft bopæl i den stat, hvortil udlevering ønskes, og en handling, der svarer til den lovovertrædelse, for hvilken der søges udlevering, efter dansk ret kan straffes med fængsel i mindst 6 måneder, eller
2) hvis handlingen efter dansk ret kan medføre højere straf end fængsel i 4 år.

Stk. 2. Justitsministeren kan på grundlag af en overenskomst med en anden stat fastsætte, at danske statsborgere kan udleveres til strafforfølgning i den pågældende stat, hvis handlingen, for hvilken der søges udlevering, efter dansk ret kan straffes med fængsel i mindst 1 år, og betingelserne i stk. 1 i øvrigt er opfyldt.

Stk. 3. Gælder der i forhold til en anden stat ikke en af de i stk. 2 nævnte overenskomster, kan justitsministeren træffe beslutning om udlevering af en dansk statsborger til strafforfølgning, hvis betingelserne i stk. 2, jf. stk. 1, er opfyldt, og særlige hensyn til retshåndhævelsen i øvrigt taler derfor.« .

2. Efter *§ 2* indsættes:

»**§ 2 a.** Udlevering af en udlænding til strafforfølgning eller til fuldbyrdelse af en dom i en medlemsstat i Den Europæiske Union kan ske, hvis en handling, der svarer til den lovovertrædelse, for hvilken der søges udlevering, efter dansk ret kan straffes med fængsel i mindst 6 måneder. Udlevering af en udlænding til andre stater kan kun ske, hvis handlingen efter dansk ret kan straffes med fængsel i mindst 1 år. Kan handlingen efter dansk ret medføre kortere fængselsstraf, kan udlevering dog ske, hvis der er overenskomst herom med den pågældende stat.«.

3. *§ 3, stk. 1,* ophæves.

Stk. 2-5 bliver herefter stk. 1-4.

4. I *§ 3, stk. 3, nr. 1,* der bliver *stk. 2, nr. 1,* ændres »frihedsstraf« til: »fængsel«.

5. I *§ 3, stk. 4,* der bliver *stk. 3,* ændres »betingelserne i stk. 1-3« til: »betingelserne i § 2, § 2 a og § 3, stk. 1 og 2,«.

6. *§ 5, stk. 3 og 4,* ophæves, og i stedet indsættes:

»*Stk. 3.* Stk. 1 og 2 finder ikke anvendelse, når handlingen er omfattet af

1) artikel 1 eller 2 i den europæiske konvention om bekæmpelse af terrorisme,
2) artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af terrorbombninger, eller
3) artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af finansiering af terrorisme.«.

7. I *§ 13* og *§ 19, stk. 1,* ændres »og kapitel 75 b om beslaglæggelse« til: », kapitel 74 om beslaglæggelse og edition samt kapitel 75 a om andre efterforskningsskridt«.

§ 6

I lov nr. 27 af 3. februar 1960 om udlevering af lovovertrædere til Finland, Island, Norge og Sverige, som ændret ved lov nr. 251 af 12. juni 1975 og § 5 i lov nr. 433 af 31. maj 2000, foretages følgende ændring:

1. I *§ 11, 1. pkt.,* og *§ 16, stk. 1, 1. pkt.,* ændres »og 74 om beslaglæggelse og edition« til: », 74 om beslaglæggelse og edition samt 75 a om andre efterforskningsskridt«.

§ 7

Stk. 1. Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende, jf. dog stk. 2. § 5, nr. 1-6, finder anvendelse på anmodninger om udlevering, der fremsættes efter lovens ikrafttræden.

Stk. 2. Justitsministeren fastsætter tidspunktet for ikrafttrædelsen af retsplejelovens § 786, stk. 4 og 6, som affattet ved denne lovs § 2, nr. 3.

Stk. 3. § 5, stk. 3, nr. 3, i lov om udlevering af lovovertrædere, som affattet ved denne lovs § 5, nr. 6, finder først anvendelse på anmodninger om udlevering, der fremsættes efter, at FN-konventionen til bekæmpelse af finansiering af terrorisme er trådt i kraft mellem Danmark og vedkommende fremmede stat.

§ 8

Justitsministeren fremsætter i folketingsåret 2005-06 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.

§ 9

Stk. 1. Loven gælder ikke for Færøerne og Grønland.

Stk. 2. § 1 kan ved kongelig anordning helt eller delvist sættes i kraft for Færøerne med de afvigelser, som de særlige færøske forhold tilsiger.

Stk. 3. § 5 kan ved kongelig anordning helt eller delvist sættes i kraft for Færøerne og Grønland med de afvigelser, som de særlige færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

1.1. Regeringens samlede lovgivningsinitiativer mod terrorisme

Terrorangrebene mod USA den 11. september 2001 gav anledning til, at der blev foretaget en nærmere vurdering af, om dansk lovgivning er tilstrækkelig til at sikre en effektiv indsats mod terrorisme. Denne vurdering har resulteret i en række forskellige lovgivningsinitiativer, som alle er rettet mod terrorisme. Lovgivningsinitiativerne, der er samlet i en fælles »anti-terrorpakke«, omfatter lovforslag fra ministeren for flygtninge, indvandrere og integration, økonomi- og erhvervsministeren, skatteministeren og justitsministeren. Lovforslagene, der vil blive fremsat af de respektive ministre, indeholder i hovedtræk følgende ændringer, idet der i øvrigt henvises til de pågældende lovforslag.

Lovforslaget, der fremsættes af ministeren for flygtninge, indvandre og integration, indeholder ændringer af udlændingeloven, der har til formål at sikre de nødvendige tiltag på udlændingeområdet som en del af regeringens samlede initiativer mod terrorisme. Forslaget har bl.a. til formål at gennemføre en række ændringer af udlændingeloven i lyset af FN's Sikkerhedsråds resolution nr. 1373 (2001).

Et andet væsentligt formål med lovforslaget er at styrke samarbejdet mellem Politiets Efterretningstjeneste og udlændingemyndighederne i asylsager og i andre sager om opholdstilladelse i Danmark ved at skabe adgang til udveksling af oplysninger myndighederne imellem i videre omfang, end det er tilfældet i dag. Forslaget skal blandt andet sikre anvendelsen af adgangen til at nægte opholdstilladelse til udlændinge, når det er påkrævet af hensyn til statens sikkerhed.

Flere af de problemstillinger, der behandles i lovforslaget, gør sig også gældende i forbindelse med meddelelse af dansk indfødsret ved naturalisation. Efter grundlovens § 44, stk. 1, sker naturalisation ved lov, og de nærmere betingelser for erhvervelse af dansk indfødsret ved naturalisation er fastlagt ved et forlig mellem et bredt flertal af Folketingets partier. Disse betingelser er beskrevet i cirkulære nr. 90 af 16. juni 1999 om dansk indfødsret ved naturalisation. I lyset af denne særlige ordning vil det ikke være relevant med lovgivningsinitiativer på dette område. Ministeren for flygtninge, indvandre og integration vil i stedet drøfte med Folketingets Indfødsretsudvalg, hvilke ændringer i den hidtidige praksis, der er anledning til at gennemføre.

Økonomi- og erhvervsministeren vil fremsætte et lovforslag om ændring af lov om forebyggende foranstaltninger mod hvidvaskning af penge, jf. lov nr. 348 af 9. juni 1993 med senere ændringer (hvidvaskloven). I dette lovforslag indgår blandt andet de lovændringer, der følger af artikel 18 i FN's konvention til bekæmpelse af finansiering af terrorisme for så vidt angår pengeinstitutters forpligtelser til at indberette mistænkelig transaktioner mv. Lovforslaget vil indebære, at alle, der er omfattet af anmeldelsespligten i hvidvaskloven, også vil være forpligtet til at anmelde mistanke om finansiering af terrorisme. Anmeldelsen skal ske til politiet. Opstår der mistanke om, at en transaktion skal bidrage til finansiere terrorisme, vil pengeinstituttet mv. først kunne gennemføre transaktionen, efter at spørgsmålet har været forelagt politiet, hvilket i praksis indebærer en form for »indefrysning« af midler. Ændringerne skal også ses i sammenhæng med gennemførelsen af artikel 1, litra c, i FN's Sikkerhedsråds resolution nr. 1373 (2001) om indefrysning af midler tilhørende terrorister. Lovforslaget indeholder endvidere de lovændringer, der er nødvendige for at gennemføre det netop vedtagne direktiv om hvidvaskning af penge.

Ikrafttrædelsen af hvidvaskloven har medført, at det er blevet mere almindeligt, at personer ved indrejse og især ved udrejse medtager store pengebeløb, som bl.a. kan hidrøre fra forbrydelser eller kan befrygtes anvendt til finansiering af terrorisme. Som følge heraf fremsætter skatteministeren forslag om ændring af toldloven, således at Told•Skat får hjemmel til at kontrollere og tilbageholde større pengebeløb, der findes i forbindelse med indrejse og udrejse til og fra Danmark, hvor det må befrygtes, at beløbene stammer fra kriminalitet eller skal bruges til kriminalitet.

Justitsministerens lovforslag indeholder en række ændringer af straffeloven, retsplejeloven, våbenloven, udleveringsloven og lov om konkurrence- og forbrugerforhold på telemarkedet. Ændringerne skal blandt andet muliggøre en ratifikation af FN's terrorfinansieringskonvention, gennemføre FN's Sikkerhedsråds resolution nr. 1373 (2001), styrke det strafferetlige værn mod terrorister samt styrke politiets efterforskningsmuligheder. Det nærmere indhold af justitsministerens lovforslag gennemgås nedenfor.

1.2. Lovforslagets indhold

Justitsministeriet har siden terrorangrebene mod USA den 11. september 2001 gennemgået den gældende lovgivning inden for ministeriets område med henblik på at undersøge, om der er behov for at iværksætte nye initiativer mod terrorisme. Dette lovforslag indeholder de lovændringer, som Justitsministeriet i lyset af den nye verdenssituation på nuværende tidspunkt har fundet nødvendige i kampen mod terrorisme.

Formålet med lovforslaget er for det første at gennemføre de ændringer, der er nødvendige for, at Danmark kan ratificere *FN-konventionen af 9. december 1999 til bekæmpelse af finansiering af terrorisme* (FN's terrorfinansieringskonvention). Denne konvention medfører blandt andet, at en stat afskæres fra at nægte udlevering udelukkende med den begrundelse, at den forbrydelse, anmodningen angår, er en politisk forbrydelse mv. Endvidere nødvendiggør konventionen en ændring af reglerne om juridiske personers strafansvar for straffelovsovertrædelser. Konventionen indeholder desuden bestemmelser om medvirken til finansiering af terrorisme, som er videregående end gældende dansk ret. FN-konventionen er optaget som *bilag 1* til lovforslaget.

Vedtagelse af lovforslaget indebærer, at Folketinget giver samtykke til, at Danmark ratificerer FN-konventionen af 9. december 1999 til bekæmpelse af finansiering af terrorisme.

Dernæst indeholder lovforslaget de ændringer på Justitsministeriets område, som *FN's Sikkerhedsråds resolution nr. 1373 (2001)* nødvendiggør. Resolutionen indeholder en række juridisk bindende forpligtelser til landene samt en række ikke-bindende opfordringer. Resolutionen medfører blandt andet, at en stat skal kunne »indefryse« midler, der tilhører terrorister mv. Ligeledes skal det være strafbart at stille finansielle midler og tjenesteydelser til rådighed for terrorister. Enkelte af resolutionens artikler vedrører udlændingelovgivningen. For disse artiklers vedkommende vil der i lovforslaget alene blive henvist til det af ministeren for flygtninge, indvandrere og integration fremsatte lovforslag om ændring af udlændingeloven. Endvidere skal gennemgangen af resolutionen ses i sammenhæng med de ændringer af hvidvaskloven, som økonomi- og erhvervsministeren foreslår. FN-resolutionen er optaget som *bilag 2* til lovforslaget.

Herudover indeholder lovforslaget en række yderligere initiativer, der skal styrke det strafferetlige værn mod terrorisme og forbedre politiets efterforskningsmuligheder.

- Et af initiativerne er indsættelsen af *en særlig terrorismeparagraf* i straffeloven. En lang række af de forbrydelser, der typisk betegnes som terrorhandlinger, straffes i dag efter særskilte bestemmelser i straffeloven. Således vil f.eks. drab blive straffet efter straffelovens § 237, uanset hvad gerningsmandens motiv for handlingen har været. Regeringen ønsker i højere grad at signalere, at terrorisme i alle dens former er uacceptabel i et demokratisk samfund. Med lovforslaget foreslås derfor, at der i straffeloven indsættes en terrorismeparagraf, der indeholder en definition af begrebet terrorisme. Bestemmelsen omfatter meget alvorlige forbrydelser, der begås for at forstyrre samfundsordenen og skræmme befolkningen, og det foreslås derfor, at strafmaksimum fastsættes til fængsel på livstid. Bestemmelsen skal samtidig gennemføre EU's rammeafgørelse om bekæmpelse af terrorisme. Forslaget til rammeafgørelse er optaget som *bilag 3* til lovforslaget.
- Som et andet initiativ foreslås, at terrorismeparagraffen – i modsætning til den nuværende bestemmelse i straffelovens § 114 – også kommer til at *værne udenlandske offentlige anliggender og samfundsordener* for bedre at kunne tage højde for terrorismens globale karakter. Det foreslås også gjort strafbart i videre omfang end i dag at *yde eller formidle økonomisk støtte til en terrororganisation eller på anden medvirke til at fremme dens kriminelle virksomhed.* Disse særlige medvirkensregler er til dels en gennemførelse af FN's terrorfinansieringskonvention og FN's Sikkerhedsråds resolution nr. 1373 (2001).
- Grove våbenlovsovertrædelser er alvorlige forbrydelser, der kan have forbindelse til terrorisme. For at skabe mulighed for at idømme strengere straffe for særlig grove overtrædelser, foreslås det at *hæve strafferammen i § 192 a* for grove våbenlovsovertrædelser fra 4 år til 6 år.
- Indsættelse af en ny bestemmelse om *ikke spredning af masseødelæggelsesvåben mv.* i straffelovens kapitel 13.
- Med henblik på at styrke politiets efterforskningsmuligheder foreslås en bestemmelse i retsplejelovens § 786, hvorefter teleselskaber og internetudbydere skal *registrere og opbevare (»logge«) de oplysninger om tele- og internetkommunikation, der er relevante for politiets indgreb i meddelelseshemmeligheden mv.* Der er alene tale om registrering og opbevaring af trafikdata og ikke af selve indholdet af kommunikationen. De nærmere regler om denne logning fastsættes af justitsministeren efter forhand-

ling med ministeren for videnskab, teknologi og udvikling og i øvrigt efter dialog med branchen.

Denne del af lovforslaget er delvis udformet på grundlag af betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning. Betænkningen er afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (»Brydensholt-udvalget«), der påpeger et behov for, at internetudbydere forpligtes til at logge data om internettrafik.

Formålet med bestemmelsen er at sikre tilstedeværelsen af de oplysninger, som politiet kan få adgang til ved blandt andet indgreb i meddelelseshemmeligheden i form at teleoplysning og udvidet teleoplysning. Forslaget berører ikke de materielle og formelle betingelser, for at politiet kan foretage indgreb i meddelelseshemmeligheden – herunder kravet om retskendelse.

- Herudover stilles der forslag om forbedring af politiets efterforskningsmuligheder på en række punkter, hvor der i praksis opstår vanskeligheder i forbindelse med den praktiske gennemførelse af indgreb i meddelelseshemmeligheden.

  Der foreslås således indsat en bestemmelse i retsplejeloven, der bemyndiger justitsministeren til efter forhandling med ministeren for videnskab, teknologi og udvikling at *fastsætte regler om teleudbydernes bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.* Den foreslåede bestemmelse erstatter en tilsvarende, ikke udnyttet bemyndigelsesbestemmelse i telelovgivningen. Også på dette punkt forudsættes branchen inddraget i forbindelse med regelfastsættelsen.

  Formålet med denne del af lovforslaget er at sikre politiet en hurtig og effektiv adgang til de oplysninger, som skal tilvejebringes ved indgreb i meddelelseshemmeligheden.

- Lovforslaget indeholder endvidere regler om *adgang for politiet til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste,* der indeholder navne- og adresseoplysninger vedrørende samtlige navneregistrerede telefonabonnementer i Danmark, herunder også hemmelige telefonnumre.

- Efter de gældende regler i retsplejeloven kan politiet ved hjælp af aflytning gøre sig bekendt med kommunikation mellem computere, ligesom politiet ved en ransagning kan gøre sig bekendt med alle registreringer i en computer, herunder modtagne elektroniske meddelelser og kopier af sådanne meddelelser, der er afsendt. På grund af tekniske forhold og som følge af risikoen for afsløring af indgrebene er det imidlertid ikke i alle tilfælde muligt at udnytte den eksisterende adgang for politiet til at gøre sig bekendt med elektroniske meddelelser og materiale i en computer. På denne baggrund foreslås det, at der i retsplejeloven indsættes en ny bestemmelse (§ 791 b), der indebærer, at politiet efter rettens kendelse får mulighed for *at aflæse ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning)* uden at være til stede på det sted, hvor et informationssystem (dvs. en computer eller andet dataanlæg) benyttes. Det er herunder muligt at tillade indgreb, hvor politiet ved hjælp af et såkaldt »snifferprogram« får tilsendt kopi af samtlige indtastninger, som brugeren af dataanlægget foretager.

- Lovforslaget indeholder endvidere en ændring af retsplejelovens § 799, således at der bliver *adgang til at foretage hemmelig ransagning i sager om grov brandstiftelse, bombesprængning, flykapring og tilsætning af giftstoffer til vandforsyningen eller madvarer mv.* Adgangen til at kunne hemmeligholde oplysninger om ransagning i disse sager vil f.eks. kunne være af afgørende betydning, hvis der formodes at være flere ukendte medgerningsmænd til forbrydelsen, og hemmeligholdelse af efterforskningen derfor er nødvendig for, at disse kan identificeres og anholdes.

- Samtidig foreslås en ændring af retsplejelovens § 799, således at der skabes adgang til, at retten ved én kendelse kan tillade politiet at foretage flere enkeltstående ransagninger uden umiddelbar underretning (*gentagen hemmelig ransagning*). Dette kan være nødvendigt, hvor der ikke findes f.eks. narkotika eller våben ved den første ransagning, men hvor der fortsat er mistanke om, at levering på det pågældende sted vil ske inden for kort tid, eller hvor en ransagning på grund af risikoen for afsløring af efterforskningen har måtte afbrydes.

- Herudover indeholder lovforslaget en ændring af retsplejelovens § 806, hvorved der skabes *mulighed for at pålægge tredjemand at udlevere dokumenter mv. (edition) uden forudgående retskendelse,* såfremt formålet forspildes, hvis retskendelse skulle afventes. Dette kan f.eks. tænkes relevant i en situation, hvor politiet har behov for øjeblikkelig udlevering af et flyselskabs passagerliste.

- Ligeledes foreslås en ændring af retsplejelovens § 802 og § 803 om beslaglæggelse, således at der bliver mulighed for at *beslaglægge penge og andre formuegoder* (og ikke kun genstande) med henblik på konfiskation efter straffelovens § 77 a. Der er tale om en nødvendig ændring som følge af den foreslåede udvidelse af straffelovens § 77 a, som gennemfører FN's terrorfinansieringskonventions

artikel 8 og FN's Sikkerhedsråds resolutions artikel 1, litra c.

- Endvidere indeholder lovforslaget en ændring af udleveringslovens forbud mod udlevering af danske statsborgere. Formålet med denne ændring er at skabe hjemmel for, at *danske statsborgere,* når visse betingelser er opfyldt, kan *udleveres til strafforfølgning i udlandet.* Baggrunden for ændringen er, at retsforfølgning som udgangspunkt bør ske der, hvor kriminaliteten er begået, da det ofte kan være forbundet med store – og til tider uoverstigelige – vanskeligheder under en straffesag i Danmark at føre beviser for kriminalitet begået i udlandet, når vidner og/eller beviser ikke befinder sig i Danmark. Lovforslaget vil således medføre en øget mulighed for at stille personer til regnskab i den stat, hvor lovovertrædelsen er begået. Endvidere vil det med lovforslaget blive muligt, at Danmark *delvist kan ophæve det forbehold* om ikke at ville udlevere egne statsborgere, som Danmark tog ved undertegnelsen af EU-udleveringskonventionen fra 1996.
- Forslaget indeholder ligeledes en ændring af udleveringslovens § 5, stk. 3, hvorefter *udlevering for en handling omfattet af artikel 1 eller 2 af den europæiske konvention om bekæmpelse af terrorisme,* ikke kan afslås med henvisning til forbudet om udlevering for politiske forbrydelser ved udlevering til en EU-medlemsstat. Det foreslås, at undtagelsen fra forbudet om udlevering for politiske forbrydelser udvides til omfatte alle anmodninger om udleveringer for handlinger omfattet af artikel 1 eller 2 af den europæiske konvention om bekæmpelse af terrorisme, uanset om der er tale om udlevering til en EU-medlemsstat eller en anden (europæisk) stat, som har ratificeret konventionen. Ændringen vil medføre, at Danmark helt kan give *afkald på det forbehold,* der blev taget ved ratifikationen af den europæiske konvention om bekæmpelse af terrorisme over for den særlige bestemmelse i konventionens artikel 1. Herudover skal anmodninger om udlevering for forhold omfattet af FN's terrorfinansieringskonvention heller ikke kunne afslås med henvisning til forbudet mod udlevering for politiske forbrydelser, jf. ovenfor.

2. Strafferetlige initiativer mod terrorisme

2.1. Internationale initiativer mod terrorisme

Internationalt er der på baggrund af angrebene mod USA taget adskillige initiativer for at styrke den internationale kamp mod terrorisme. Nedenfor redegøres for de initiativer, der er taget af FN og af EU. Herudover er der også i FATF (Financial Action Task Force) og Europarådet igangsat konkrete initiativer på området.

2.1.1. FN-initiativer vedrørende terrorisme

2.1.1.1. FN's terrorfinansieringskonvention

FN-konventionen til bekæmpelse af finansiering af terrorisme (terrorfinansieringskonventionen) blev vedtaget af Generalforsamlingen den 9. december 1999 og åbnet for undertegnelse den 10. januar 2000. Danmark har undertegnet konventionen den 25. september 2001.

Formålet med FN's terrorfinansieringskonvention er at forbedre det internationale samarbejde om forebyggelse og strafferetlig forfølgning af terrorhandlinger ved at forebygge og bekæmpe finansiering af terrorisme. Ved konventionen forpligter de deltagende stater sig til på grundlag af en række fælles definitioner at betragte tilvejebringelse og indsamling af midler i den hensigt, at de skal anvendes, eller med viden om, at de vil blive anvendt, helt eller delvist til at udføre nærmere beskrevne handlinger, som strafbare handlinger, som skal kunne straffes under hensyn til deres alvorlige karakter, herunder også i forhold til juridiske personer. Konventionen indeholder endvidere en forpligtelse til at straffe medvirken til finansiering af terrorangreb i vidt omfang. Endelig medfører konventionen gennem regler om straffemyndighed, udlevering og retshjælp mv. udvidede muligheder for at strafforfølge gerningsmænd uden hensyn til, hvor den strafbare handling er begået, og hvor gerningsmanden hører hjemme.

FN's terrorfinansieringskonvention *er optaget som bilag 1 til lovforslaget.*

Artikel 1 indeholder *definitioner* af en række udtryk, som indgår i afgrænsningen af den kriminaliseringspligt, som konventionen pålægger de deltagende stater.

Efter stk. 1 forstås ved *»midler«* aktiver af enhver art, hvad enten de er materielle eller immaterielle, løsøre eller fast ejendom, uanset erhvervelsesmåde, samt juridiske dokumenter eller instrumenter i enhver form, herunder elektronisk eller digital, der er bevis på ejendomsret til eller rettighed til sådanne aktiver, herunder blandt andet remburser, rejsechecks, bankchecks, pengeanvisninger, aktier, værdipapirer, obligationer, veksler eller akkreditiver.

Efter stk. 2 forstås ved *»stats- eller regeringsfacilitet«* ethvert permanent eller midlertidigt anlæg eller transportmiddel, der anvendes eller er optaget af statsrepræsentanter, medlemmer af regering, lovgivnings-

Det kan i den forbindelse i øvrigt oplyses, at Erhvervsfremme Styrelsen for tiden planlægger en betydelig øget indsats på eksportkontrolområdet. Det drejer sig bl.a. om øget information til virksomhederne for at udbrede kendskabet til eksportrestriktionerne, øget kontrol med overholdelsen af styrelsens udførselstilladelser samt øget opmærksomhed og bedre kvalitetsstyring i virksomhederne.

3. Styrkelse af politiets efterforskningsmuligheder

3.1. Logning af trafikdata vedrørende telekommunikation

3.1.1. Gældende ret

3.1.1.1. Indgreb i meddelelseshemmeligheden

Ved lov nr. 465 af 7. juni 2001 om ændring af straffeloven og retsplejeloven (Hæleri og anden efterfølgende medvirken samt IT-efterforskning) er der i retsplejelovens § 780, stk. 1, indsat en bestemmelse (nr. 4), hvorefter politiet kan foretage indgreb i meddelelseshemmeligheden ved at indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område, der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning). Bestemmelsen giver politiet mulighed for at få adgang til de såkaldte masteoplysninger i forbindelse med efterforskning af forbrydelser, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Bestemmelsen er indsat på baggrund af et forslag fra Brydensholt-udvalget i betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning.

Der henvises herom nærmere til loven samt til Folketingstidende 2000-01, forhandlingerne, s. 6443-6459, 8674-8675 og 9050-9062, tillæg A, s. 5690-5721, samt tillæg B, s. 1525-1533.

Efter retsplejelovens § 780, stk. 1, nr. 3, kan politiet foretage indgreb i meddelelseshemmeligheden ved at indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater, der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning). Efter denne bestemmelse kan politiet således indhente teleoplysning vedrørende bestemte telefonnumre, eksempelvis oplysninger om opkald til eller fra en mistænkt.

Bestemmelserne om teleoplysning og udvidet teleoplysning giver politiet adgang til – almindeligvis efter forudgående retskendelse – at få udleveret data, som teleudbyderne i anden anledning registrerer og opbevarer (logning). Bestemmelserne indebærer derimod ikke en pligt for teleudbyderne til at logge bestemte trafikdata.

3.1.1.2. Opbevaring af trafikdata

Lov nr. 418 af 31. maj 2000 om konkurrence- og forbrugerforhold på telemarkedet indeholder i § 14 en bemyndigelsesbestemmelse, hvorefter ministeren for videnskab, teknologi og udvikling (tidligere IT- og forskningsministeren) kan fastsætte regler for udbydere af offentlige telenet eller teletjenester om minimumskrav til behandling af personoplysninger i forbindelse med telekommunikation. Bemyndigelsen er udnyttet ved bekendtgørelse nr. 1169 af 15. december 2000 om udbud af telenet og teletjenester, der bl.a. indeholder bestemmelser om behandling af trafik- og debiteringsdata.

Bekendtgørelsens § 30, stk. 1, fastsætter, at udbydere af offentlige telenet eller teletjenester skal sikre, at trafikdata vedrørende slutbrugere slettes eller anonymiseres efter samtalens afslutning. Trafikdata kan være oplysninger om A- og B-nummer (dvs. det kaldende og kaldte telefonnummer) og tidspunktet for kommunikationen.

Fra udgangspunktet om sletning gøres visse undtagelser i § 30, stk. 2 og 3. Efter stk. 2 er det således tilladt at behandle og opbevare trafikdata med henblik på debitering af slutbrugere og afregning for samtrafik. En sådan behandling og opbevaring er tilladt indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger. § 30, stk. 3, tillader teleudbyderne at opbevare trafikdata med henblik på markedsføring af egne teletjenester, forudsat at kunden har givet samtykke.

Bekendtgørelsen regulerer således spørgsmålet om, hvornår trafikdata lovligt kan opbevares, men indeholder ingen bestemmelser, der forpligter udbyderne til at opbevare disse oplysninger. Den enkelte teleudbyder må således selv afgøre – inden for rammerne af bekendtgørelsens § 30 – om og i hvilket omfang trafikdata opbevares.

Teleselskabernes praksis med hensyn til logning af masteoplysninger varierer betydeligt. Det er således ikke alle teleudbydere, der registrerer oplysninger om, hvilke mobiltelefoner der i et givent område og inden for et bestemt tidsrum har været sat i forbindelse med andre telefoner.

Bekendtgørelsens § 30 gennemfører artikel 6 i Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (97/66/EF) i dansk ret.

Efter direktivets artikel 6, stk. 1, skal trafikdata vedrørende abonnenter og brugere, som behandles ved etablering af samtaler, og som lagres af leverandøren af et offentligt telenet og/eller en offentligt tilgængelig teletjeneste, slettes eller gøres anonyme efter samtalens afslutning. Fra denne forpligtelse kan der gøres undtagelse, i det omfang det sker med henblik på debitering af abonnenten og afregning for samtrafik, jf. artikel 6, stk. 2, eller – med kundens samtykke – med henblik på markedsføring af egne teletjenester, jf. artikel 6, stk. 3. Disse regler svarer således til bestemmelserne i § 30 i bekendtgørelse om udbud af telenet og teletjenester.

Direktivet begrænser imidlertid ikke mulighederne for at behandle trafikdata i forhold til efterforskning og retsforfølgning af strafbare forhold. Det fremgår således af artikel 14, stk. 1, at medlemsstaterne kan vedtage lovbestemmelser med henblik på at indskrænke rækkevidden af de forpligtelser og rettigheder, der nævnes i artikel 6, hvis en sådan indskrænkning er nødvendig af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af telekommunikationssystemet.

Denne bestemmelse tillader således, at der i national lovgivning kan fastsættes regler, der fraviger kravet om sletning af trafikdata. Betingelsen er imidlertid, at det sker for at varetage et eller flere af de hensyn, der er nævnt i artikel 14, stk. 1.

Europa-Kommissionen har den 12. juli 2000 fremlagt et forslag til Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000) 385).

Det foreslåede direktiv skal erstatte direktiv 97/66/EF. Kommissionen anfører i begrundelsen for direktivforslaget, at det ikke er hensigten at foretage »en gennemgribende ændring af substansen i det eksisterende direktiv, men blot at tilpasse og ajourføre de eksisterende bestemmelser efter den udvikling, der allerede er sket, eller som kan forventes inden for elektroniske kommunikationstjenester eller -teknologier«. Den væsentligste ændring består således i, at anvendelsesområdet for direktivet udvides fra kun at omfatte telefoni til generelt at omfatte elektronisk kommunikation, herunder Internet og e-post.

Der er også efter det foreslåede direktiv adgang til at indskrænke rækkevidden af direktivets forpligtelser og rettigheder med hensyn til behandling af bl.a. trafikdata, hvis en sådan indskrænkning er nødvendig af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem.

3.1.2. Brydensholt-udvalgets forslag

I september 1999 afgav Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (»Brydensholt-udvalget«) betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning.

Betænkningen indeholder udvalgets overvejelser og forslag om ændring af straffelovens § 235 om børnepornografi og om ændring af retsplejelovens regler om indgreb i meddelelseshemmeligheden i sager om børnepornografi. Disse dele af betænkningen blev medtaget i lovforslag nr. L 281 af 27. april 2000, jf. nu lov nr. 441 af 31. maj 2000 om ændring af straffeloven og retsplejeloven (Forældelse, styrket indsats mod seksuelt misbrug af børn og unge samt IT-efterforskning). Der henvises herom til lov nr. 441 af 31. maj 2000 samt til Folketingstidende 1999-2000, forhandlingerne, s. 7423-7431, 8474-8477 og 8756, tillæg A, s. 7784-7826, samt tillæg B, s. 1327-1330.

Udvalget overvejer endvidere i betænkningen en række forslag til, hvordan politiets efterforskningsmuligheder kan forbedres i sager, hvor der i forbindelse med en lovovertrædelse anvendes informationsteknologi. Således indeholder betænkningen også nogle forslag, som ikke i særlig grad vedrører sager om børnepornografi. Udvalget stiller bl.a. forslag om en særlig regulering af adgangen til at indhente masteoplysninger. Herved forstås bl.a. oplysninger om, hvilke mobiltelefoner der i et givent område og inden for et bestemt tidsrum har været sat i forbindelse med andre telefoner. Udvalget har endvidere mere generelt berørt betingelserne for og afgrænsningen mellem de forskellige straffeprocessuelle indgreb i forhold til elektronisk kommunikation.

Justitsministeriet tilkendegav i bemærkningerne til lovforslag nr. L 281, at Justitsministeriet i forbindelse med kommende forslag om ændringer af retsplejelovens straffeprocessuelle regler ville inddrage de øvrige mere generelle overvejelser og forslag til, hvordan efterforskningsmulighederne kan forbedres med henblik på tilfælde, hvor der i forbindelse med overtrædelserne anvendes informationsteknologi.

Disse dele af udvalgets betænkning blev herefter medtaget i lovforslag nr. L 194 af 21. marts 2001, jf. nu lov nr. 465 af 7. juni 2001 om ændring af straffeloven og retsplejeloven (Hæleri og anden efterfølgende medvirken samt IT-efterforskning). Der henvises herom til pkt. 3.1.1.1. ovenfor.

Et enkelt forslag blev dog ikke medtaget i lovforslaget. Udvalget overvejer således i betænkningen

spørgsmålet om at indføre en pligt for internetudbydere og teleselskaber til at logge visse oplysninger, således at det under en efterfølgende politimæssig efterforskning vil være muligt at spore den kommunikation, der har fundet sted. Udvalget anser en sådan logningspligt for i særlig grad at have betydning for efterforskningen af lovovertrædelser vedrørende børnepornografi, men oplysningerne vil kunne bidrage til efterforskningen af alle former for kriminalitet, der foregår på eller ved hjælp af Internettet.

Som det fremgår af pkt. 8.2.2. i de almindelige bemærkninger til lovforslaget om forældelse, styrket indsats mod seksuelt misbrug af børn og unge samt IT-efterforskning (lovforslag nr. L 281 af 27. april 2000), jf. Folketingstidende 1999-2000, tillæg A, s. 7809, er der fra IT-branchens side i høringssvarene over betænkningen udtrykt betænkelighed ved udvalgets forslag om registrering af logoplysninger og opbevaring heraf. Justitsministeriet fandt det derfor rigtigst, at der ikke på det da foreliggende grundlag blev stillet forslag om at indføre en sådan pligt for internetudbydere og teleselskaber. Justitsministeriet iværksatte på denne baggrund i samarbejde med Ministeriet for Videnskab, Teknologi og Udvikling en nærmere undersøgelse af konsekvenserne af udvalgets forslag i lyset af de indvendinger, der er fremført i visse af høringssvarene vedrørende betænkningen. På tidspunktet for fremsættelse af lovforslaget om hæleri og efterfølgende medvirken samt IT-efterforskning (lovforslag nr. L 194 af 21. marts 2001) var Justitsministeriets og Ministeriet for Videnskab, Teknologi og Udviklings overvejelser endnu ikke afsluttet, jf. Folketingstidende 2000-2001, tillæg A, s. 5704. Justitsministeriet tilkendegav på denne baggrund, at man i forbindelse med en fremtidig ændring af retsplejeloven ville tage spørgsmålet op på ny, når overvejelserne var afsluttet.

Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling er enige om, at der – bl.a. i lyset af de tragiske begivenheder, der fandt sted ved terrorangrebet i USA den 11. september 2001 – nu er grundlag for at foreslå en regulering på dette område.

3.1.2.1. Udvalgets generelle overvejelser

Udvalget konstaterer, at manglende eller mangelfulde oplysninger hos internetudbydere udgør et efterforskningsmæssigt problem. Dette problem forstærkes, når efterforskningen vedrører forhold, hvor der er anvendt flere internetadresser til kommunikationen. De kriminelle udnytter herved, at oplysninger om datastrømmene, herunder oplysninger om, hvilket land der opereres fra, ikke er tilgængelige for politiet.

Udvalget anfører, at modhensynet, der taler for få registreringer og kortvarig opbevaring af oplysningerne hos formidlerne, især er hensynet til privatlivets fred.

Udvalget erkender, at det ikke er muligt at tilgodese begge disse modsatrettede hensyn fuldt ud. Der er endvidere ikke tale om et problem, der kan totalløses via dansk lovgivning, men udvalget finder, at en dansk regulering under alle omstændigheder vil være nyttig.

3.1.2.2. Behovet for regulering

Udvalget bemærker generelt, at der ofte kan være meget stor teknisk usikkerhed med hensyn til loggens indhold og fuldstændighed, og at det kan være omkostningskrævende at stille krav på dette område.

Udvalget anfører, at oplysninger om B-nummeret (eksempelvis det nummer hos en internetudbyder, der kaldes op til) i dag kun fastholdes kortvarigt hos teleudbyderne. Dette vanskeliggør efterforskningen, idet der nødvendigvis går tid med behandling af anmeldelsen og visitering af sagen, inden efterforskningen kan påbegyndes. B-numrene bruges f.eks. til regningsspecifikationer, således at den kaldende abonnent har mulighed for at identificere, hvilke numre der har været kaldt op til i den seneste regningsperiode.

Ud fra et efterforskningsmæssigt synspunkt har det stor betydning, at A-nummeret (det nummer, der ringes fra) logges. Dette gælder uanset, om den pågældende har benyttet muligheden for at blokere for visning af A-nummeret hos den, der ringes til. Adgangen hertil må antages primært at skulle beskytte imod, at nummeret kan vises hos modtageren (indehaveren/brugeren af B-nummeret) og ikke at tage sigte på de registreringer, der kan være behov for i telekæden.

Registrering og opbevaring af oplysninger om A-nummeret i tilknytning til en given internetopkobling, vil gøre det muligt efterfølgende – f.eks. i forbindelse med efterforskning af lovovertrædelser, der er begået under den pågældende internetsession – at føre sporet helt tilbage til det telefonnummer – og dermed almindeligvis det sted – hvorfra den ulovlige aktivitet er begået.

Udvalget konstaterer, at i hvert fald én af de større internetudbydere kun tilslutter til Internettet, hvis A-nummeret samtidig registreres (hvilket sker, uanset om det er visningsbeskyttet eller ej).

Endelig påpeger udvalget vigtigheden af, at der også sker registrering af den IP-adresse, som brugeren tildeles i forbindelse med den konkrete internetsession. For at styre kommunikationen på Internettet har hver server (computer), som er koblet til Internettet, en unik IP-adresse (Internet Protocol). Adressen over-

føres med hver elektronisk impuls, der sendes over nettet og efterlader således et elektronisk spor. Adresserne, der dannes ved hjælp af en algoritme, består af fire talsekvenser med indtil tre cifre hver. Antallet af IP-adresser er på denne baggrund begrænset til ca. 4,3 milliarder. Af økonomiske årsager har kun brugere, der anvender Internettet i stort omfang en fast IP-adresse. F.eks. råder internetudbydere over flere IP-adresser, der på mere eller mindre tilfældig måde tildeles brugerne, når disse logger sig på nettet (dynamiske IP-adresser).

På Internettet er centrale fortegnelser over indehaverne af IP-adresser tilgængelige. Såfremt en anvendt IP-adresse tilhører en internetudbyder, slutter det elektroniske spor hos denne. Kun hvis udbyderen registrerer, hvilken kunde der på et bestemt tidspunkt har været tildelt den pågældende dynamiske IP-adresse, kan sporet føres tilbage til brugeren.

3.1.2.3. Det nærmere indhold af reguleringen

Brydensholt-udvalget foreslår på baggrund af disse overvejelser, at der stilles krav om, at internetudbydere ved opkobling via telefonnettet skal logge både A og B-nummeret – for A-nummerets vedkommende uanset om den pågældende har benyttet muligheden for, at der ikke sker visning af A-nummeret.

Endvidere bør udbyderen logge IP-adresse for den, der tilslutter sig Internettet, brugertid, tidspunkt for opkobling/nedkobling, opkoblingens varighed og sessionstype (FTP/Telnet). Der bør tillige stilles krav om opbevaringsformat (læsbarhed) og foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen. Derudover bør eventuelle kontooplysninger opbevares.

Opbevaring af oplysninger skal ske her i landet, hvis udbyderen driver virksomhed i Danmark, uanset om udbyderen er selvstændig eller en filial af en udenlandsk virksomhed.

Endvidere bør det tilstræbes, at det sikres, at korrekt dansk realtid registreres. I praksis har det under efterforskning vist sig, at teleselskabers og internetudbyderes tidsangivelser i loggen har været upræcise. Det vil derfor set fra et efterforskningsmæssigt synspunkt være hensigtsmæssigt, hvis der stilles krav om, at der etableres et system med korrekt dansk realtid, f.eks. ved at serveren jævnligt synkroniseres med realtid. Hvis tidsregistreringer i logninger, der indgår i en efterforskning, ikke er korrekte, risikerer politiet at målrette efterforskningen mod forkerte personer.

Udvalget har nærmere drøftet de forskellige hensyn, der kan tale for henholdsvis en længere og en kortere opbevaringstid af oplysningerne, og har på baggrund af drøftelserne valgt at anbefale en opbevaringsfrist på 6 måneder.

Med hensyn til formen for reguleringen har udvalget indgående drøftet, om de ønskede registreringer og opbevaringen heraf ville kunne gennemføres ved en selvregulering. Et *flertal* i udvalget (15 medlemmer) finder, at reguleringen skal ske ved lov, mens et *mindretal* i udvalget (4 medlemmer) finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen. Dette mindretal er dog enige i en lovgivningsmæssig løsning, såfremt det viser sig, at reguleringsbestræbelserne ikke bærer frugt.

Udvalget drøfter også de problemer, der opstår ved almindeligt tilgængelige computere (på biblioteker, internetcaféer mv. og i et vist omfang på arbejdspladser), der kan benyttes til at opnå anonymitet ved anvendelse af Internettet, men afstår fra at foreslå en regulering på dette område. Hvis efterforskningen viser, at en sådan computer er blevet benyttet, og der ikke findes oplysninger om brugeren, må det i stedet forsøges via afhøringer at afgrænse den mulige brugerkreds.

Om udvalgets nærmere overvejelser henvises til betænkningen s. 63-71 og s. 101-103.

3.1.3. Justitsministeriets overvejelser

I høringssvarene fra telebranchen vedrørende det lovudkast, der har været sendt til høring, er det påpeget, at en række teleudbydere alene betjener en afgrænset kundegruppe, f.eks. banker eller skoler. Grænsedragningen i forhold til udbydere af offentlige telenet eller teletjenester er derfor ikke helt klar. Endvidere vil det kunne have en negativ indflydelse på konkurrenceforholdene i branchen, såfremt udbyderne ikke behandles ens. Det fremhæves på denne baggrund, at lovforslaget derfor bør stille krav til udbyderne, uanset om de henvender sig til et begrænset kundesegment eller til offentligheden i almindelighed.

Justitsministeriet er enig i dette synspunkt. Både hensynet til en effektiv regulering og hensynet til konkurrenceforholdene i branchen tilsiger, at den foreslåede bestemmelse omfatter alle udbydere, uanset til hvilken kundegruppe de udbyder telenet og teletjenester.

3.1.3.1. Teletrafikdata

Bestemmelserne om udvidet teleoplysning i lovforslag nr. L 194 om ændring af straffeloven og retsplejeloven (Hæleri og anden efterfølgende medvirken), jf. nu lov nr. 465 af 7. juni 2001, vedrører alene politiets adgang til f.eks. masteoplysningerne. Baggrunden for lovforslaget var, at der i retspraksis var opstået

tvivl om, hvorvidt retsplejelovens bestemmelser om indgreb i meddelelseshemmeligheden indeholdt den fornødne hjemmel til indgrebet. Justitsministeriet forudsatte således, at de pågældende oplysninger i praksis ville være tilgængelige hos teleudbyderne, når politiet på baggrund af retskendelse anmoder om oplysningerne. Der blev derfor ikke samtidig stillet forslag om regler vedrørende teleudbydernes registrering og opbevaring (logning) af disse oplysninger.

Som det imidlertid er anført under pkt. 3.1.1.2. ovenfor, har det vist sig, at der ikke er fast praksis hos teleselskaberne for at logge masteoplysninger. Et teleselskabs fravalg af en sådan logning kan skyldes forskellige forhold. Der kan være tale om, at man ikke har indrettet sig teknisk på at gemme de pågældende oplysninger, eller at oplysningerne ikke logges, fordi selskabet finder, at de ikke er nødvendige af hensyn til kundedebitering, f.eks. hvor kunden betaler et fast beløb for samtaler, uanset hvor mange eller få samtaler, der føres (såkaldt »flat rate-abonnement«).

Som det fremgår af pkt. 4.4. i bemærkningerne til lovforslaget om hæleri og masteoplysninger, jf. Folketingstidende 2000-01, tillæg A, s. 5707, kan disse oplysninger være nødvendige for at politiet kan komme videre med opklaringen af en alvorlig forbrydelse. Dette var baggrunden for forslaget om at sikre politiet adgang til at foretage indgreb i meddelelseshemmeligheden i form af udvidet teleoplysning, jf. nu retsplejelovens § 780, stk. 1, nr. 4.

Det er imidlertid tilsvarende vigtigt, at det er muligt at sikre, at der sker registrering af teleoplysninger i traditionel forstand, herunder oplysninger om A- og B-nummer, opkaldstidspunkter og varigheden af samtaler. Også disse oplysninger registreres i dag i et omfang, som hvert enkelt teleselskab selv fastsætter.

På baggrund af politiets erfaringer med hensyn til de kriminelles anvendelse af moderne kommunikationsmidler, herunder ikke mindst i forbindelse med alvorlige lovovertrædelser, er det efter Justitsministeriets opfattelse nødvendigt at sikre, at der sker opbevaring af de teleoplysninger, som politiet kan få brug for ved bekæmpelsen af alvorlig kriminalitet, herunder bl.a. terrorhandlinger.

Efter Justitsministeriets opfattelse er der behov for at sikre, at teletrafikdata er tilgængelige med henblik på gennemførelse af indgreb i meddelelseshemmeligheden. Der stilles på denne baggrund forslag om, at teleselskaberne skal logge de former for trafikdata, som politiet har brug for i forbindelse med efterforskning af lovovertrædelser.

Justitsministeriet er i den forbindelse opmærksom på, at indehavere af mobiltelefoner med taletidskort normalt vil være anonyme i forhold til det teleselskab, der leverer teleydelsen, og at det således i disse tilfælde ikke vil være muligt for telefonselskabet at fremskaffe oplysninger om navn og adresse på den pågældende kunde. Det samme kan være tilfældet for så vidt angår visse e-posttjenester.

Det er dog ikke udelukket, at kundens navn alligevel kan være registreret hos telefonselskabet, f.eks. af markedsføringsmæssige årsager. Det forekommer også, at politiet ad anden vej er bekendt med, hvem der benytter f.eks. et bestemt taletidskort.

Det er hensigten at fastsætte de nærmere regler om logningspligtens indhold og omfang efter dialog med teleudbyderne. Dette er ikke mindst afgørende for at sikre en teknologisk hensigtsmæssig udformning af reglerne.

Om baggrunden for forslaget om anvendelse af en bemyndigelsesbestemmelse henvises til pkt. 3.1.3.3. nedenfor.

Justitsministeriet foreslår, at opbevaringsperiodens varighed fastsættes til 1 år. Dette vil være i overensstemmelse med Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (97/66/EF), jf. pkt. 2.1.2. ovenfor. I det omfang, der ikke er tale om oplysninger, der i henhold til direktivet kan opbevares med henblik på kundedebitering, kan opbevaringstiden ikke være længere end hensynet til »forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager« tilsiger, jf. direktivets artikel 14, stk. 1. Efter Justitsministeriets opfattelse går en opbevaringsperiode på 1 år ikke videre, end dette hensyn tilsiger. Trafikdata, der gemmes med henblik på debitering, vil – uanset om de pågældende data omfattes af den lovbestemte logningspligt – som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktivet og § 30, stk. 2, i bekendtgørelse om udbud af telenet og teletjenester. Dette indebærer i praksis, at oplysningerne kan gemmes i op til 5 år.

Det skal understreges, at der ikke stilles forslag om ændring af retsplejelovens betingelser for at foretage indgreb i meddelelseshemmeligheden. De oplysninger, som teleselskaberne vil have pligt til at logge, vil således kun kunne kræves udleveret af politiet, hvis der er grundlag for at foretage indgreb i meddelelseshemmeligheden. Dette indebærer, at der skal være bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt, at indgrebet må antages at være af afgørende betydning for efterforskningen, og

at der i almindelighed skal være tale om efterforskning af en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, jf. retsplejelovens § 781, stk. 1. Endvidere skal proportionalitetskravet i § 782 være opfyldt. Kravet om »bestemte grunde« skal ikke være opfyldt ved udvidet teleoplysning, men der er omvendt kun adgang til disse oplysninger, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier, jf. § 781, stk. 5.

Denne del af forslaget giver således ikke politiet adgang til oplysninger i videre omfang end i dag. Forslaget skal alene sikre, at de pågældende oplysninger rent faktisk findes, hvis der bliver brug for dem.

3.1.3.2. Internettrafikdata

Internettets anvendelsesmuligheder er mangfoldige. Det udgør en væsentlig lettelse i den daglige kommunikation mellem mennesker og giver mulighed for at søge og udveksle oplysninger på en enkel, hurtig og billig måde. I kraft af Internettets komplicerede struktur giver det også gode muligheder for at være anonym i forbindelse med kommunikation og informationsudveksling. Disse muligheder udnyttes ikke mindst af de kriminelle.

Det ville være en illusion at tro, at det er muligt at overvåge hele Internettet. En sådant mål er heller ikke ønskeligt. Selv om det således ikke er muligt at bekæmpe al internetkriminalitet, bør man efter Justitsministeriets opfattelse ikke undlade at forbedre politiets efterforskningsmuligheder på de områder, hvor det kan lade sig gøre uden at tilsidesætte væsentlige hensyn til økonomi og privatlivets fred.

Justitsministeriet finder af de af Brydensholt-udvalget anførte grunde, at der – af hensyn til mulighederne for en effektiv efterforskning og bekæmpelse af kriminalitet, der begås på eller ved hjælp af Internettet – bør tilvejebringes hjemmel til at kræve logning af internettrafik. Den seneste tids alvorlige terrorangreb på USA, herunder udbredelsen af miltbrandbakterier, forstærker denne opfattelse. Angrebene viser, hvor sårbare vore moderne samfærdsels- og kommunikationsmidler er over for de udspekulerede og – forud for angrebene – nærmest utænkelige handlinger, som terrorister foretager, og der er al mulig grund til at antage, at terrorister i forbindelse med planlægningen af terrorhandlinger kommunikerer med hinanden og tilvejebringer information ved hjælp af Internettet.

Det er hensigten at fastsætte de nærmere regler om logningspligtens indhold og omfang efter dialog med internetudbyderne. Dette er ikke mindst afgørende for at sikre en hensigtsmæssig teknologisk udformning af reglerne.

En ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold vil være en nyskabelse i forhold til den gældende retstilstand. Uanset, at forslaget om en nærmere regulering ved bekendtgørelse i vid udstrækning giver mulighed for løbende at tage højde for det praktiske behov for logning og den tekniske udvikling på området, finder Justitsministeriet det hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse. Bestemmelsen i lovforslagets § 8 indebærer således, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse.

Om baggrunden for forslaget om anvendelse af en bemyndigelsesbestemmelse henvises til pkt. 3.1.3.3. nedenfor.

Formålet med den foreslåede regulering er at sikre, at de elektroniske spor, der findes på Internettet i tilknytning til en kriminel aktivitet, ikke ender blindt hos internetudbyderen. Dette forudsætter, at udbyderen er i stand til at levere oplysninger om, hvem der har efterladt det pågældende spor. I praksis vil dette kun være muligt, hvis udbyderen er i besiddelse af præcise oplysninger om, hvilken kunde, der på det pågældende tidspunkt har anvendt en tildelt IP-adresse. Af hensyn til værdien af disse oplysninger er det vigtigt, at oplysningerne er nøjagtige, herunder ikke mindst for så vidt angår tidsangivelser. Ved anvendelsen af dynamiske IP-adresser vil det forekomme, at den IP-adresse, som den kriminelle har anvendt, kort tid før eller efter anvendes af en anden kunde hos den pågældende udbyder. Korrekt tidsangivelse er af afgørende betydning for, at det elektroniske spor kan føres tilbage til den person, der anvendte den pågældende IP-adresse på gerningstidspunktet.

Det har over for Justitsministeriet været fremført, at der i praksis vil kunne være tekniske hindringer for internetudbyderes registrering af det kaldende nummer (A-nummeret). Denne registrering, der kun vil være relevant, hvor forbindelsen til internetudbyderens server er etableret via telefonnettet, vil være af betydning ved undersøgelsen af, hvorfra opkaldet er etableret. Politiet vil dermed hurtigere kunne målrette efterforskningen mod den reelle gerningsmand. Dette medvirker til at styrke retssikkerheden for den kunde, hvis internetkonto måtte være blevet misbrugt til at skaffe kriminelle adgang til Internettet. Her vil det kunne være af væsentlig betydning for efterforskningen straks at kunne fastslå, at opkaldet til internetudbyderen er etableret fra en telefon, som kunden ikke kan have haft adgang til. Justitsministeriet finder, at

der i forbindelse med den nærmere regelfastsættelse må foretages en afvejning af på den ene side det efterforskningsmæssige behov for denne type af oplysninger og på den anden side de tekniske vanskeligheder ved en logning heraf.

Registrering af B-nummeret vil have betydning i de tilfælde, hvor udbyderen stiller flere forskellige telefonnumre til rådighed for deres kunder med henblik på at etablere forbindelse til Internettet. Her vil man ved at sammenholde B-nummeroplysningerne fra det telefonselskab, som kunden anvender, have en ekstra sikkerhed for at der er kaldt op til internetudbyderen fra pågældende kunde på det relevante tidspunkt. Herudover forekommer krav om logning af B-nummer navnlig at være relevant i forhold til teleudbyderne. Det må i forbindelse med den nærmere regelfastsættelse overvejes, om der kan påvises et sådant behov for internetudbyderes logning af B-nummer, at der bør opstilles krav herom.

Hvor forbindelsen til Internettet ikke etableres via telefonnettet, men etableres via en fast forbindelse, f.eks. såkaldte ADSL-forbindelser, vil der ikke være teknisk grundlag for at opstille krav om, at internetudbyderen logger A-nummer. I stedet vil der skulle registreres de tilsvarende oplysninger, der gør det muligt at føre det elektroniske spor tilbage til en bestemt kunde.

Det skal understreges, at der ikke med forslaget lægges op til, at internetudbyderne skal foretage en kortlægning af kundernes aktiviteter, mens de anvender Internettet. Udbyderne vil således ikke løbende skulle foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger. Hensigten er som anført ovenfor at kunne føre elektroniske spor, der findes på Internettet i forbindelse med kriminelle aktiviteter tilbage til gerningsmændene.

Justitsministeriet kan derfor tiltræde udvalgets overvejelser vedrørende det nærmere indhold af reguleringen. Det må dog fremhæves, at den tekniske udvikling siden afgivelsen af Brydensholt-udvalgets betænkning – og ikke mindst de praktiske erfaringer med IT-efterforskning i denne periode – kan vise sig at have ændret behovet for omfanget af en logningsforpligtelse. Ved at lade den nærmere tekniske udmøntning finde sted ved bekendtgørelse, kan der tages højde for dette forhold. Det må således i forbindelse med den nærmere regelfastsættelse, overvejes nærmere, hvilket omfang logningsforpligtelsen skal have. Hvis der i dag ikke ses at være behov for at logge oplysninger om f.eks. sessionstype (FTP/Telnet), så skal der ikke opstilles et krav herom.

Udvalget kommer ikke ind på, om og i givet fald hvilke yderligere oplysninger der bør registreres i forbindelse med anvendelse af elektronisk post. Justitsministeriet finder, at der ikke bør stilles forslag om en generel logning af indholdsdata, men alene af oplysninger svarende til teleoplysninger, dvs. oplysninger som f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen. Den påtænkte regulering vedrørende elektronisk post vil således ikke forpligte internetudbydere til generelt at gemme indholdet af elektroniske breve. Opbevaringspligten vil være begrænset til oplysninger om, hvilken kommunikation der har fundet sted.

Det skal fremhæves, at den foreslåede logning af oplysninger om internettrafik ikke uden videre giver politiet adgang til logoplysningerne. Dette spørgsmål vil fortsat skulle afgøres efter retsplejelovens regler om edition eller indgreb i meddelelseshemmeligheden afhængigt af, hvilke logoplysninger der er tale om.

Brydensholt-udvalget anfører, at opbevaringstiden for logoplysningerne set fra et efterforskningsmæssigt synspunkt ideelt bør være 5 år, svarende til opbevaringsfristerne i bogføringsloven og hvidvaskloven. Justitsministeriet kan tilslutte sig udvalgets opfattelse af, at dette bl.a. af praktiske grunde vil være for vidtgående.

Det må derfor tilstræbes, at der fastsættes en opbevaringsperiode, der i hvert fald muliggør efterforskning i de fleste sager, hvor der er behov for disse oplysninger.

Udvalget finder, at efterforskningsmæssige hensyn taler for en frist på ikke under 1 år. Ikke mindst i sager med ekstremt store datamængder eller i sager, der efterforskningsmæssigt starter i et andet land, hvorefter det konstateres, at der skal efterforskes også i Danmark, vil en kortere frist kunne betyde, at videre efterforskning umuliggøres.

Udvalget vurderer, at for langt de fleste sagers vedkommende vil en frist på 6 måneder imidlertid være tilstrækkelig. Udvalget anbefaler på denne baggrund en opbevaringsfrist på 6 måneder. Så vidt udvalget er orienteret, opbevares loggen vedrørende e-post ofte i 6 måneder, mens der ikke i øvrigt er nogen fast praksis.

Der er, som udvalget ligeledes anfører, tale om en vanskelig afvejning mellem på den ene side hensynet til kriminalitetsbekæmpelse og på den anden side hensynet til både privatlivets fred og de omkostninger, der påføres udbyderne. Særligt vedrørende hensynet til privatlivets fred tilsiger dette hensyn, at der logges mindst muligt, og at loggen opbevares i så kort tid som muligt, idet risikoen for, at oplysningerne falder

i forkerte hænder, er større, jo længere opbevaringsperioden er.

Imidlertid tager selv terrorhandlinger af væsentlig mindre omfang end de tragiske angreb på New York og Washington den 11. september 2001 normalt lang tid at planlægge. Justitsministeriet finder det i lyset heraf tvivlsomt, om en opbevaringsfrist på kun 6 måneder dækker det behov for adgang til oplysninger, som politiet måtte have i en konkret sag. Efter Justitsministeriets opfattelse bør der derfor lægges afgørende vægt på de efterforskningsmæssige hensyn, der – som Brydensholt-udvalget påpeger – taler for en frist på ikke under 1 år. Justitsministeriet stiller på den baggrund forslag om en lovfæstet opbevaringsperiode på 1 år.

Det bemærkes i den forbindelse, at Justitsministeriet samtidig foreslår, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse. Der henvises herved til lovforslagets § 8.

3.1.3.3. Lovtekniske overvejelser

I det lovudkast, der har været sendt i høring, lagde Justitsministeriet ikke op til, at logningspligten skulle fremgå direkte af retsplejeloven. I stedet skulle reguleringen gennemføres ved bekendtgørelse. Justitsministeriet anførte i den forbindelse, at både praktiske og lovtekniske forhold taler for, at den foreslåede regulering foretages administrativt ved bekendtgørelse på grundlag af en generel bemyndigelsesbestemmelse i loven.

I visse af de høringssvar, som Justitsministeriet har modtaget vedrørende lovudkastet, er det imidlertid påpeget, at forpligtelsen til at registrere og opbevare trafikdata, herunder spørgsmålet om opbevaringsperiodens udstrækning, bør fastsættes i en lov. Justitsministeriet kan tilslutte sig dette synspunkt. Det foreslås således, at det af retsplejeloven kommer til at fremgå, at det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. den foreslåede bestemmelse i retsplejelovens § 786, stk. 4, 1. pkt.

Den nærmere tekniske udmøntning foreslås imidlertid fortsat at skulle ske administrativt. Justitsministeriet foreslår således i tilknytning til den lovfæstede logningspligt og opbevaringsfrist en bemyndigelsesbestemmelse, hvorefter justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler om logningen, jf. den foreslåede bestemmelse i retsplejelovens § 786, stk. 4, 2. pkt.

Baggrunden herfor er, at de nærmere regler efter Justitsministeriets opfattelse vil være af en sådan karakter og detaljeringsgrad, at det ikke vil være hensigtsmæssigt at fastsætte dem ved lov. Endvidere vil det være ganske omstændeligt at skulle fremsætte lovforslag, når der måtte vise sig behov for justering af disse regler, der i væsentligt omfang vil være af teknisk karakter. Her vil det være mere smidigt, at justeringerne kan foretages ved ændring af en bekendtgørelse.

Samtidig har de tidsmæssige rammer for udarbejdelsen af dette lovforslag ikke muliggjort, at der har kunnet skabes klarhed over alle de tekniske aspekter af forslaget, herunder gennem inddragelse af tele- og internetbranchen. Behovet for regulering vil skulle vurderes i lyset af de praktiske og tekniske muligheder, der ikke har kunnet afklares endeligt inden for den korte tidsfrist.

Justitsministeriet forudsætter som anført, at tele- og internetbranchen inddrages i forbindelse med regelfastsættelsen i forbindelse med udnyttelse af bemyndigelsen.

Henset til, at ordningen med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold udgør en nyskabelse i forhold til den gældende retstilstand, foreslår Justitsministeriet, at ordningen evalueres nogle år efter dens iværksættelse. Bestemmelsen i lovforslagets § 8 indebærer, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse.

Der henvises til lovforslagets § 2, nr. 3, og § 8.

3.2. Politiets praktiske muligheder for at foretage indgreb i meddelelseshemmeligheden

De hårde konkurrenceforhold i telesektoren medfører, at teleudbyderne i vidt omfang tilskyndes til at begrænse driftsomkostningerne. De udbydere, som anvender ressourcer på at samarbejde med politiet, herunder f.eks. ved at opbygge en sikkerhedsorganisation med døgnbetjening, kan derfor blive stillet ringere i konkurrencen med de udbydere, der ikke prioriterer denne opgave.

Det kan i praksis vanskeliggøre eller endda umuliggøre politiets efterforskning i en konkret sag, hvis politiet ikke har mulighed for på alle tider af døgnet at komme i kontakt med teknisk kyndigt personale, når der f.eks. skal etableres telefonaflytning eller indhentes teleoplysninger. Under pkt. 3.2.1. nedenfor beskrives nogle af de praktiske problemer, der kan opstå i forbindelse med politiets samarbejde med teleselskaberne.

Efter Justitsministeriets opfattelse ville det være at foretrække, at den fornødne bistand til politiet kunne

sikres gennem selvregulering i telebranchen og på grundlag af aftaler mellem politiet og selskaberne.

Samarbejdet mellem politiet og teleselskaberne fungerer i praksis tilfredsstillende på langt de fleste punkter. Dette forhindrer imidlertid ikke, at der i forbindelse med visse former for bistand eller i forhold til visse selskaber opstår tekniske eller praktiske problemer.

Samtidig har forholdene på teleområdet, herunder navnlig antallet af teleudbydere, udviklet sig således, at det er vanskeligt på alle punkter at sikre den fornødne standard og ensartethed på tværs af teleselskaberne alene gennem interne regler mv. i branchen.

Telelovgivningens krav om nummerportabilitet indebærer endvidere, at det ikke er muligt alene ud fra et telefonnummer at afgøre, hvilket selskab, der har det pågældende kundeforhold. En kunde kan således medtage sit gamle telefonnummer ved operatørskift. Når fuld nummerportabilitet er en realitet, vil det end ikke være muligt at fastslå, om et givent telefonnummer vedrører en fastnettelefon eller en mobiltelefon. Teleselskaberne har oprettet det såkaldte Operator's Clearing House (OCH), der indeholder opdaterede oplysninger om operatørtilknytning for så vidt angår alle telefonnumre her i landet.

Selv om der således på visse områder kan være behov for en mere generel regelfastsættelse, udelukker det ikke, at telebranchen inddrages i regelfastsættelsen. Tværtimod tilsiger hensynet til en hensigtsmæssig udformning af den nærmere regulering, herunder ikke mindst de tekniske aspekter, at reguleringen udformes efter dialog med telebranchen.

Udbydere af offentlige telenet eller teletjenester har efter retsplejelovens § 786, stk. 1, pligt til at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden. Lov om konkurrence- og forbrugerforhold på teleområdet § 15, stk. 3, indeholder en bemyndigelsesbestemmelse, hvorefter ministeren for videnskab, teknologi og udvikling efter forhandling med justitsministeren kan fastsætte nærmere regler om udbyderens bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden. Denne bemyndigelse er imidlertid ikke udnyttet.

De hensyn, der varetages gennem fastsættelse af regler i medfør af denne bestemmelse, vil i højere grad være af kriminalitetsbekæmpende karakter end af telepolitisk karakter.

Efter Justitsministeriets og Ministeriet for Videnskab, Teknologi og Udviklings opfattelse hører bemyndigelsesbestemmelsen derfor naturligt hjemme i retsplejeloven. Det foreslås på denne baggrund, at denne bemyndigelsesbestemmelse erstattes af en tilsvarende bestemmelse i retsplejelovens § 786, stk. 5, dog således at adgangen til at fastsætte regler tilkommer justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling. Også her forudsættes det, at tele- og internetbranchen inddrages i forbindelse med regelfastsættelsen.

Der henvises til lovforslagets § 2, nr. 3, og § 3, nr. 1.

3.2.1. Kontakten mellem politiet og teleselskaberne

For at gøre politiet i stand til at rette henvendelse til det eller de relevante teleselskaber vil der kunne være behov for at sikre politiet hurtig adgang til oplysninger om, hvilket teleselskab, der varetager kundeforholdet vedrørende et bestemt telefonnummer, jf. pkt. 3.2 ovenfor om nummerportabilitet og det såkaldte Operator's Clearing House. Udlevering af oplysninger fra OCH sker efter retsplejelovens regler om edition, sammenlign herved de foreslåede regler om adgang for politiet til selv at træffe beslutning om edition, hvor en retskendelse ikke kan afventes, uden at indgrebets øjemed ville forspildes.

I praksis giver det endvidere anledning til efterforskningsmæssige vanskeligheder, at ikke alle udbydere har et døgnbemandet kontaktpunkt, hvortil politiet kan rette henvendelse om f.eks. etablering af aflytning og udlevering af teleoplysninger.

Endvidere indebærer betingelserne for, at retten kan træffe beslutning om indgreb i meddelelseshemmeligheden, at der almindeligvis vil være tale om alvorlige sager, der ofte indeholder følsomme oplysninger, som skal behandles fortroligt.

Det er væsentligt for en effektiv efterforskning og retsforfølgning i disse sager, at teleselskaberne har personale, der er i stand til at behandle disse oplysninger sikkerhedsmæssigt forsvarligt og med en sådan hurtighed, som det efterforskningsmæssige behov tilsiger.

I praksis kan det være helt afgørende, at der er mulighed for straks at etablere en aflytning. Hvis politiet i en sådan situation er henvist til at rette henvendelse inden for almindelig arbejdstid, er der risiko for at formålet med aflytningen forspildes.

Efter den foreslåede bemyndigelsesbestemmelse i retsplejelovens § 786, stk. 5, vil der eksempelvis kunne fastsættes regler, der sikrer politiet mulighed for at kunne komme i kontakt med teleselskaberne hele døgnet. Der vil også kunne opstilles regler om sikkerhedsgodkendelse af personale.

Sådanne regler kan dog ikke være mere vidtgående, end formålet tilsiger. Ved fastsættelse af regler om udvidet adgang til at rette henvendelse til selskaberne vil der således skulle foretages en afvejning mellem på

den ene side det efterforskningsmæssige behov for at kunne rette henvendelse uden for almindelig arbejdstid og på den anden side de økonomiske konsekvenser for selskaberne af en sådan ordning. Der vil ikke altid være behov for at kræve, at der er personale til stede hele døgnet i teleselskabet. Alt efter behov vil der kunne være tale om en vagtordning, hvor politiet har adgang til at rette henvendelse til bestemte medarbejdere i det pågældende teleselskab, der kan sørge for det videre fornødne i forhold til gennemførelsen af indgreb i meddelelseshemmeligheden.

3.2.2. Ansvaret for etablering af aflytninger mv.

Den nuværende struktur på telemarkedet, hvor et selskab kan være ejer af de fysiske installationer, der muliggør kommunikationen (netværk, centraler mv.), mens et andet selskab varetager kundeforholdet, giver også i praksis anledning til vanskeligheder.

Det kan forekomme, at et selskab, der i en sådan situation er ejer af de fysiske installationer, afviser politiets anmodning om bistand med den begrundelse, at den pågældende abonnent ikke er kunde hos selskabet, mens selskabet med kundeforholdet henviser til, at man ikke teknisk har adgang til eksempelvis at etablere en aflytning.

Den nærmere regulering af dette forhold efter den foreslåede bemyndigelsesbestemmelse i retsplejelovens § 786, stk. 5, kan i sagens natur ikke gribe ind i de ejendomsretlige forhold vedrørende de tekniske installationer, men problemet vil f.eks. kunne løses ved at fastsætte regler om et samarbejde i form af konkret informationsudveksling mellem de berørte teleselskaber.

3.2.3. Politiets adgang til abonnentoplysninger

Efter § 34, stk. 3, i lov om konkurrence- og forbrugerforhold på telemarkedet kan en telefonabonnent kræve, at den pågældendes nummeroplysningsdata ikke oplyses i forbindelse med udbud af nummeroplysningstjenester eller videregives til andre (såkaldte hemmelige og udeladte numre). Uanset denne bestemmelse skal disse nummeroplysningsdata altid videregives til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste, jf. § 34, stk. 4, nr. 2. Efter § 34, stk. 5, kan oplysninger som nævnt i § 34, stk. 4, nr. 2, alene videregives af forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste til brug for besvarelse af henvendelser fra den offentlige alarmtjeneste.

Af bemærkningerne til § 34 fremgår, at stk. 4, nr. 2, og stk. 5 skal sikre, at den nummeroplysningsdatabase (»118«), som er omfattet af forsyningspligten, indeholder alle telefonnumre, der er tildelt til slutbrugere og anvendes som slutbrugernumre, med henblik på at sådanne nummer oplysningsdata kan videregives til den offentlige alarmtjeneste, jf. Folketingstidende 1999-2000, tillæg A, s. 6990-6991. Disse nummeroplysningsdata kan efter de gældende bestemmelser ikke videregives til andre end alarmtjenesten. Den offentlige alarmtjeneste omfatter alle de offentlige alarmfunktioner, der bestrides af politiet, Københavns Brandvæsen og andre.

Politiet kan således ikke i forbindelse med en efterforskning anvende databasen. Forsyningspligtudbyderen (TDC Tele Danmark A/S) er kun forpligtet til at udlevere oplysninger til politiet fra databasen om abonnementsforhold, som den pågældende abonnent ønsker hemmeligholdt, hvis der foreligger en editionskendelse, jf. retsplejelovens § 806, jf. § 804.

Politiet har ikke efter de gældende bestemmelser mulighed for selv at træffe beslutning om edition – heller ikke i tilfælde, hvor indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes.

Der er i praksis to muligheder for at give politiet en bedre og mere effektiv adgang til oplysninger om teleabonnenter.

Den første mulighed består i at give politiet adgang til selv at træffe beslutning om edition. Dette muliggøres med den foreslåede ændring af retsplejelovens regler om edition, jf. lovforslagets § 2, nr. 9. Der henvises herom til pkt. 3.5. nedenfor samt til bemærkningerne til lovforslagets § 2, nr. 9.

Denne ændring vil indebære, at politiet enten – som hidtil – kan indhente en editionskendelse fra retten eller selv har mulighed for at træffe beslutning om edition, hvor en retskendelse ikke kan afventes, uden at indgrebets øjemed ville forspildes.

Betingelserne for edition vil være opfyldt, hvis efterforskningen vedrører en lovovertrædelse, der er undergivet offentlig påtale, og der er grund til at antage, at de oplysninger, som ønskes fremlagt kan tjene som bevis.

Der vil i praksis næppe forekomme tilfælde, hvor disse betingelser ikke er opfyldt med hensyn til oplysninger om navn og adresse på kunder til bestemte telefonnumre. De praktiske problemer opstår først og fremmest ved, at der går en vis tid, inden teleselskaberne kan levere de ønskede oplysninger.

I praksis indhenter politiet ofte en editionskendelse samtidig med kendelser om indgreb i meddelelseshemmeligheden i form af teleoplysning eller udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4. Dette indebærer i praksis, at politiet har adgang til abonnentoplysninger vedrørende de numre, som et

indgreb i meddelelseshemmeligheden måtte omfatte. Dette løser dog ikke problemet med ventetid på levering af oplysningerne.

Efter Justitsministeriets opfattelse findes det på baggrund af det anførte ikke betænkeligt at vælge den anden mulighed for at give politiet en bedre og mere effektiv adgang til abonnentoplysninger. Denne består i, at give politiet direkte (on-line) adgang til oplysningerne i forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste, uden at der foreligger en kendelse eller beslutning om edition.

Den således foreslåede ændring af § 34, stk. 5, vil ikke indebære, at politiet i praksis får adgang til oplysninger, som ikke i dag er tilgængelige for politiet. Formålet med forslaget er alene at sikre, at politiet på den mest effektive måde selv kan søge og hente de pågældende oplysninger i databasen.

På en række området har politiet allerede i dag direkte adgang til oplysninger i forskellige databaser, der indeholder personoplysninger. Det gælder eksempelvis Det Centrale Personregister (CPR), der bl.a. indeholder beskyttede adresseoplysninger. Her er det således ikke nødvendigt for politiet at rette henvendelse til et folkeregister med en editionskendelse for at få adgang til de ønskede oplysninger. Tilsvarende har politiet adgang til oplysninger i Centralregistret for Motorkøretøjer, der indeholder oplysninger om navn og adresse på ejere af motorkøretøjer, der er indregistreret i Danmark.

Samtidig vil den foreslåede ordning reducere politiets behov for at kunne kontakte teleselskaberne hele døgnet, jf. pkt. 3.2.1. ovenfor.

En ordning som den foreslåede kendes i dag f.eks. i norsk ret. Efter § 9-3 i den norske lov om telekommunikation (teleloven) af 23. juni 1995 har politiet adgang til oplysninger om navn, adresse, telefonnummer og datakommunikationsadresse uden kendelse.

Der henvises til lovforslagets § 3, nr. 2.

3.3.Ransagning

3.3.1. Gældende ret

Retsplejelovens regler om ransagning, der er indsat ved lov nr. 411 af 10. juni 1997, findes i lovens kapitel 73 (§§ 793-799). Der henvises herom til Folketingstidende 1996-97, forhandlingerne, s. 2202-2215, 7453 og 7938, tillæg A, s. 2475-2538, samt tillæg B, s. 988-993 og 1294-1299. Reglerne bygger på Strafferetsplejeudvalgets betænkning 1159/1989 om ransagning under efterforskning.

Herudover indeholder retsplejeloven i §§ 759 og 761 regler om ransagning med henblik på at finde en mistænkt, der skal anholdes, eller en person, der skal pågribes for at fuldbyrde en straffedom eller forvandlingsstraffen for bøde. Retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden indeholder desuden regler om undersøgelse af breve, telegrammer og lignende under forsendelse, og kapitel 72 indeholder regler om undersøgelse af en persons legeme og visitation af det tøj, som den pågældende er iført.

Såfremt de i retsplejelovens kapitel 73 nævnte betingelser er opfyldt, kan politiet ifølge § 793, stk. 1, foretage ransagning af (1) boliger og andre husrum (f.eks. kontorer, værksteder mv.), dokumenter, papirer og lignende (f.eks. elektronisk lagrede dokumenter) og indholdet af aflåste genstande samt (2) andre genstande og lokaliteter uden for husrum (f.eks. uaflåste tasker, kufferter eller biler).

Undersøgelser af lokaliteter eller genstande, som er frit tilgængelige for politiet, er ikke omfattet af reglerne om ransagning, jf. stk. 2.

Efter § 794, stk. 1, må ransagning af husrum og andre lokaliteter eller genstande, *som en mistænkt råder over,* kun foretages, hvis (1) den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og (2) ransagningen må antages at være af væsentlig betydning for efterforskningen.

Hvis der er tale om ransagning i medfør af § 793, stk. 1, nr. 1, af boliger og andre husrum, dokumenter, papirer og af indholdet af aflåste genstande kræves efter stk. 2 desuden, at sagen angår en lovovertrædelse, der efter loven kan medføre fængselsstraf, eller at der er bestemte grunde til at antage, at der ved ransagningen kan findes bevis i sagen eller genstande, der kan beslaglægges.

Efter stk. 3, må der ikke foretages ransagning af skriftlige meddelelser eller lignende, der findes hos en mistænkt, hvis meddelelsen hidrører fra en person, der efter reglerne i § 170 er udelukket fra at afgive forklaring som vidne i sagen (dvs. præster, læger, forsvarere og advokater). Det samme gælder materiale, som hidrører fra en person, der er omfattet af § 172 (redaktører og redaktionelle medarbejdere), når materialet indeholder oplysninger, som den pågældende er fritaget for at afgive forklaring om som vidne i sagen.

Ransagning hos en *person, der ikke er mistænkt,* må kun finde sted, såfremt (1) efterforskningen vedrører en lovovertrædelse, der efter loven kan medføre fængselsstraf, og (2) der er bestemte grunde til at antage, at bevis i sagen eller genstande, der kan beslaglægges, kan findes ved ransagningen, jf. § 795, stk. 1.

Ransagning kan herudover alene finde sted hos en *person, der ikke er mistænkt,* hvis den pågældende

Til § 2

Retsplejeloven

Til nr. 1 (overskriften til retsplejelovens kapitel 71)

Ændringen af overskriften til kapitel 71 er en konsekvens af den foreslåede nye regel i § 791 b om dataaflæsning, jf. forslagets § 2, nr. 4.

Til nr. 2 og 3 (retsplejelovens § 786, stk. 1, 4, 5, 6 og 7)

Den foreslåede ændring af *retsplejelovens § 786, stk. 1,* indebærer, at det vil påhvile også udbydere af telenet og teletjenester, der henvender sig til afgrænsede kundesegmenter, at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden. Som det fremgår under pkt. 3.1.3. ovenfor finder Justitsministeriet, at både hensynet til en effektiv regulering og hensynet til konkurrenceforholdene i branchen tilsiger, at der skal kunne stilles krav til udbyderne, uanset til hvilke kundegrupper de udbyder telenet og teletjenester.

Den foreslåede bestemmelse i *retsplejelovens § 786, stk. 4,* fastsætter i *1. pkt.* en pligt for udbydere af telenet og teletjenester til at foretage registrering og opbevaring (logning) i 1 år af de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold. Endvidere gives der i *2. pkt.* hjemmel til, at justitsministeren ved bekendtgørelse kan fastsætte nærmere regler om logningspligtens indhold og omfang..

Både udbydere af offentlige telenet og teletjenester og udbydere, der henvender sig til specifikke, på forhånd afgrænsede kundesegmenter, vil kunne omfattes af den foreslåede regulering.

For så vidt angår *teletrafik* vil de oplysninger, som logningspligten kan omfatte, navnlig være de oplysninger, som politiet har brug for i forbindelse med indgreb i meddelelseshemmeligheden i form af teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4. Det kan eksempelvis være det kaldende og det kaldte nummer (A- og B-nummer), opkaldstidspunkter og varigheden af samtaler samt – for mobiltelefoners vedkommende – oplysninger om anvendte sendemaster/celler.

For så vidt angår *internettrafik* vil der kunne fastsættes regler om logning af den dynamiske tildeling af IP-adresser, tidspunkt for opkobling og nedkobling samt opkoblingens varighed. I praksis vil udbyderen kun være i stand til at levere oplysninger om, hvem der har efterladt et elektronisk spor på Internettet, hvis udbyderen er i besiddelse af præcise oplysninger om, hvilken kunde, der på det pågældende tidspunkt har anvendt en tildelt IP-adresse.

Det må overvejes i forbindelse med den nærmere regelfastsættelse, om der er behov for at stille krav om, at internetudbydere ved opkobling via telefonnettet skal logge A og B-nummeret. Som anført under pkt. 3.1.3.2. ovenfor har det over for Justitsministeriet været fremført, at der i praksis vil kunne være tekniske hindringer for internetudbyderes registrering af det kaldende nummer (A-nummeret).

Hvor forbindelsen til Internettet ikke etableres via telefonnettet, men etableres via en fast forbindelse, f.eks. såkaldte ADSL-forbindelser, vil der ikke være teknisk grundlag for at opstille krav om, at internetudbyderen logger A-nummeret. I stedet vil der skulle registreres de tilsvarende oplysninger, der gør det muligt at føre det elektroniske spor tilbage til en bestemt kunde.

Der vil kunne opstilles regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger, f.eks. i en periode efter at et kundeforhold er bragt til ophør. Også spørgsmålet om opbevaring af oplysningerne her i landet, hvor udbyderen er en filial af en udenlandsk virksomhed, vil også kunne reguleres.

Endvidere bør det tilstræbes, at reglerne sikrer, at korrekt dansk realtid registreres.

Der vil ikke kunne fastsættes regler om, at internetudbyderne løbende skal foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger. Hensigten med forslaget er alene at kunne føre elektroniske spor, der findes på Internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

For så vidt angår *elektronisk post* stilles der ikke forslag om en generel logning af indholdsdata, men alene af oplysninger svarende til teleoplysninger, dvs. oplysninger som f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen. Den nærmere regulering vedrørende elektronisk post vil således ikke kunne forpligte internetudbydere til generelt at gemme indholdet af elektroniske breve.

Opbevaringsperioden vil være 1 år for de oplysninger, der ikke opbevares med henblik på debitering. Trafikdata, der gemmes med henblik på debitering, vil – uanset om de pågældende data omfattes af den lovbestemte logningspligt – som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktivet og § 30, stk. 2, i bekendtgørelse om udbud af telenet og teletjenester. Dette in-

debærer i praksis, at oplysningerne kan gemmes i op til 5 år.

Det forudsættes, at de nærmere regler fastsættes efter dialog med tele- og internetudbyderne. Dette er ikke mindst afgørende for at sikre en hensigtsmæssig teknologisk udformning af reglerne.

Der henvises i øvrigt til pkt. 3.1.2. og 3.1.3. i de almindelige bemærkninger til lovforslaget.

Efter den foreslåede bestemmelse i *retsplejelovens § 786, stk. 5,* vil der kunne fastsættes nærmere regler om udbydere af telenet eller teletjenesters praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden. Også på dette punkt vil både udbydere af offentlige telenet og teletjenester og udbydere, der henvender sig til specifikke, på forhånd afgrænses kundesegmenter, kunne omfattes af den foreslåede regulering.

Bestemmelsen svarer til den gældende bestemmelse i § 15, stk. 3, i lov om konkurrence- og forbrugerforhold på teleområdet, dog med den forskel, at bemyndigelsen til at fastsætte regler foreslås overført til justitsministeren. Baggrunden herfor er, at de hensyn, der varetages gennem fastsættelse af regler i medfør af denne bestemmelse, i højere grad vil være af kriminalitetsbekæmpende karakter end af telepolitisk karakter. § 15, stk. 3, foreslås samtidig ophævet, jf. lovforslagets § 3, nr. 1.

De administrative forskrifter vil f.eks. kunne omfatte regler om døgnbemanding af kontaktpunkter vedrørende etablering af aflytning og indhentelse af teleoplysninger mv., sikkerhedsgodkendelse af personale, der håndterer fortroligt materiale samt afklaring af, hvem pligten til at bistå politiet påhviler. Den sidste problemstilling opstår, når de fysiske installationer på den ene side og kundeforholdet på den anden side ligger hos forskellige selskaber.

Der tilsigtes imidlertid ikke hermed en udtømmende angivelse af, hvilke forhold der kan reguleres. Formålet med bestemmelsen er, at der løbende kan tages højde for praktiske og tekniske problemer, der måtte opstå i forbindelse med samarbejdet mellem politiet og udbyderne.

Der henvises i øvrigt til pkt. 3.2, herunder pkt. 3.2.1. og 3.2.2., i de almindelige bemærkninger til lovforslaget.

Efter den foreslåede bestemmelse i *retsplejelovens § 786, stk. 6,* vil forsætlig eller uagtsom overtrædelse af logningspligten kunne straffes med bøde. Der kan endvidere pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Efter den foreslåede bestemmelse i *retsplejelovens § 786, stk. 7,* vil der kunne fastsættes regler om bødestraf for forsætlig eller uagtsom overtrædelse af de udfyldende regler om logningspligten, jf. stk. 4, 2. pkt., og om praktisk bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden, jf. stk. 5. Der kan endvidere fastsættes bestemmelser om at pålægge selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til nr. 4 (retsplejelovens § 791 b)

Bestemmelsen i stk. 1 indebærer, at politiet – uden at være til stede der, hvor et informationssystem benyttes – ved hjælp af edb-programmer eller andet udstyr løbende kan aflæse ikke offentligt tilgængelige oplysninger i informationssystemet. Det foreslås, at indgrebet betegnes som »dataaflæsning«.

Den foreslåede bestemmelse giver adgang for politiet til at foretage dataaflæsning i et informationssystem af oplysninger, *der ikke er offentligt tilgængelige.* Aflæsning af oplysninger som er offentligt tilgængelige, således at politiet har fri adgang hertil – f.eks. fordi oplysningerne er lagt ud på en offentligt tilgængelig hjemmeside på Internettet – udgør ikke i sig selv et straffeprocessuelt tvangsindgreb og er derfor ikke omfattet af reglen om dataaflæsning.

Ved *et informationssystem* forstås en computer eller andet databehandlingsanlæg. Omfattet heraf er navnlig personlige computere, herunder både stationære og bærbare computere. Også andet elektronisk udstyr vil imidlertid kunne være omfattet af bestemmelsen, hvis udstyret har funktioner svarende til dem, der findes i personlige computere. Det gælder således elektronisk udstyr, der kan anvendes til at oprette og/eller behandle dokumenter, billeder og lyde, udføre regnskabsfunktioner og lignende, herunder også hvis sådanne funktioner senere forekommer i kombination med andet elektronisk udstyr, f.eks. et fjernsyn. Bestemmelsen vil således f.eks. omfatte en elektronisk kalender, som er indrettet så den ud over anvendelsen som kalender, desuden kan anvendes til at sende og modtage elektroniske meddelelser samt indhente oplysninger fra Internettet mv.

Indgreb i form af dataaflæsning omfatter bl.a. den situation, hvor politiet ved hjælp af et såkaldt »snifferprogram«, får tilsendt kopi af samtlige indtastninger, som brugeren af edb-udstyret foretager, herunder åbning af computeren, oprettelse af nye dokumenter og regnskaber mv. og nye indtastninger i allerede eksisterende dokumenter, eller af visse nærmere angivne indtastninger.

Sådanne edb-programmer kan endvidere gøre det muligt for politiet automatisk og uden den pågældendes vidende at modtage kopi af e-post, der afsendes fra en computer, og af opslag på Internettet, der foretages på computeren. En kendelse om aflæsning i medfør af den foreslåede bestemmelse vil også omfatte aflæsning af elektroniske meddelelser, der modtages i computeren. Det er ikke et krav, at den elektroniske meddelelse skal være åbnet og læst af modtageren, men den skal være modtaget af den computer, som indgrebet omfatter.

For elektroniske meddelelser, som er under forsendelse, gælder reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71.

Dataaflæsning af computere mv. i medfør af bestemmelsen kan ske ved hjælp af (teknisk) udstyr, der fysisk installeres i computeren, eller, i det omfang dette er teknisk muligt, ved at edb-programmer eller lignende sendes til den pågældende computer. Det forudsættes, at rettens tilladelse til aflæsning også giver politiet mulighed for at skaffe sig adgang til det pågældende edb-udstyr, hvis dette er nødvendigt for at installere det tekniske udstyr, der skal anvendes ved indgrebet, sådan som det også i dag gælder med hensyn til installation af rumaflytningsudstyr og udstyr til observation af personer i bolig og andre husrum.

Indgrebet kan således indebære en løbende undersøgelse fra et andet sted af det materiale, der til enhver tid kan findes i computeren.

Den foreslåede regel begrænser ikke den adgang, der er efter de gældende regler om ransagning til at tilvejebringe oplysninger af denne art. Ligeledes berøres adgangen til efter reglerne om indgreb i meddelelseshemmeligheden at få teleoplysninger eller at »aflytte« elektroniske meddelelser ikke af den foreslåede nye bestemmelse.

Hvis et indgreb kun indebærer, at der sker »aflytning« af elektroniske meddelelser, kan dette fortsat ske efter reglerne om aflytning af telefonsamtaler eller anden tilsvarende telekommunikation, også når en sådan aflytning sker ved hjælp af teknisk udstyr, der har lighed med det, som er omfattet af reglen i § 791 b.

Det foreslås, at betingelserne for indgreb i form af dataaflæsning udformes med udgangspunkt navnlig i de regler, som i dag gælder for indgreb i meddelelseshemmeligheden, jf. § 781, stk. 1, og for hemmelig ransagning, jf. § 799. Det foreslås således som betingelse, at indgrebet må antages at være af afgørende betydning for efterforskningen, og at der er bestemte grunde til at antage, at den pågældende computer mv. anvendes i forbindelse med forbrydelsen.

Det skal for det første efter *stk. 1, nr. 1,* være en betingelse, at der er *bestemte grunde* til at antage, at et informationssystem anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3. Kravet om, at der skal være bestemte grunde til den nævnte antagelse, svarer til det krav, der stilles ved bestemmelsen i § 781, stk. 1, nr. 1, om indgreb i meddelelseshemmeligheden, og ved bestemmelsen i § 791 a, stk. 3, nr. 1, om observation af personer i bolig eller andre husrum.

Det skal endvidere kunne antages, at det pågældende informationssystem benyttes i forbindelse med udførelsen af den kriminalitet, der er nævnt i stk. 3.

Det er uden betydning, hvem informationssystemet tilhører. Indgrebet kan således rettes mod mistænktes eget edb-udstyr eller f.eks. en privat computer, der tilhører en anden end den mistænkte, eller mistænktes computer på arbejdspladsen, uanset om computeren også benyttes af andre. Såfremt betingelserne for dataaflæsning i øvrigt er opfyldt – herunder kravet i § 791 b om proportionalitet – kan der således også ske dataaflæsning af computere på biblioteker, internetcaféer og lignende. Dette adskiller sig ikke fra, hvad der gælder for telefonaflytning.

I *stk. 1, nr. 2,* foreslås, at indgrebet kan foretages, hvis det er af *afgørende betydning for efterforskningen* (indikationskravet), jf. herved også det tilsvarende krav i § 781, stk. 1, nr. 2 (indgreb i meddelelseshemmeligheden), i § 791 a, stk. 3, nr. 2 (observation af personer i bolig eller andre husrum) og i § 799, stk. 1, 1. pkt. (hemmelig ransagning).

Ved denne betingelse angives, at indgrebet skal have en meget væsentlig betydning for efterforskningen af den pågældende sag, men bestemmelsen indebærer ikke, at indgrebet skal være den eneste mulighed for efterforskning i sagen, eller at andre af de straffeprocessuelle indgreb i retsplejeloven ikke samtidig kan anvendes.

Kriminalitetskravet i *stk. 1, nr. 3,* foreslås udformet, således at indgreb i form af dataaflæsning kan foretages, hvis efterforskningen angår en forsætlig overtrædelse af straffelovens kapitel 12 og kapitel 13 eller en overtrædelse af straffelovens §§ 180, 183, stk. 1 og 2, 183 a, 186, stk. 1, 187, stk. 1, 191, 192 a og 237. Dette svarer til kriminalitetskravet ved hemmelig ransagning.

Der er således ikke mulighed for at iværksætte dataaflæsning i medfør af den foreslåede bestemmelse på grundlag om en mistanke om, at computerudstyr f.eks. anvendes til fremstilling af falske pas eller andre falske dokumenter, medmindre der samtidig foreligger mistanke om, at fremstillingen sker som et led i

forberedelsen af en af de i bestemmelsen nævnte alvorlige lovovertrædelser – f.eks. flykapring.

Stk. 2 indeholder en proportionalitetsgrundsætning svarende til reglen i § 782, stk. 1, om indgreb i meddelelseshemmeligheden og § 791 a, stk. 5, om observation.

Efter *stk. 3* skal kompetencen til at træffe bestemmelse om aflæsning af computere mv. efter den foreslåede § 791 b – ligesom ved indgreb i meddelelseshemmeligheden, observation og hemmelig ransagning – henhøre under retten. Bestemmelsen henviser til kompetencebestemmelsen i § 783 om indgreb i meddelelseshemmeligheden.

I en kendelse, der tillader aflæsning, må det angives, hvilket informationssystem (computer eller lignende databehandlingsanlæg) indgrebet skal angå, jf. de foreslåede bestemmelser i § 791 b, stk. 3, 1. og 2. pkt. Er det ikke muligt for politiet at give nærmere oplysninger om edb-udstyrets fabrikat, nummer eller lignende, der entydigt kan identificere dette, kan der i stedet afsiges kendelse om, at indgrebet skal angå det edb-udstyr, der benyttes på et bestemt, nærmere afgrænset sted, f.eks. en bestemt privatadresse eller et bestemt kontor på en arbejdsplads.

En computer eller andet tilsvarende edb-udstyr kan efter omstændighederne også identificeres ved en angivelse af, hvem der har rådighed herover, f.eks. den bærbare computer, som tilhører den mistænkte.

Efter § 783, stk. 2, skal der i kendelsen fastsættes et tidsrum, inden for hvilket indgrebet kan foretages. Tidsrummet skal være så kort som muligt og må ikke overstige 4 uger. Tidsrummet kan forlænges ved en ny kendelse, men højst med 4 uger ad gangen.

Den foreslåede regel i *stk. 4* indebærer, at en række af de regler, der gælder for indgreb i meddelelseshemmeligheden og for observation af personer i bolig eller andet husrum, også skal finde anvendelse ved aflæsning af registreringer i computere mv.

Således gælder bestemmelserne i § 788, stk. 1, 3 og 4, om efterfølgende underretning om indgrebet. En bestemmelse, der erstatter § 788, stk. 2, om hvem der skal have underretning om et foretaget indgreb, foreslås udformet sådan, at underretningen skal gives til den, der har rådigheden over computeren. Underretning skal således normalt gives til ejeren af den pågældende computer mv. En bruger, som ikke er ejer af en computer mv., kan dog have en sådan rådighed over denne, at underretning skal ske til den pågældende, f.eks. hvis der er foretaget aflæsning af en computer, som en arbejdsgiver har stillet til rådighed for en arbejdstager i dennes hjem.

Stk. 4 henviser endvidere til § 782, stk. 2, hvorefter der ikke må foretages aflytning mv. med hensyn til den mistænktes forbindelse med personer, der efter § 170 er udelukket fra at afgive forklaring som vidne, til §§ 784-785 om advokatbeskikkelse, § 789 om politiets adgang til at anvende de oplysninger, der er fremkommet ved indgrebet, og § 791 om politiets adgang til at opbevare det fremkomne materiale.

Der henvises i øvrigt til pkt. 3.4.2.

Til nr. 5 (retsplejelovens § 799, stk. 1, 1. pkt.)

Bestemmelsen indebærer en udvidelse af politiets adgang til at foretage ransagning uden at mistænkte eller andre gøres bekendt hermed (hemmelig ransagning). Efter den foreslåede bestemmelse kan der således foretages hemmelig ransagning, såfremt det er af afgørende betydning for efterforskningen, at ransagningen foretages, uden at den mistænkte eller andre gøres bekendt hermed, hvis efterforskningen angår en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af straffelovens §§ 180, 183, stk. 1 og 2, 183 a, 186, stk. 1, 187, stk. 1, 191, 192 a eller 237.

Der henvises i øvrigt til pkt. 3.3.2.1. i de almindelige bemærkninger.

Til nr. 6 (retsplejelovens § 799, stk. 3.)

Bestemmelsen indeholder en ny regel, hvorefter retten ved en kendelse, der tillader politiet at foretage ransagning, uden at mistænkte eller andre gøres bekendt hermed (hemmelig ransagning), kan tillade, at der gennemføres gentagne ransagninger.

Der henvises i øvrigt til pkt. 3.3.2.2. i de almindelige bemærkninger.

Ved forslaget gives der adgang til, at retten kan tillade politiet at foretage flere enkeltstående hemmelige ransagninger. Politiet må ved anmodningen til retten om en sådan kendelse oplyse om baggrunden for, at der findes behov for at foretage mere end en enkelt ransagning.

Der skal efter bestemmelsen i retsplejelovens § 783, stk. 2, fastsættes et tidsrum på indtil 4 uger, inden for hvilket indgrebene skal foretages. Retten kan således fastsætte en kortere tidsfrist for indgrebene. Der skal endvidere i rettens kendelse træffes nærmere bestemmelse om antallet af ransagninger, som politiet kan gennemføre inden for den fastsatte frist.

Det følger i øvrigt af henvisningen i retsplejelovens § 799, stk. 2, til § 783, stk. 3, at politiet kan gennemføre uopsættelige indgreb uden forudgående retskendelse, og at politiet i så fald snarest muligt og inden 24 timer fra indgrebets iværksættelse skal forelægge det-

te for retten. Det vil næppe i praksis forekomme, at politiet inden for 24 timer får behov for at gennemføre flere enkeltstående ransagninger uden umiddelbar underretning, men hvis dette sker, gælder fristen på 24 timer for forelæggelse for retten for hvert enkelt indgreb.

Gentagne hemmelige ransagninger sker i øvrigt under de betingelser, der er fastsat i § 799, stk. 1 og 2.

Til nr. 7 (retsplejelovens § 802, stk. 2, nr. 2, § 805, stk. 3, og § 807 d, stk. 2, 1. pkt.)

Ændringen af bestemmelsen i retsplejelovens § 802, stk. 2, nr. 2, giver adgang til beslaglæggelse af en mistænkt persons gods i tilfælde, hvor betingelserne for konfiskation efter den nye bestemmelse i § 77 a, 2. pkt., er opfyldt. Beslaglæggelse med henblik på konfiskation efter straffelovens § 77 a, 1. pkt., af genstande, som en mistænkt har rådighed over, skal fortsat ske med hjemmel i retsplejelovens § 802, stk. 1.

Ændringen er en konsekvens af lovforslagets § 1, nr. 2, hvor straffelovens § 77 a foreslås udvidet til at omfatte konfiskation af andre formuegoder (end genstande), herunder penge.

Det følger af bestemmelsen i retsplejelovens § 807 b, at beslaglæggelsen alene har virkning som arrest. En arrest sikrer, at sigtede ikke ved sine egen dispositioner over sin formue forringer denne. Beslaglæggelsen hindrer imidlertid ikke, at sigtedes øvrige kreditorer søger sig fyldestgjort gennem udlæg og efterfølgende tvangsauktion eller ved sigtedes konkurs.

Ændringen af retsplejelovens § 805, stk. 3, medfører, at både beslaglæggelse efter retsplejelovens § 802, stk. 2, (mistænkte) og § 803, stk. 1, 2. pkt. (ikke-mistænkte) ligestilles med de regler, der gælder for foretagelse af arrest (retsplejelovens § 631, stk. 2, jf. §§ 509-516), således at der alene kan foretages beslaglæggelse i de tilfælde, hvor der efter de fogedretlige regler er adgang til udlæg.

Efter § 807 d, stk. 2, 1. pkt., skal gods, der er beslaglagt efter blandt andet § 802 anvendes først til fyldestgørelse af forurettedes krav på erstatning, dernæst det offentliges krav på sagsomkostninger, dernæst konfiskation efter straffelovens § 75, stk. 1, 1. pkt., 2. led, og 2. pkt., og stk. 3, og § 76 a, stk. 5, og dernæst bødekrav, medmindre retten træffer anden bestemmelse herom. Efter lovforslaget skal denne ændring også gælde beslaglæggelse med henblik på konfiskation efter straffelovens § 77 a, 2. pkt.

Til nr. 8 (retsplejelovens § 803)

Ændringen, der er en konsekvens af den foreslåede udvidelse af straffelovens § 77 a til at omfatte andre formuegoder (end genstande), herunder penge, giver adgang til beslaglæggelse af formuegoder, som en person, der ikke er mistænkt, har rådighed over, hvis der er grund til at antage, at formuegoderne bør konfiskeres.

Beslaglæggelse med henblik på konfiskation efter straffelovens § 77 a, 1. pkt., af genstande, som en person, der ikke er mistænkt, har rådighed over, skal fortsat ske med hjemmel i retsplejelovens § 803, stk. 1, 1. pkt.

Til nr. 9 (retsplejelovens § 806, stk. 3, 1. pkt.)

Den foreslåede ændring af § 806, stk. 3, 1. pkt., indebærer, at politiet på tilsvarende måde som ved beslaglæggelse får adgang til træffe en foreløbig beslutning om pålæg af edition i tilfælde, hvor indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes (»periculum in mora«).

Som ved beslaglæggelse skal politiet, hvis den, som indgrebet retter sig imod, fremsætter anmodning om det, snarest muligt og senest inden 24 timer forelægge sagen for retten, der herefter ved kendelse afgør, om editionspålægget kan godkendes. Politiet skal vejlede den pågældende om adgangen til at få spørgsmålet om beslaglæggelsens lovlighed indbragt for retten.

Der henvises i øvrigt til pkt. 3.5 i de almindelige bemærkninger.

Til nr. 10 (retsplejelovens § 807 b, stk. 1, og § 807 d, stk. 1, 1. pkt.)

Der er tale om konsekvensændringer som følge af lovforslagets § 2, nr. 7 og 8.

Efter retsplejelovens § 807 b, stk. 1, medfører beslaglæggelse til sikring af bevismidler, genstands- og udbyttekonfiskation og vindikation, at der hverken ved aftale eller kreditorforfølgning kan foretages dispositioner over det beslaglagte, som er i strid med indgrebets formål. Med ændringen præciseres, at alene beslaglæggelse efter § 803, stk. 1,1. pkt., er omfattet af § 807 b, stk. 1.

Af retsplejelovens § 807 d, stk. 1, følger, hvornår en rådighedsberøvelse som følge af beslaglæggelse ophører. Med ændringen præciseres, at alene beslaglæggelse efter § 803, stk. 1, 1. pkt., er omfattet af reglen i § 807 d, stk. 1.

Til nr. 11 (retsplejelovens § 807 b, stk. 2, og § 807 d, stk. 2, 1. pkt.)

Der er alene tale om konsekvensændringer som følge af lovforslagets § 2, nr. 7 og 8.

Med ændringen præciseres, at beslaglæggelse efter § 803, stk. 1, 2. pkt., (beslaglæggelse hos ikke-mis-

tænkte med henblik på konfiskation efter den nye bestemmelse i straffelovens § 77 a, 2. pkt.) skal behandles efter samme regler som en beslaglæggelse efter § 802, stk. 2 (beslaglæggelse hos en mistænkt med samme sigte).

Til § 3

Lov om konkurrence- og forbrugerforhold på telemarkedet

Til nr. 1 (§ 15, stk. 3)

Dette forslag er en konsekvens af forslaget om indførelse af bemyndigelsesbestemmelsen i retsplejelovens § 786, stk. 5, jf. lovforslagets § 2, nr. 3.

Ophævelsen af adgangen for forskningsministeren (nu ministeren for videnskab, teknologi og udvikling) til efter forhandling med justitsministeren at fastsætte nærmere regler om udbyderens bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden skal således ses i sammenhæng med forslaget om indførelse af en tilsvarende bemyndigelse til justitsministeren.

Der henvises i øvrigt til pkt. 3.2 i de almindelige bemærkninger til lovforslaget.

Til nr. 2 (§ 34, stk. 5)

Den foreslåede bestemmelse vil give politiet adgang til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste, jf. § 34, stk. 4, nr. 2, i lov om konkurrence- og forbrugerforhold på telemarkedet. Nummeroplysningsdatabasen indeholder alle telefonnumre, der er tildelt slutbrugere og anvendes som slutbrugernumre.

Politiet vil på denne baggrund kunne hente oplysninger direkte i databasen uden at betingelserne for edition skal være opfyldt, og politiet vil således have (on-line) adgang til basen i samme omfang som den offentlige alarmtjeneste i dag har adgang. Formålet hermed er at give politiet en bedre og mere effektiv adgang til abonnentoplysninger.

Der henvises i øvrigt til pkt. 3.2.3. i de almindelige bemærkninger til lovforslaget.

Til § 4

Våbenloven

Den forslåede tilføjelse til § 5 i våbenloven præciserer, at forbudet i § 5 mod at tilvirke faste stoffer, væsker eller luftarter, som ved spredning virker skadevoldende, bedøvende eller irriterende, ikke kun omfatter fremstilling af kemiske og biologiske våben, men også udvikling af disse våben. Tilføjelsen udvider endvidere forbudet til at omfatte forskning.

Det bemærkes, at der efter praksis ikke gives tilladelse efter § 5, da konventionen af 10. april 1972 om forbud mod udvikling, fremstilling og oplagring af bakteriologiske (biologiske) våben og toksinvåben samt om disse våbens tilintetgørelse og konventionen af 13. januar 1993 om forbud mod udvikling, fremstilling, oplagring og anvendelse af kemiske våben og sådanne våbens tilintetgørelse bl.a. er forpligtet til ikke at udvikle eller fremstille biologiske eller kemiske våben.

Der henvises i øvrigt til pkt. 2.3.3. i de almindelige bemærkninger til lovforslaget

Til § 5

Udleveringsloven

Til nr. 1 (udleveringslovens § 2)

Efter den gældende bestemmelse kan en dansk statsborger ikke udleveres – hverken til strafforfølgning eller straffuldbyrdelse.

Forslaget indebærer, at det bliver muligt i visse situationer at udlevere en dansk statsborger til strafforfølgning (men ikke straffuldbyrdelse) i udlandet, hvis den pågældende er sigtet eller tiltalt for at have begået en alvorlig forbrydelse, eller hvis den pågældende har en mere begrænset tilknytning til Danmark.

Der henvises i øvrigt til pkt. 4.3 i de almindelige bemærkninger til lovforslaget.

Til nr. 2 (udleveringslovens § 2 a)

Som konsekvens af den foreslåede adgang til at udlevere danske statsborgere, jf. forslagets § 5, nr. 1, foreslås den gældende bestemmelse i udleveringslovens § 3, stk. 1, om udlevering af personer uden dansk statsborgerskab, af systematiske grunde udskilt til en selvstændig bestemmelse i § 2 a, idet de nugældende bestemmelser i udleveringslovens § 3, stk. 2-5, efter forslaget bliver fællesbestemmelser for udlevering af danske statsborgere (§ 2) og andre (§ 2 a).

Den foreslåede formulering af § 2 a er delvist en konsekvensændring af indsættelsen af en hjemmel til at udlevere danske statsborgere til strafforfølgning i udlandet. Den foreslåede ændring skal tydeliggøre, at § 2 a omfatter udlevering af personer, der ikke er danske statsborgere (jf. tilføjelsen af ordene »af en udlænding«), mens § 2 som affattet ved denne lov, omhandler udlevering af personer, der er danske statsborgere. Der er ikke med denne ændring tilsigtet nogen ændring af reglens anvendelsesområde.

Med udtrykket »udlænding« forstås således personer, der (udelukkende) har et andet statsborgerskab end dansk, eller som er statsløse. Personer, som både har dansk og udenlandsk statsborgerskab (dobbelt statsborgerskab), omfattes af den foreslåede § 2 om udlevering af danske statsborgere.

Endvidere fastsættes kriminalitetskravet i 2. pkt., således at ordlyden bringes i overensstemmelse med artikel 2, stk. 1, i den europæiske udleveringskonvention fra 1957. Det er herefter en betingelse for, at udlevering af en udlænding fra Danmark til en stat uden EU kan tillades, hvis den strafbare handling efter dansk ret kan straffes med fængsel i *mindst* 1 år (og ikke som hidtil handlinger, der kan medføre *højere* straf end fængsel i 1 år).

Til nr. 3 og 5 (udleveringslovens § 3)

Der er tale om en konsekvensændringer som følge af den foreslåede adgang til at udlevere danske statsborgere og udskillelsen af den hidtidige bestemmelse i udleveringslovens § 3, stk. 1, til en selvstændig bestemmelse i § 2 a om udlevering af udlændinge, jf. forslagets § 5, nr. 1 og 2.

Til nr. 4 (udleveringslovens § 3, stk. 2, nr. 1)

Ændringen af ordet »frihedsstraf« til »fængsel« er en konsekvensændring som følge af afskaffelsen af hæftestraffen, jf. lov nr. 433 af 31. maj 2000.

Til nr. 6 (udleveringslovens § 5)

Efter udleveringslovens § 5, stk. 3, finder forbudet mod at nægte udlevering for politiske lovovertrædelser mv., jf. udleveringslovens § 5, stk. 2, ikke anvendelse ved udlevering til en medlemsstat i Den Europæiske Union, når handlingen er omfattet af artikel 1 eller 2 i den europæiske konvention om bekæmpelse af terrorisme, dvs. grove forbrydelser, der retter sig mod personers liv, fysiske integritet eller frihed, f.eks. kapring af og sabotage mod luftfartøjer, grove forbrydelser mod diplomater mv., bortførelse, gidseltagning mv. og anvendelse af bomber, granater, raketter mv., der rummer fare for personer.

Endvidere finder forbudet ikke anvendelse ved udlevering for en handling, der er omfattet af artikel 2, jf. artikel 1 i FN-konventionen til bekæmpelse af terrorbombninger, jf. udleveringslovens § 5, stk. 4.

Med lovforslaget foreslås det at samle de gældende stk. 3 og 4 i et stykke. Endvidere foreslås det, at forbudet mod at nægte udlevering for politiske forbrydelser udvides til også at omfatte handlinger omfattet af artikel 2, jf. artikel 1 i FN's terrorfinansieringskonvention. Endelig foreslås det, at en udleveringsanmodning vedrørende en handling omfattet af artikel 1 eller 2 i den europæiske konvention om bekæmpelse af terrorisme fra 1977 skal være omfattet af undtagelsesbestemmelsen i det foreslåede stk. 3, uanset om der er tale om et EU-land eller en anden europæisk stat, der har ratificeret 1977-konventionen.

Begrebet »omfattet af« indebærer både, at den konkrete handling skal kunne henføres til en af de nævnte konventionsbestemmelser, samt at den stat, der anmoder om udlevering, skal have ratificeret den pågældende konvention.

Om en overtrædelse er omfattet af artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af finansiering af terrorisme, afhænger af en konkret vurdering. Den berørte person kan efter omstændighederne kræve en beslutning om udlevering for en handling, som anses for omfattet af de nævnte bestemmelser, indbragt for domstolene, så udlevering først kan finde sted, når beslutningen er fundet lovlig ved endelig retskendelse, jf. udleveringslovens §§ 16 og 17.

Den nye bestemmelse indebærer, at udlevering ikke kan nægtes, når nægtelsen udelukkende begrundes med, at den forbrydelse, som udlevering angår, er en politisk forbrydelse mv. At den pågældende tilhører en frihedsbevægelse eller lignende, som man fra dansk side sympatiserer med, kan derfor som udgangspunkt ikke begrunde, at udlevering nægtes.

Udlevering kan dog efter omstændighederne fortsat nægtes med henvisning til andre bestemmelser i udleveringsloven, f.eks. § 6, hvorefter udlevering ikke må finde sted, hvis der er fare for, at den pågældende efter udleveringen på grund af sin afstamning, sit tilhørsforhold til en bestemt befolkningsgruppe, sin religiøse eller politiske opfattelse eller i øvrigt på grund af politiske forhold vil blive udsat for forfølgelse, som retter sig mod den berørte persons liv eller frihed eller i øvrigt er af alvorlig karakter.

Det vil også være muligt at afslå udlevering, hvis det i særlige tilfælde, navnlig under hensyn til den pågældendes alder, helbredstilstand eller andre personlige forhold må antages, at udlevering ville være uforenelig med humanitære hensyn, jf. udleveringslovens § 7.

Endelig kan udlevering fortsat kun ske på vilkår, at dødsstraf ikke fuldbyrdes for den pågældende handling, jf. § 10, nr. 3.

Til nr. 7 (udleveringslovens § 13 og § 19, stk. 1)

Ændringen indebærer en ajourføring af henvisningerne til retsplejelovens regler om beslaglæggelse og edition.

Den foreslåede tilføjelse af en henvisning til retsplejelovens regler om andre efterforskningsskridt (fotoforevisning, konfrontation og efterlysning) skal ses i lyset af, at disse efterforskningsskridt indtil lov nr. 229 af 21. april 1999 ikke var lovregulerede. Idet ikke mindst reglerne om efterlysning i retsplejelovens § 818 og § 819 vil kunne være relevante i forbindelse med en sag om udlevering, foreslås en generel henvisning til retsplejelovens kap. 75 a.

Til § 6

Den nordiske udleveringslov

Til nr. 1 (§ 11, 1. pkt., og § 16, stk. 1, 1. pkt.)

Den foreslåede tilføjelse af en henvisning til retsplejelovens regler om andre efterforskningsskridt (fotoforevisning, konfrontation og efterlysning) skal ses i lyset af, at disse efterforskningsskridt indtil lov nr. 229 af 21. april 1999 ikke var lovregulerede. Idet ikke mindst reglerne om efterlysning i retsplejelovens § 818 og § 819 vil kunne være relevante i forbindelse med en sag om udlevering, foreslås en generel henvisning til retsplejelovens kap. 75 a.

Til § 7

Det foreslås, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Det foreslås dog, at tidspunktet for ikrafttrædelsen af retsplejelovens § 786, stk. 4 og 6, (logningspligt for udbydere af telenet og teletrafik) fastsættes af justitsministeren.

Endvidere foreslås det, at § 5, nr. 1-6, om ændringer i udleveringsloven finder anvendelse i sager, hvor der fremsættes anmodning om udlevering efter lovens ikrafttræden, uanset om lovovertrædelsen er begået før lovens ikrafttræden.

Det foreslås dog, at § 5, stk. 3, nr. 3, i lov om udlevering af lovovertrædere, som affattet ved denne lovs § 5, nr. 6, først finder anvendelse på anmodninger om udlevering, der fremsættes efter, at FN-konventionen til bekæmpelse af finansiering af terrorisme er trådt i kraft mellem Danmark og vedkommende fremmede stat.

Til § 8

Ordningen med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold er en nyskabelse i forhold til den gældende retstilstand. Forslaget om, at den nærmere tekniske udmøntning skal ske administrativt, giver i vid udstrækning mulighed for løbende at tage højde for det praktiske behov for logning og den tekniske udvikling på området. Den foreslåede bestemmelse i retsplejelovens § 786, stk. 4, indebærer imidlertid, at der skal ske pligtmæssig registrering og opbevaring i 1 år af oplysningerne.

Justitsministeriet finder det på denne baggrund hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse. Bestemmelsen i lovforslagets § 8 indebærer, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse.

Til § 9

Bestemmelsen indebærer, at loven ikke gælder for Færøerne og Grønland.

Lovens § 1 (ændringer af straffeloven) kan dog sættes i kraft helt eller delvist for Færøerne ved kongelig anordning. For Grønland gælder der en særlig kriminallov, og der er derfor ikke foreslået en hjemmel til at sætte loven i kraft for Grønland.

Endvidere kan lovens § 5 (ændringer af udleveringsloven) sættes i kraft helt eller delvist for Færøerne og Grønland ved kongelig anordning.

2005/1 LSF 217 Justitsministeriet

Yderligere oplysninger ›

Fremsat den 31. marts 2006 af justitsministeren (Lene Espersen)

Forslag

til

Lov om ændring af straffeloven, retsplejeloven og forskellige andre love

(Styrkelse af indsatsen for at bekæmpe terrorisme mv.)

§ 1

I straffeloven, jf. lovbekendtgørelse nr. 909 af 27. september 2005, som ændret senest ved lov nr. 1400 af 21. december 2005, foretages følgende ændringer:

1. I *§ 110 d* indsættes efter »det halve«: », medmindre forholdet er omfattet af kapitel 13«.

2. *Overskriften* til *13. kapitel* affattes således:

»Forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv.«.

3. I *§ 114, stk. 1,* indsættes efter nr. 7:

»8) Besiddelse eller anvendelse mv. af radioaktive stoffer efter § 192 b.«

4. *§§ 114 a og 114 b* ophæves og i stedet indsættes:

» **§ 114 a.** Begås en af de i nr. 1-6 nævnte handlinger, uden at forholdet omfattes af § 114, kan straffen overstige den højeste for lovovertrædelsen foreskrevne straf med indtil det halve; hvis den højeste straf, der er foreskrevet for den pågældende handling, er mindre end 4 års fængsel, kan straffen dog stige til fængsel indtil 6 år.

1) Overtrædelse af §§ 180, 181, stk. 1, 183, stk. 1 eller 2, 183 a, 184, stk. 1, 192 a, 193, stk. 1, 237, 244, 245, 246, 250, 252, stk. 1, 266, 288 eller 291, stk. 1 eller 2, når handlingen er omfattet af artikel 1 i konventionen af 16. december 1970 om bekæmpelse af ulovlig bemægtigelse af luftfartøjer, artikel 1 i konventionen af 23. september 1971 til bekæmpelse af ulovlige handlinger mod den civile luftfarts sikkerhed eller artikel II i protokollen af 24. februar 1988 til bekæmpelse af ulovlige voldshandlinger i lufthavne, der betjener den internationale civile luftfart.

2) Overtrædelse af §§ 180, 181, stk. 1, 183, stk. 1 eller 2, 184, stk. 1, 237, 244, 245, 246, 250, 252, stk. 1, 260, 261, stk. 1 eller 2, 266 eller 291, stk. 1 eller 2, når handlingen er omfattet af artikel 2 i konventionen af 14. december 1973 om forebyggelse af og straf for forbrydelser mod internationalt beskyttede personer, herunder diplomatiske repræsentanter.

3) Overtrædelse af § 261, stk. 1 eller 2, når handlingen er omfattet af artikel 1 i den internationale konvention imod gidseltagning af 17. december 1979.

4) Overtrædelse af §§ 180, 181, stk. 1, 183, stk. 1 eller 2, 186, stk. 1, 192 a, 192 b, 237, 244, 245, 246, 260, 266, 276, 278, 279, 279 a, 281, 288 eller 291, stk. 2, når handlingen er omfattet af artikel 7 i IAEA-konventionen (Det Internationale Atomenergiagenturs konvention) af 26. oktober 1979 om fysisk beskyttelse af nukleare materialer.

5) Overtrædelse af §§ 180, 181, stk. 1, 183, stk. 1 eller 2, 183 a, 184, stk. 1, 192 a, 193, stk. 1, 237, 244, 245, 246, 252, stk. 1, 260, 266, 288 eller 291, stk. 1 eller 2, når handlingen er omfattet af artikel 3 i konventionen af 10. marts 1988 til bekæmpelse af ulovlige handlinger mod søfartssikkerheden eller artikel 2 i protokollen af 10. marts 1988 til bekæmpelse af ulovlige handlinger mod sikkerheden for fastgjorte platforme, der befinder sig på kontinentalsokkelen.

6) Overtrædelse af §§ 180, 181, stk. 1, 183, stk. 1 eller 2, 183 a, 184, stk. 1, 186, stk. 1, 192 a, 193, stk. 1, 237, 244, 245, 246, 250, 252, stk. 1, 266 eller 291, stk. 2, når handlingen er omfattet af artikel 2 i den internationale konvention af 15. december 1997 til bekæmpelse af terrorbombninger.

§ 114 b. Med fængsel indtil 10 år straffes den, som

1) direkte eller indirekte yder økonomisk støtte til,

2) direkte eller indirekte tilvejebringer eller indsamler midler til eller

3) direkte eller indirekte stiller penge, andre formuegoder eller finansielle eller andre lignende ydelser til rådighed for

en person, en gruppe eller en sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af § 114 eller § 114 a.

§ 114 c. Med fængsel indtil 10 år straffes den, som hverver en person til at begå eller fremme handlinger omfattet af § 114 eller § 114 a eller til at slutte sig til en gruppe eller sammenslutning for at fremme, at gruppen eller sammenslutningen begår handlinger af denne karakter. Under særligt skærpende omstændigheder kan straffen stige til fængsel indtil 16 år. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor der er tale om overtrædelser af systematisk eller organiseret karakter.

Stk. 2. Med fængsel indtil 6 år straffes den, som hverver en person til at begå eller fremme handlinger omfattet af § 114 b eller til at slutte sig til en gruppe eller sammenslutning for at fremme, at gruppen eller sammenslutningen begår handlinger af denne karakter.

Stk. 3. Med fængsel indtil 6 år straffes den, som lader sig hverve til at begå handlinger omfattet af § 114 eller § 114 a.

§ 114 d. Med fængsel indtil 10 år straffes den, som træner, instruerer eller på anden måde oplærer en person til at begå eller fremme handlinger omfattet af § 114 eller § 114 a med viden om, at personen har til hensigt at anvende færdighederne til dette formål. Under særligt skærpende omstændigheder kan straffen stige til fængsel indtil 16 år. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor der er tale om overtrædelser af systematisk eller organiseret karakter.

Stk. 2. Med fængsel indtil 6 år straffes den, som træner, instruerer eller på anden måde oplærer en person til at begå eller fremme handlinger omfattet af § 114 b med viden om, at personen har til hensigt at anvende de tillærte færdigheder til dette formål.

Stk. 3. Med fængsel indtil 6 år straffes den, som lader sig træne, instruere eller på anden måde oplære til at begå handlinger omfattet af § 114 eller § 114 a.

§ 114 e. Med fængsel indtil 6 år straffes den, som i øvrigt fremmer virksomheden for en person, en gruppe eller en sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af §§ 114, 114 a, 114 b, 114 c eller 114 d.«

§§ 114 c-114 e bliver herefter §§ 114 f-114 h.

5. I *§ 114 c,* der bliver *§ 114 f,* ændres »§§ 114-114 b« til: »§§ 114-114 e«, og i *§ 114 d* , der bliver *§ 114 g* , ændres »§§ 114-114 c« til: »§§ 114-114 f«.

6. *§ 183 a* affattes således:

» **§ 183 a.** Den, som ved ulovlig tvang, jf. § 260, tager kontrollen over et luftfartøj, et skib eller et andet kollektivt transportmiddel eller godstransportmiddel eller griber ind i dets manøvrering, straffes med fængsel indtil på livstid.

Stk. 2. På samme måde straffes den, som ved ulovlig tvang, jf. § 260, tager kontrollen over et offshoreanlæg.«

7. Efter *§ 192 a* indsættes:

» **§ 192 b.** Den, der med forsæt til skade på andres person eller til betydelig skade på andres ting eller på miljøet modtager, besidder, overdrager eller ændrer radioaktive stoffer eller fremstiller eller besidder en eksplosiv nuklear anordning eller en anordning, der er beregnet til at sprede radioaktive stoffer eller kan udsende ioniserende stråling, straffes med fængsel indtil 6 år.

Stk. 2. Med fængsel indtil 12 år straffes den, der med forsæt til skade på andres person eller til betydelig skade på andres ting eller på miljøet eller til at tvinge nogen til at foretage eller undlade at foretage en handling

1) anvender radioaktive stoffer eller anordninger, der udsender ioniserende stråling,

2) fjerner, ændrer eller beskadiger en nødvendig beskyttelse mod spredning af radioaktive stoffer eller mod ioniserende stråling eller

3) anvender eller beskadiger et nukleart anlæg med den følge, at der sker udslip af radioaktive stoffer eller fremkaldes fare derfor.

Stk. 3. Foretages en af de i stk. 2 nævnte handlinger under de i § 180 angivne omstændigheder eller med den følge, at der sker omfattende skade på miljøet eller fremkaldes nærliggende fare derfor, er straffen fængsel indtil på livstid.

Stk. 4. Begås forbrydelsen uagtsomt, er straffen bøde eller fængsel indtil 2 år.«

§ 2

I retsplejeloven, jf. lovbekendtgørelse nr. 910 af 27. september 2005, som ændret senest ved lov nr. 1399 af 21. december 2005, foretages følgende ændringer:

1. Efter *§ 110* indsættes:

» **§ 110 a.** Politiets Efterretningstjeneste kan videregive oplysninger til Forsvarets Efterretningstjeneste i det omfang, videregivelsen kan have betydning for varetagelse af tjenesternes opgaver.

Stk. 2. Politiets Efterretningstjeneste kan indhente oplysninger fra andre forvaltningsmyndigheder i det omfang, oplysningerne må antages at have betydning for varetagelse af tjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.«

2. *Overskriften* til *kapitel 71* affattes således:

»Indgreb i meddelelseshemmeligheden, observation, dataaflæsning og forstyrrelse eller afbrydelse af radio- eller telekommunikation«.

3. I *§ 783, stk. 1,* indsættes efter »angår«: », jf. dog stk. 2«.

4. I *§ 783* indsættes efter *stk. 1* som nyt stykke:

» *Stk. 2* . Angår efterforskningen en overtrædelse af straffelovens kapitel 12 eller 13, kan der i rettens kendelse i medfør af § 780, stk. 1, nr. 1 eller 3, i stedet for bestemte telefonnumre anføres den person, som indgrebet angår (den mistænkte). I så fald skal politiet snarest muligt efter udløbet af det tidsrum, inden for hvilket indgrebet kan foretages, underrette retten om de telefonnumre, som indgrebet har været rettet imod, samt om de bestemte grunde, der er til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte. Retten underretter den beskikkede advokat, jf. § 784, stk. 1, der herefter kan indbringe spørgsmålet om lovligheden af indgrebet for retten. Retten træffer afgørelse ved kendelse. Burde indgrebet efter rettens opfattelse ikke være foretaget, skal retten give meddelelse herom til Justitsministeriet.«

Stk. 2-4 bliver herefter stk. 3-5.

5. I *§ 788, stk. 4,* indsættes efter »eller taler«: »hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller«.

6. I *§ 791 a* indsættes efter stk. 4 som nye stykker:

» *Stk. 5* . Politiet kan fra udbydere af telenet eller teletjenester indhente oplysninger vedrørende lokaliseringen af en mobiltelefon, der antages at benyttes af en mistænkt (teleobservation), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.

Stk. 6. Det påhviler udbydere af telenet eller teletjenester at bistå politiet ved gennemførelse af teleobservation, herunder ved at give de i stk. 5 nævnte oplysninger.«

Stk. 5-6 bliver herefter stk. 7-8.

7. I *§ 791 a, stk. 6,* der bliver *stk. 8* , indsættes som 2. pkt.:

»Reglerne i §§ 783-785, § 788, stk. 1, § 788, stk. 2, nr. 1, § 788, stk. 3 og 4, samt § 791 finder tilsvarende anvendelse på de i stk. 5 omhandlede tilfælde.«

8. I *§ 791 b, stk. 3,* ændres »samt stk. 2 og 3« til: »samt stk. 3 og 4«.

9. Efter *§ 791 b* indsættes:

» **§ 791 c.** Politiet kan forstyrre eller afbryde radio- eller telekommunikation i et område, hvis der er afgørende grunde til det med henblik på at forebygge, at der i det pågældende område vil blive begået en lovovertrædelse, der efter loven kan straffes med fængsel i 6 år eller derover, eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, og som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.

Stk. 2. Indgreb som nævnt i stk. 1 må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages af forvolde den eller de personer, som indgrebet rammer, ville være et uforholdsmæssigt indgreb.

Stk. 3. Indgreb efter stk. 1 sker efter rettens kendelse. I kendelsen anføres det område, som indgrebet angår, og de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres. Endvidere fastsættes det tidsrum, inden for hvilket indgrebet kan foretages. Tidsrummet kan forlænges. Forlængelsen sker ved kendelse.

Stk. 4. Såfremt indgrebets øjemed ville forspildes, dersom retskendelse skulle afventes, kan politiet træffe beslutning om at foretage indgrebet. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes, samt om det kan opretholdes, og i bekræftende fald for hvilket tidsrum, jf. stk. 3, 2. og 4.-6. pkt. Burde indgrebet efter rettens opfattelse ikke have været foretaget, skal retten give meddelelse herom til Justitsministeriet.

Stk. 5. I øvrigt finder reglerne i §§ 784 og 785 tilsvarende anvendelse.«

§ 3

I lov om forbud mod tv-overvågning m.v., jf. lovbekendtgørelse nr. 788 af 12. august 2005, foretages følgende ændringer:

1. Efter *§ 4* indsættes:

» **§ 4 a.** Politimesteren (Politidirektøren) kan henstille, at offentlige myndigheder eller private foretager tv-overvågning i overensstemmelse med gældende lovgivning.

§ 4 b. Politimesteren (Politidirektøren) kan meddele offentlige myndigheder eller private, som foretager eller planlægger at iværksætte tv-overvågning efter gældende lovgivning, pålæg med hensyn til kvaliteten af optagelser af billeder på videobånd, film eller lignende samt med hensyn til opbevaringen af sådanne optagelser.«

2. I *§ 5* indsættes efter stk. 1 som nyt stykke:

» *Stk. 2* . Overtrædelse af pålæg meddelt i medfør af § 4 b straffes med bøde.«

Stk. 2–4 bliver herefter stk. 3-5.

§ 4

I lov om luftfart, jf. lovbekendtgørelse nr. 1484 af 19. december 2005, foretages følgende ændringer:

1. Efter *§ 148* indsættes:

»Kapitel 12 a.

Passageroplysninger

§ 148 a. Luftfartsselskaber skal foretage registrering og opbevaring i 1 år af oplysninger om passagerer og besætningsmedlemmer på luftfartøjer, der ankommer til eller afgår fra Danmark.

Stk. 2. Luftfartsselskaber skal på begæring af Politiets Efterretningstjeneste udlevere de i stk. 1 nævnte oplysninger til brug for forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.

Stk. 3. Transport- og energiministeren fastsætter efter forhandling med justitsministeren nærmere regler om registrering og opbevaring i medfør af stk. 1 og om luftfartsselskabernes praktiske bistand til Politiets Efterretningstjeneste i medfør af stk. 2.

Stk. 4. Transport- og energiministeren kan efter forhandling med justitsministeren fastsætte nærmere regler om Politiets Efterretningstjenestes adgang til luftfartsselskabernes bookingsystemer til brug for forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.«.

2. I *§ 149, stk. 5,* ændres »og § 72« til: »§ 72 og § 148 a, stk. 1 og 2«.

§ 5

I udleveringsloven, jf. lovbekendtgørelse nr. 833 af 25. august 2005, foretages følgende ændringer:

1. *§ 5, stk. 3, nr. 2 og 3* , ophæves og i stedet indsættes:

»2) artikel 6 og 7 og artikel 9, jf. artikel 6 og 7, i Europarådets konvention om forebyggelse af terrorisme,

3) artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af terrorbombninger,

4) artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af finansiering af terrorisme eller

5) artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af nuklear terrorisme.«

2. Efter *§ 5, stk. 3 ,* indsættes:

» *Stk. 4* . I særlige tilfælde kan udlevering for en handling omfattet af artikel 5 eller artikel 9, jf. artikel 5, i Europarådets konvention om forebyggelse af terrorisme nægtes, hvis det vurderes, at der er tale om en politisk lovovertrædelse.«

§ 6

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) foretages følgende ændring:

1. I *§ 8* ændres »2005-06« til: »2009-10«.

§ 7

Stk. 1. Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende, jf. dog stk. 2-4. § 5 finder anvendelse på anmodninger om udlevering efter Europarådets konvention om forebyggelse af terrorisme, henholdsvis FN-konventionen til bekæmpelse af nuklear terrorisme, der fremsættes efter, at den pågældende konvention er trådt i kraft mellem Danmark og vedkommende fremmede stat.

Stk. 2. Justitsministeren fastsætter efter forhandling med ministeren for videnskab, teknologi og udvikling tidspunktet for ikrafttrædelsen af retsplejelovens § 791 a, stk. 6, som affattet ved denne lovs § 2, nr. 6.

Stk. 3. Retsplejelovens § 791 c, som affattet ved denne lovs § 2, nr. 9, træder i kraft den 1. juli 2006.

Stk. 4. Transport- og energiministeren fastsætter efter forhandling med justitsministeren tidspunktet for ikrafttrædelsen af luftfartslovens § 148 a, som affattet ved denne lovs § 4, nr. 1.

§ 8

Loven gælder ikke for Færøerne og Grønland. Lovens § 1 kan dog ved kongelig anordning sættes i kraft for Færøerne med de afvigelser, som de særlige færøske forhold tilsiger. Lovens §§ 3-5 kan ved kongelig anordning sættes i kraft for Færøerne og Grønland med de afvigelser, som de særlige færøske og grønlandske forhold tilsiger.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

1.1. Oversigt

Lovforslaget har to overordnede formål:

Det ene formål er at gennemføre de dele af regeringens handlingsplan for terrorbekæmpelse, der vedrører lovændringer på Justitsministeriets område, jf. nærmere pkt. 1.3. nedenfor.

Det andet formål er at gennemføre forslagene i Straffelovrådets betænkning nr. 1474/2006 om det strafferetlige værn mod terrorisme, jf. nærmere pkt. 1.4. nedenfor.

En samlet oversigt over de enkelte dele af lovforslaget findes under pkt. 1.5. nedenfor. Som det fremgår heraf, indgår der i lovforslaget også en ændring af udleveringsloven som følge af konventionsmæssige forpligtelser samt en udskydelse af tidspunktet for revision af den såkaldte logningsbestemmelse i retsplejelovens § 786, stk. 4, der blev indført ved anti-terrorpakken i 2002.

1.2. Indsatsen mod terrorisme

Siden terrorangrebene i USA den 11. september 2001 har der bestået et generelt forhøjet trusselniveau i den vestlige verden og i forhold til vestlige interesser. Terrorhandlingerne i Madrid i 2004 og i London i 2005 har vist, at også de europæiske lande er sårbare over for den internationale terrorisme.

For Danmarks vedkommende er terrorismen en trussel mod samfundet og de værdier, som det bygger på, og mod den enkelte borger.

Efter regeringens opfattelse er det derfor afgørende, at myndighederne har de nødvendige redskaber med henblik på forebyggelse, afværgelse og efterforskning af terrorisme. For politiets vedkommende lægger regeringen således vægt på, at der er de relevante muligheder for f.eks. indhentelse af efterretningsmæssige oplysninger og for efterforskning og strafforfølgning i konkrete sager. Samtidig er regeringen meget opmærksom på vigtigheden af, at der i forbindelse med nye initiativer på terrorområdet sikres den rigtige balance mellem sikkerhed og retssikkerhed, således at indsatsen for at beskytte samfundet som sådan ikke kommer til at ske på bekostning af hensynet til den enkeltes frihed.

Der har siden den 11. september 2001 været iværksat en lang række initiativer bl.a. med henblik på at tage højde for terrorismens globale karakter og styrke politiets efterforskningsmuligheder. Som led i opfølgningen på terrorangrebene i USA vedtog et bredt flertal i Folketinget således f.eks. i maj 2002 den såkaldte anti-terrorpakke.

Der er endvidere bl.a. bevilget ressourcer med henblik på styrkelse af efterretningstjenesterne og med henblik på at skabe en effektiv og forebyggende beredskabsmæssig indsats, ligesom regeringen i maj 2005 har truffet beslutning om en række tiltag som opfølgning på den såkaldte sårbarhedsudredning.

I lyset af terrorangrebet i London i juli 2005 fandt regeringen imidlertid anledning til at foretage en samlet gennemgang og vurdering af det danske samfunds indsats og beredskab over for terrorhandlinger. Regeringen nedsatte derfor en tværministeriel arbejdsgruppe om terrorbekæmpelse, der fik til opgave at overveje behovet for yderligere initiativer.

1.3. Den tværministerielle arbejdsgruppes rapport og regeringens handlingsplan for terrorbekæmpelse

Den tværministerielle arbejdsgruppe offentliggjorde den 3. november 2005 rapporten »Det danske samfunds indsats og beredskab mod terror«. Rapporten indeholder 49 anbefalinger, som efter arbejdsgruppens opfattelse kan komme på tale for at styrke indsatsen og beredskabet mod terror. Der er tale om en bred vifte af forslag, der berører flere ministerområder.

På baggrund af arbejdsgruppens anbefalinger fremlagde regeringen den 16. november 2005 en handlingsplan for terrorbekæmpelse, som indeholder en række initiativer med henblik på at styrke det danske samfunds indsats og beredskab mod terror. I handlingsplanen er angivet, hvordan regeringen vil arbejde videre med hver enkelt af arbejdsgruppens anbefalinger.

En række af anbefalingerne vil kunne gennemføres administrativt, mens andre kræver ny lovgivning. Det fremgår derfor af handlingsplanen, at regeringen i foråret 2006 vil fremlægge en række lovforslag som led i en anti-terrorlovpakke. Endelig er der enkelte af arbejdsgruppens forslag, som kræver yderligere overvejelser og udredningsarbejde, før regeringen tager endelig stilling.

Det foreliggende lovforslag er et led i regeringens samlede anti-terrorlovpakke, som herudover bl.a. omfatter de samtidigt fremsatte forslag fra forsvarsministeren og ministeren for videnskab, teknologi og udvikling.

I regeringens handlingsplan for terrorbekæmpelse er det i relation til bl.a. de anbefalinger fra den tværministerielle arbejdsgruppe, som udmøntes i det foreliggende lovforslag, anført, at regeringen vil arbejde videre med at konkretisere de enkelte anbefalinger. I overensstemmelse hermed har det i forbindelse med udarbejdelsen af lovforslaget på enkelte punkter vist sig nødvendigt eller hensigtsmæssigt at justere de foreslåede bestemmelser i forhold til de pågældende anbefalinger. Der henvises nærmere til omtalen af de enkelte forslag under pkt. 3-8 nedenfor, hvor der også er redegjort for, i hvilket omfang de foreslåede bestemmelser alene kan finde anvendelse på terrorområdet, eller om de også kan finde anvendelse i forhold til anden kriminalitet.

1.4. Europarådets konvention om forebyggelse af terrorisme og FN's konvention om nuklear terrorisme

Siden gennemførelsen af anti-terrorpakken i 2002 er der vedtaget to nye internationale konventioner på terrorbekæmpelsesområdet. Det drejer sig om dels Europarådets konvention om forebyggelse af terrorisme, som blev vedtaget af Europarådets Ministerkomité den 3. maj 2005, dels FN's konvention om nuklear terrorisme, der blev vedtaget af FN's Generalforsamling den 13. april 2005. Danmark har i maj 2005 undertegnet Europarådskonventionen. Regeringen har endvidere undertegnet FN-konventionen med sædvanligt ratifikationsforbehold på Danmarks vegne i forbindelse med FN-topmødet i New York i september 2005.

Europarådskonventionen om forebyggelse af terrorisme indebærer en forpligtelse for de kontraherende stater til at kriminalisere visse forberedende handlinger til terrorhandlinger. Det drejer sig om opfordring til terrorhandlinger, rekruttering til terrorhandlinger og oplæring i at begå terrorhandlinger. Konventionen er optaget som *bilag 1* til lovforslaget sammen med en uofficiel oversættelse heraf.

FN-konventionen om nuklear terrorisme indeholder en forpligtelse for de kontraherende stater til at kriminalisere en række handlinger vedrørende ulovlig besiddelse og brug mv. af radioaktivt materiale med forsæt til at forårsage død eller alvorlig personskade eller til at forårsage betydelig tings- eller miljøskade. Konventionen er optaget som *bilag 2* til lovforslaget sammen med en uofficiel oversættelse heraf.

Den 19. august 2005 anmodede Justitsministeriet Straffelovrådet om nærmere at overveje, hvilke lovgivningsmæssige ændringer en dansk ratifikation og gennemførelse af Europarådets konvention om forebyggelse af terrorisme og FN's konvention om nuklear terrorisme vil nødvendiggøre på det strafferetlige område. Justitsministeriet anmodede samtidig Straffelovrådet om i lyset af den senere tids udvikling og erfaringer på terrorområdet mere generelt at overveje, om straffelovens anti-terrorbestemmelser (§§ 114-114 e) i sammenhæng med den øvrige strafferetlige lovgivning fortsat giver et tilstrækkeligt strafferetligt værn mod terrorisme.

Straffelovrådet har den 1. marts 2006 afgivet betænkning nr. 1474/2006 om det strafferetlige værn mod terrorisme. Lovforslaget bygger på Straffelovrådets betænkning.

Formålet med lovforslaget er at gennemføre de ændringer, der er nødvendige for, at Danmark kan ratificere og gennemføre Europarådets konvention om forebyggelse af terrorisme og FN's konvention om nuklear terrorisme. Folketingets vedtagelse af forslaget vil indebære samtykke efter grundlovens § 19 til ratifikation af Europarådets konvention og FN-konventionen.

1.5. Lovforslagets nærmere indhold

1.5.1. Formålet med lovforslaget er som anført ovenfor for det første at gennemføre de ændringer, der er nødvendige for, at Danmark kan ratificere og gennemføre Europarådets konvention om forebyggelse af terrorisme og FN's konvention om nuklear terrorisme. Denne del af lovforslaget bygger som nævnt på Straffelovrådets betænkning nr. 1474/2006 om det strafferetlige værn mod terrorisme.

Lovforslaget indeholder forslag til bestemmelser i straffelovens §§ 114 a-e med henblik på at opfylde kriminaliseringspligten i artiklerne 6 (rekruttering til terrorisme) og 7 (oplæring til terrorisme) sammenholdt med artikel 9 i Europarådets konvention.

Lovforslaget indeholder således forslag til to nye bestemmelser i straffelovens § 114 c og § 114 d om henholdsvis hvervning og oplæring til at begå terrorhandlinger. I forlængelse heraf foreslås bestemmelser, der kriminaliserer den, der lader sig hverve eller oplære til at begå terrorhandlinger (§ 114 c, stk. 3, og § 114 d, stk. 3).

Det foreslås endvidere at indsætte en ny bestemmelse i straffelovens § 114 a, der omfatter handlinger, som efter Europarådskonventionen skal anses som terrorhandlinger, og som ikke allerede er omfattet af terrorismebestemmelsen i straffelovens § 114. Formålet med bestemmelsen er at indføje en sidestrafferamme med mulighed for strafforhøjelse, når overtrædelse af nærmere angivne bestemmelser i straffeloven er begået under omstændigheder omfattet af de berørte artikler i en række nærmere opregnede internationale konventioner. Der er således ikke med den foreslåede bestemmelse tilsigtet nogen nykriminalisering.

Den gældende bestemmelse i straffelovens § 114 a om finansiering af terrorisme foreslås videreført som ny § 114 b således, at bestemmelsen fremover omfatter finansiering af terrorhandlinger og terrorlignende handlinger efter både bestemmelsen i straffelovens § 114 og den foreslåede nye bestemmelse i straffelovens § 114 a.

Der foreslås endvidere en tilpasning af den udvidede medvirkensregel i den gældende bestemmelse i straffelovens § 114 b (den foreslåede bestemmelse i § 114 e), således at denne bestemmelse kommer til at omfatte fremme af enkeltpersoners virksomhed og dermed bringes på linje med den gældende bestemmelse i straffelovens § 114 a (den foreslåede bestemmelse i § 114 b), og således at bestemmelsen udvides med fremme af handlinger af den beskaffenhed, der er omhandlet i de foreslåede bestemmelser i § 114 b, nr. 3, § 114 a og §§ 114 c og d.

Lovforslaget indeholder desuden en ændring af straffelovens § 183 a om kapring af transportmidler, der tilsigter at sidestille kapring af offshoreanlæg, f.eks. borerigge og beboelsesplatforme, med kapringer af bl.a. skibe.

Herudover foreslås det at indsætte en ny bestemmelse i straffelovens § 192 b, der retter sig mod besiddelse og anvendelse af radioaktive stoffer mv. med forsæt til skade på andres person eller til betydelig skade på andres ting eller på miljøet. Bestemmelsen vil f.eks. omfatte placering af radioaktive kilder på en sådan måde, at personer udsættes for skadelig bestråling.

Der henvises nærmere til pkt. 2 nedenfor.

Med henblik på at gennemføre de ændringer i udleveringsloven, som en ratifikation af Europarådets konvention om forebyggelse af terrorisme og FN's konvention om nuklear terrorisme vil kræve, foreslås det endvidere, at undtagelsesbestemmelsen i udleveringslovens § 5, stk. 3, udvides til også at omfatte handlinger, som er omfattet af artikel 6 (rekruttering til terrorisme) og 7 (oplæring til terrorisme) og artikel 9 i Europarådets konvention samt artikel 2, jf. artikel 1, i FN-konventionen. Dette indebærer, at forbudet mod udlevering for politiske lovovertrædelser mv. ikke finder anvendelse for handlinger omfattet heraf.

Det foreslås endvidere at indsætte en ny bestemmelse i udleveringslovens § 5, stk. 4, der tilsigter at tydeliggøre, at der i medfør af Europarådets konvention ikke består en ubetinget pligt til udlevering for en politisk forbrydelse, når handlingen er omfattet af konventionens artikel 5 (offentlige opfordringer til terrorisme) eller artikel 9, jf. artikel 5, sådan som det er tilfældet, hvis handlingen er omfattet af konventionens artikel 6 eller 7 eller artikel 9.

Der henvises til pkt. 9 nedenfor.

1.5.2. Formålet med lovforslaget er som anført ovenfor – som led i regeringens samlede anti-terrorlovpakke – for det andet at gennemføre dele af regeringens handlingsplan for terrorbekæmpelse. Lovforslaget indeholder i den forbindelse en række initiativer, der skal forbedre politiets muligheder for at forebygge, efterforske og bekæmpe terrorhandlinger.

Lovforslaget indeholder forslag til en ny bestemmelse i retsplejeloven, der har til formål at skabe grundlag for, at Politiets Efterretningstjeneste kan videregive oplysninger til Forsvarets Efterretningstjeneste, uden at der i hvert enkelt tilfælde skal foretages en nærmere konkret vurdering og interesseafvejning i forhold til den enkelte oplysning. Efter den foreslåede bestemmelse i retsplejelovens § 110 a, stk. 1, kan Politiets Efterretningstjeneste således videregive oplysninger til Forsvarets Efterretningstjeneste i det omfang, videregivelsen kan have betydning for varetagelse af tjenesternes opgaver. Den foreslåede bestemmelse skal ses i sammenhæng med en bestemmelse, der i det lovforslag, som forsvarsministeren samtidig har fremsat, foreslås indsat i forsvarsloven om videregivelse af oplysninger fra Forsvarets Efterretningstjeneste til Politiets Efterretningstjeneste.

Der foreslås endvidere etableret et særligt lovgrundlag for Politiets Efterretningstjenestes indhentelse af oplysninger fra andre forvaltningsmyndigheder. Efter den foreslåede bestemmelse i retsplejelovens § 110 a, stk. 2, kan Politiets Efterretningstjeneste således indhente oplysninger fra andre forvaltningsmyndigheder i det omfang, oplysningerne må antages at have betydning for varetagelse af efterretningstjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13. Bestemmelsen vil for de pågældende forvaltningsmyndigheder udgøre en særlig hjemmel til videregivelse af de omhandlede oplysninger samt til den behandling af oplysninger, som i den forbindelse er nødvendig.

Der henvises nærmere til pkt. 3 nedenfor.

Dernæst indeholder lovforslaget nogle ændringer i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, observation og dataaflæsning. Disse ændringer har navnlig til formål at sikre, at politiets efterforskningsmidler mv. er i overensstemmelse med den teknologiske udvikling og udviklingen i terrortruslen mod Danmark.

Der stilles således bl.a. forslag om at forenkle proceduren for indhentelse af retskendelser vedrørende telefonaflytning og teleoplysning. Den gældende bestemmelse i retsplejelovens § 783, stk. 1, 2. pkt., hvorefter der i en kendelse om aflytning mv. skal anføres de telefonnumre, som indgrebet angår, foreslås – for så vidt angår sager om overtrædelse af straffelovens kapitel 12 og 13 – tilpasset den teknologiske udvikling, således at der i kendelsen i stedet for telefonnumre kan anføres den person, som indgrebet angår (den mistænkte). En sådan kendelse vil indebære, at politiet kan iværksætte aflytning af den mistænkte og indhente teleoplysninger, uanset hvilke kommunikationsmidler den pågældende måtte vælge at benytte sig af.

De almindelige betingelser for, hvornår indgreb i form af telefonaflytning og teleoplysning kan foretages, videreføres uændret, og der er således ikke tale om, at politiet vil kunne foretage telefonaflytning mv. i videre omfang end i dag. Ordningen foreslås endvidere etableret således, at retten efterfølgende – på begæring af den beskikkede advokat – kan kontrollere, at politiets aflytning af konkrete telefonnumre mv. er sket inden for rammerne af den foreliggende retskendelse og retsplejelovens almindelige betingelser.

Der henvises nærmere til pkt. 4 nedenfor.

Herudover foreslås det at ændre retsplejelovens § 788, stk. 4, om underretning om indgreb i meddelelseshemmeligheden, således at det kommer til at fremgå udtrykkeligt, at retten – hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder taler for det – efter begæring fra politiet kan beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum.

Der henvises nærmere til pkt. 4 nedenfor.

Lovforslaget indeholder desuden en ændring af retsplejelovens § 791 a, der indebærer, at spørgsmålet om såkaldt teleobservation – det vil sige indhentelse af oplysninger fra udbydere af telenet og teletjenester om, hvilke mobiltelefonmaster en mistænkts mobiltelefon er i kontakt med – udtrykkeligt reguleres i retsplejeloven. Det foreslås således, at der i retsplejelovens § 791 a, stk. 5-6, indsættes bestemmelser om denne form for indgreb, herunder om de betingelser, der skal være opfyldt, og om krav om retskendelse.

Der henvises nærmere til pkt. 5 nedenfor.

Med henblik på at forebygge konkret forestående terrorhandlinger eller anden alvorlig kriminalitet foreslås der indsat en udtrykkelig bestemmelse i retsplejelovens § 791 c om forstyrrelse eller afbrydelse af radio- eller telekommunikation i helt særlige tilfælde. Efter bestemmelsen kan politiet – på grundlag af retskendelse – forstyrre eller afbryde radio- eller telekommunikation i et område, hvis der er afgørende grunde til det med henblik på at forebygge, at der vil blive begået en lovovertrædelse, der efter loven kan straffes med fængsel i 6 år eller derover, eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13.

Det er herudover en betingelse, at den pågældende lovovertrædelse kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Bestemmelsen tager f.eks. sigte på tilfælde, hvor der måtte foreligge konkrete oplysninger om et forestående terrorangreb med bomber, der planlægges udløst via mobiltelefoner eller andet radioudstyr.

Der henvises nærmere til pkt. 6 nedenfor.

Lovforslaget indeholder endvidere enkelte ændringer af lov om forbud mod tv-overvågning m.v.

Politiet har ikke i dag udtrykkelig hjemmel til at henstille til offentlige myndigheder eller private, at deres muligheder for at foretage tv-overvågning udnyttes. Det foreslås at indsætte en bestemmelse i tv-overvågningslovens § 4 a, hvorefter politiet kan henstille, at offentlige myndigheder eller private foretager tv-overvågning i overensstemmelse med gældende lovgivning. Henstilling om at iværksætte tv-overvågning forudsættes navnlig anvendt, hvor tv-overvågning vurderes at kunne have betydning for forebyggelse eller efterforskning af eventuelle terrorangreb.

Der vil ikke med hjemmel i den foreslåede bestemmelse kunne iværksættes tv-overvågning i videre omfang end i dag.

Endvidere foreslås der indsat en bestemmelse i tv-overvågningslovens § 4 b, der giver politiet mulighed for at meddele offentlige myndigheder eller private, som efter gældende lovgivning foretager eller planlægger at iværksætte tv-overvågning, pålæg med hensyn til kvaliteten af optagelser af billeder på videobånd, film eller lignende samt med hensyn til opbevaringen af sådanne optagelser. Dette skal bl.a. ses i lyset af, at anvendelse af tv-overvågningsoptagelser i efterforskningen af straffesager forudsætter, at optagelserne er af tilstrækkelig god kvalitet. Den foreslåede bestemmelse giver ikke adgang til at pålægge en myndighed eller en privat at iværksætte tv-overvågning, og der vil heller ikke med hjemmel i denne bestemmelse kunne foretages tv-overvågning i videre omfang end i dag.

Der henvises nærmere til pkt. 7 nedenfor.

Endelig foreslås der en ændring af luftfartsloven, således at der sikres Politiets Efterretningstjeneste en hurtigere og mere effektiv adgang til standardmæssige passageroplysninger, det vil sige oplysninger om passagerer og besætningsmedlemmer på luftfartøjer, der ankommer til eller afgår fra Danmark. Der foreslås således indsat en bestemmelse i luftfartslovens § 148 a, hvorefter luftfartsselskaber på begæring af Politiets Efterretningstjeneste uden retskendelse skal udlevere nærmere angivne passageroplysninger til brug for forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13. Den foreslåede ordning bygger på de regler, der i dag gælder på udlændingeområdet.

Med henblik på at sikre, at passageroplysninger er tilgængelige i en vis periode, foreslås det endvidere, at luftfartsselskaber skal foretage registrering og opbevaring af passageroplysninger i 1 år. Det foreslås, at transport- og energiministeren efter forhandling med justitsministeren fastsætter nærmere regler om registrering og opbevaring af sådanne oplysninger og om luftfartsselskabernes praktiske bistand til politiet, ligesom transport- og energiministeren efter forhandling med justitsministeren kan fastsætte nærmere regler om Politiets Efterretningstjenestes on-line adgang til luftfartsselskabernes bookingsystemer.

Der henvises nærmere til pkt. 8 nedenfor.

Lovforslaget har endelig til formål at fastsætte et nyt tidspunkt for revision af bestemmelsen i retsplejelovens § 786, stk. 4, hvorefter udbydere af telenet og teletjenester skal foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Lovforslaget indebærer således, at justitsministeren i folketingsåret 2009-10 fremsætter forslag om revision.

Der henvises til pkt. 10 nedenfor.

1.5.3. Justitsministeriet finder det hensigtsmæssigt, at der efter en passende periode gøres status over erfaringerne med de foreslåede nye regler. På den baggrund vil Justitsministeriet i folketingsåret 2009-10 – det vil sige tre år efter lovforslagets gennemførelse – give Folketingets Retsudvalg en orientering herom.

2. Det strafferetlige værn mod terrorisme

2.1. Gældende ret

Terrorangrebene den 11. september 2001 gav anledning til, at der blev foretaget en nærmere vurdering af, om dansk lovgivning var tilstrækkelig til at sikre en effektiv indsats mod terrorisme. Denne vurdering resulterede bl.a. i en række forskellige lovgivningsinitiativer rettet mod terrorisme. Det gælder bl.a. lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge eller Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) – den såkaldte anti-terrorpakke. Der henvises til Folketingstidende 2001-02, 2. samling, tillæg A, side 808 f, tillæg B, side 1605 f, og Folketingets forhandlinger, side 1321 f, 7439 f og 7747 f.

Formålet med loven er i første række at gennemføre tre internationale instrumenter i dansk ret: FN-konventionen af 9. december 1999 til bekæmpelse af finansiering af terrorisme (FN's terrorfinansieringskonvention), FN's Sikkerhedsråds resolution nr. 1373 (2001) af 28. september 2001 om bekæmpelse af terrorisme samt EU's rammeafgørelse om bekæmpelse af terrorisme, som der blev opnået politisk enighed om i EU i december 2001 (EU-rammeafgørelsen er efterfølgende endeligt vedtaget blandt EU-landene i juni 2002, jf. De Europæiske Fællesskabers Tidende L 164 af 22. juni 2002, side 3 ff).

Ved loven blev der bl.a. indsat en særlig terrorismebestemmelse i straffelovens § 114, der indeholder en definition af begrebet terrorisme. § 114 har følgende ordlyd:

» **§ 114.** For terrorisme straffes med fængsel indtil på livstid den, som med forsæt til at skræmme en befolkning i alvorlig grad eller uretmæssigt at tvinge danske eller udenlandske offentlige myndigheder eller en international organisation til at foretage eller undlade at foretage en handling eller at destabilisere eller ødelægge et lands eller en international organisations grundlæggende politiske, forfatningsmæssige, økonomiske eller samfundsmæssige strukturer begår en eller flere af følgende handlinger, når handlingen i kraft af sin karakter eller den sammenhæng, hvori den begås, kan tilføje et land eller en international organisation alvorlig skade:

1) Manddrab efter § 237.

2) Grov vold efter § 245 eller § 246.

3) Frihedsberøvelse efter § 261.

4) Forstyrrelse af trafiksikkerheden efter § 184, stk. 1, retsstridige forstyrrelser i driften af almindelige samfærdselsmidler m.v. efter § 193, stk. 1, eller groft hærværk efter § 291, stk. 2, hvis disse overtrædelser begås på en måde, der kan bringe menneskeliv i fare eller forårsage betydelige økonomiske tab.

5) Kapring af transportmidler efter § 183 a.

6) Grove våbenlovsovertrædelser efter § 192 a eller lov om våben og eksplosivstoffer § 10, stk. 2.

7) Brandstiftelse efter § 180, sprængning, spredning af skadevoldende luftarter, oversvømmelse, skibbrud, jernbane- eller anden transportulykke efter § 183, stk. 1 og 2, sundhedsfarlig forurening af vandforsyningen efter § 186, stk. 1, sundhedsfarlig forurening af ting bestemt til almindelig udbredelse m.v. efter § 187, stk. 1.

Stk. 2. På samme måde straffes den, som med det i stk. 1 nævnte forsæt transporterer våben eller eksplosivstoffer.

Stk. 3. Endvidere straffes på samme måde den, der med det i stk. 1 nævnte forsæt truer med at begå en af de i stk. 1 og 2 nævnte handlinger.«

Bestemmelsen skal navnlig gennemføre EU's rammeafgørelse om bekæmpelse af terrorisme, der i artikel 1 forpligter medlemslandene til særskilt at kriminalisere en række forsætlige handlinger som terrorhandlinger.

Bestemmelsen omfatter meget alvorlige forbrydelser, der begås for at forstyrre samfundsordenen og skræmme befolkningen.

§ 114 er – i modsætning til, hvad der er antaget om den hidtidige terrorismebestemmelse i § 114 – ikke begrænset til at beskytte danske samfundsforhold mv. Derimod beskytter bestemmelsen både danske og udenlandske myndigheder samt internationale organisationer, f.eks. FN. Denne ændring blev gennemført med henblik på bedre at kunne tage højde for terrorismens globale karakter.

Der vil kunne forekomme tilfælde, hvor Politiets Efterretningstjeneste efter den foreslåede bestemmelse i § 110 a, stk. 2, modtager oplysninger, som viser sig at være uden betydning for efterretningstjenestens virksomhed, men som kan være relevante for andre myndigheder, herunder andre dele af politiet. Det kan f.eks. dreje sig om oplysninger, som kan have betydning for efterforskning af anden kriminalitet end den, som efterretningstjenesten er ansvarlig for.

I sådanne situationer må Politiets Efterretningstjeneste tage stilling til, om tjenesten kan videregive disse oplysninger til de relevante myndigheder.

Dette spørgsmål er ikke reguleret af det foreliggende lovforslag.

Det indebærer, at spørgsmålet – på samme måde, som hvis tjenesten i øvrigt kommer i besiddelse af oplysninger, som kan være relevante for andre forvaltningsmyndigheder – må afgøres efter de almindelige regler om videregivelse af oplysninger i forvaltningslovens kapitel 8. Er der tale om oplysninger vedrørende enkeltpersoners rent private forhold, vil videregivelse til andre forvaltningsmyndigheder således kun kunne ske under de skærpede betingelser, der fremgår af forvaltningslovens § 28, stk. 2, jf. om denne bestemmelse pkt. 3.1.2. ovenfor.

3.4.3. Forholdet til databeskyttelsesdirektivet

Som det fremgår af pkt. 3.4.2.1., vil bestemmelsen i § 110 a, stk. 2, gøre det muligt for Politiets Efterretningstjeneste at indhente oplysninger fra andre forvaltningsmyndigheder, uden at der i hvert enkelt tilfælde skal foretages en nærmere konkret vurdering i forhold til de pågældende oplysninger.

Efter behandlingsreglerne i persondataloven vil spørgsmålet om videregivelse af oplysninger i vidt omfang bygge på en konkret vurdering af en række forskellige hensyn og de enkelte oplysninger. For så vidt angår det nærmere indhold af disse regler henvises til pkt. 3.1.3.

Bestemmelsen i § 110 a, stk. 2, indebærer en fravigelse af visse af persondatalovens regler for de myndigheder, der efter anmodning videregiver oplysninger til Politiets Efterretningstjeneste i medfør af den omhandlede bestemmelse, jf. nærmere herom pkt. 3.4.2.1.

Om forholdet til databeskyttelsesdirektivet (direktiv 95/46/EF af 24. oktober 1995) bemærkes, at det fremgår af direktivets artikel 13, stk. 1, at medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der bl.a. er fastsat i direktivets artikel 6 (svarende til persondatalovens § 5 vedrørende de grundlæggende principper for behandling af personoplysninger). Sådanne foranstaltninger kan træffes, hvis hensynet til bl.a. statens sikkerhed, den offentlige sikkerhed eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager nødvendiggør det.

Med hensyn til behandling af oplysninger, der er omfattet af databeskyttelsesdirektivets artikel 8 (følsomme oplysninger), fremgår det endvidere af artikel 8, stk. 4, at med forbehold af, at der gives tilstrækkelige garantier, kan medlemsstaterne af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser bl.a. ved lovgivning fastsætte andre undtagelser end dem, der er nævnt i artikel 8, stk. 2.

Den foreslåede bestemmelse i retsplejelovens § 110 a, stk. 2, er fastsat med henblik på at give Politiets Efterretningstjeneste de nødvendige redskaber med henblik på forebyggelse, afværgelse og efterforskning af terrorisme. Det er i overensstemmelse hermed en betingelse for, at Politiets Efterretningstjeneste i medfør af bestemmelsen i § 110 a, stk. 2, kan indhente oplysninger, at oplysningerne må antages at have betydning for varetagelse af tjenestens opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13. De pågældende oplysninger indhentes således af hensyn til opgaver af central sikkerhedsmæssig betydning.

Der kan endvidere henvises til, at bestemmelsen forudsætter, at Politiets Efterretningstjeneste ikke må skaffe sig oplysninger fra andre forvaltningsmyndigheder, medmindre der foreligger en mere konkret formodning for, at de pågældende oplysninger vil have betydning for varetagelsen af efterretningstjenestens opgaver vedrørende forebyggelse eller efterforskning af overtrædelser af straffelovens kapitel 12 og 13. Det forudsættes endvidere, at Politiets Efterretningstjeneste i overensstemmelse med de retningslinjer, der i dag gælder for tjenestens behandling af oplysninger af den nævnte karakter, inden for en rimelig tid træffer afgørelse om, hvorvidt de personer, som tjenesten har indsamlet oplysninger om, har relevans for tjenesten. Hvis dette viser sig ikke at være tilfældet, skal oplysningerne vedrørende de pågældende personer destrueres. Der henvises i øvrigt til pkt. 3.4.2.1. og 3.4.2.3.

Det bemærkes endeligt, at der ved udarbejdelse af nye retningslinjer for det såkaldte Wamberg-udvalg forudsættes etableret en ordning, hvorefter Wamberg-udvalget vil have mulighed for mere generelt at påse, at Politiets Efterretningstjenestes anvendelse af bestemmelsen i § 110 a, stk. 2, ligger inden for rammerne af bestemmelsen, jf. nærmere pkt. 3.4.2.3.

På den anførte baggrund ligger den foreslåede bestemmelse i § 110 a, stk. 2, efter Justitsministeriets opfattelse inden for rammerne af databeskyttelsesdirektivet.

4. Indgreb i meddelelseshemmeligheden

4.1. Gældende ret

4.1.1. Overordnet om retsplejelovens regler

Reglerne om indgreb i meddelelseshemmeligheden er fastsat i retsplejelovens kapitel 71, der blev indsat ved lov nr. 227 af 6. juni 1985 om ændring af retsplejeloven (Telefonaflytning mv.). Der henvises til Folketingstidende 1984-85, tillæg A, spalte 2955, tillæg B, spalte 1709 og 2225, samt Folketingets forhandlinger, spalte 5403, 5985, 10678 og 11229. Denne lovændring byggede på Strafferetsplejeudvalgets betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Det følger af retsplejelovens § 780, stk. 1, at politiet kan foretage indgreb i meddelelseshemmeligheden ved at

1) aflytte telefonsamtaler eller anden tilsvarende telekommunikation (*telefonaflytning*),

2) aflytte andre samtaler eller udtalelser ved hjælp af et apparat (*anden aflytning*),

3) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (*teleoplysning*),

4) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (*udvidet teleoplysning*),

5) tilbageholde, åbne og gøre sig bekendt med indholdet af breve, telegrammer og andre forsendelser (*brevåbning*), og

6) standse den videre befordring af forsendelser som nævnt i nr. 5 (*brevstandsning*).

Efter retsplejelovens § 780, stk. 2, kan politiet foretage optagelser eller tage kopier af de samtaler, udtalelser, forsendelser mv., som er nævnt i stk. 1, i samme omfang, som politiet er berettiget til at gøre sig bekendt med indholdet heraf.

De almindelige betingelser for, at politiet kan foretage indgreb i meddelelseshemmeligheden, er fastsat i retsplejelovens § 781, stk. 1. Det følger af denne bestemmelse, at der kun må foretages indgreb i meddelelseshemmeligheden, hvis

1) der er *bestemte grunde* til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt,

2) indgrebet må antages at være af afgørende betydning for efterforskningen (*indikationskrav*), og

3) efterforskningen angår en lovovertrædelse, der kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller kapitel 13 eller en overtrædelse af straffelovens §§ 124, stk. 2, 125, 127, stk. 1, 193, stk. 1, 228, 235, 266, 281 eller en overtrædelse af udlændingelovens § 59, stk. 5, (*kriminalitetskrav*).

Der er ikke fastsat noget krav til mistankens styrke (mistankekrav) i § 781, stk. 1. Om baggrunden herfor anførte Strafferetsplejeudvalget i betænkning nr. 1023/1984, side 97 f, bl.a., at der i loven bør fastlægges et fælles mistankekrav for alle indgreb i meddelelseshemmeligheden, og at dette bør udformes således, at mistankens styrke ikke nærmere beskrives, men at det blot angives, at der skal foreligge en mistanke. Det forudsættes i betænkningen, at mistanken skal være rimelig og konkret begrundet i de foreliggende oplysninger.

Som en fravigelse af det almindelige kriminalitetskrav kan der i medfør af § 781, stk. 2 og 3, foretages telefonaflytning og teleoplysning i sager om fredskrænkelser omfattet af straffelovens § 263, stk. 2 og 3, samt teleoplysning i sager om gentagne fredskrænkelser omfattet af straffelovens § 265 eller om overtrædelse af straffelovens § 279 a eller 293, stk. 1, begået ved anvendelse af en telekommunikationstjeneste.

Efter § 781, stk. 4, fraviges det almindelige kriminalitetskrav og indikationskrav endvidere ved foretagelse af brevåbning og brevstandsning, hvor der foreligger en særlig bestyrket mistanke om, at der i forsendelsen findes genstande, som bør konfiskeres, eller som ved en forbrydelse er fravendt nogen, som kan kræve dem tilbage.

Endelig følger der af § 781, stk. 5, et skærpet kriminalitetskrav ved anden aflytning (også kaldet rumaflytning) og udvidet teleoplysning, som kun kan foretages, når mistanken vedrører en forbrydelse, der har medført, eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Til gengæld kan der foretages udvidet teleoplysning, selv om der ikke foreligger bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt.

I overensstemmelse med den almindelige proportionalitetsgrundsætning må der i medfør af retsplejelovens § 782, stk. 1, ikke foretages et indgreb i meddelelseshemmeligheden, hvis det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde, ville være et uforholdsmæssigt indgreb.

Det følger af § 783, stk. 1, at indgreb i meddelelseshemmeligheden sker efter rettens kendelse. I kendelsen anføres de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår. Endvidere anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Efter § 783, stk. 2, fastsættes der ligeledes i kendelsen det tidsrum, inden for hvilket indgrebet i meddelelseshemmeligheden kan foretages. Dette tidsrum skal være så kort som muligt og må ikke overstige 4 uger. Tidsrummet kan ved kendelse forlænges med højst 4 uger ad gangen.

Politiet kan således som udgangspunkt kun foretage indgreb i meddelelseshemmeligheden efter at have indhentet en retskendelse.

Ville indgrebets øjemed blive forspildt, hvis politiet skulle afvente en forudgående retskendelse, kan politiet dog i medfør af § 783, stk. 3, selv træffe beslutning om indgrebet og derefter – snarest muligt og inden 24 timer – forelægge sagen for retten. Retten afgør herefter ved kendelse, om indgrebet kan godkendes, samt om det kan opretholdes og i bekræftende fald for hvilket tidsrum. Burde indgrebet efter rettens opfattelse ikke

være foretaget, skal retten give meddelelse herom til Justitsministeriet.

I medfør af retsplejelovens § 784, stk. 1, skal der beskikkes en advokat for den, indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig, inden retten træffer afgørelse efter § 783. Advokatbeskikkelse skal ske, uanset om der allerede er beskikket en forsvarer for den mistænkte person, som kan varetage dennes interesser.

Den advokat, der beskikkes efter § 784, stk. 1, skal således varetage interesserne ikke blot for den eller de mistænkte, men også for indehaverne af de telefoner eller lokaler mv., der aflyttes, samt for de personer, der mere eller mindre tilfældigt taler i en telefon, der aflyttes, eller som på anden måde bliver berørt af indgrebet, jf. betænkning nr. 1023/1984, side 81 f.

Angår efterforskningen en overtrædelse af straffelovens kapitel 12 eller 13, beskikkes advokaten fra en særlig kreds af advokater, jf. § 784, stk. 2. Der er i § 785 og § 787 fastsat regler om den beskikkede advokats rettigheder og pligter i forbindelse med sagens behandling.

Det følger af retsplejelovens § 786, stk. 1, at det påhviler postvirksomheder og udbydere af telenet eller teletjenester at bistå politiet ved gennemførelse af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler mv.

Når et indgreb i meddelelseshemmeligheden er afsluttet, skal der i medfør af § 788, stk. 1, jf. stk. 2, gives underretning om indgrebet til henholdsvis indehaveren af den pågældende telefon (telefonaflytning og teleoplysning), den der har rådighed over det pågældende lokale (rumaflytning), og afsenderen eller modtageren af forsendelsen (brevåbning og brevstandsning). Der skal ikke gives underretning om udvidet teleoplysning, jf. § 788, stk. 5.

Den advokat, der er beskikket i medfør af retsplejelovens § 784, stk. 1, skal modtage genpart af underretningen, jf. § 788, stk. 3, 3. pkt.

Det er den byret, som har truffet afgørelse om indgrebet, der skal foretage underretningen, jf. § 788, stk. 3, 1. pkt. Underretningen skal gives snarest muligt, hvis politiet ikke senest 14 dage efter udløbet af det tidsrum, hvor indgrebet har været tilladt, jf. § 783, stk. 2, har fremsat begæring om undladelse af eller udsættelse med underretning, jf. § 788, stk. 3, 2. pkt.

I medfør af § 788, stk. 4, 1. pkt., kan retten efter begæring fra politiet beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum, hvis underretningen vil være til skade for efterforskningen eller til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller hvis omstændighederne i øvrigt taler imod underretning.

Den advokat, der er beskikket i medfør af retsplejelovens § 784, stk. 1, skal have lejlighed til at udtale sig, inden retten træffer beslutning om undladelse af eller udsættelse med underretningen, jf. § 788, stk. 4, 2. pkt.

4.1.2. Særligt om kravet om anførelse af telefonnumre

Som nævnt i pkt. 4.1.1. følger det af retsplejelovens § 783, stk. 1, 2. pkt., at der i en kendelse om indgreb i meddelelseshemmeligheden skal anføres de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår.

Betydningen af denne bestemmelse for så vidt angår spørgsmålet om anførelse af telefonnumre fremgår bl.a. af en sag, der er gengivet i Ugeskrift for Retsvæsen 1999, side 1771. I denne sag havde anklagemyndigheden i byretten anmodet om rettens kendelse om, at det fremover skulle være tilladt for politiet at aflytte enhver samtale ført på de telefoner, som den mistænkte måtte skaffe sig rådighed over, og at der ligeledes blev givet politiet adgang til for disse telefoner at få teleoplysninger.

Anklagemyndigheden henviste under sagens behandling til, at en kendelse med det beskrevne indhold var af afgørende betydning for efterforskningen. I den forbindelse henviste anklagemyndigheden til, at politiet på grund af den sigtedes hurtige udskiftning af telefoner altid var 2-3 dage bagefter med efterforskningen og derved mistede afgørende oplysninger. Anklagemyndigheden anførte videre, at retten i hvert tilfælde ville blive underrettet, så der kunne afsiges kendelse efter retsplejelovens § 783, stk. 3.

Østre Landsret stadfæstede byrettens afgørelse om ikke at tage anklagemyndighedens anmodning til følge. Landsretten begrundede sit resultat med, at efter det oplyste ville en imødekommelse af anklagemyndighedens begæring ikke gøre det muligt i kendelsen at angive det eller de abonnentnumre, SIM-kortnumre eller IMEI-numre (en mobiltelefons serienummer), som begæredes aflyttet, hvorfor en sådan tilladelse ikke ville kunne opfylde kravene i retsplejelovens § 783, stk. 1, 2. pkt., om, at der bl.a. skal anføres de telefonnumre, lokaliteter og adressater, som indgrebet angår. Det begærede indgreb fandtes derfor ikke at have hjemmel i retsplejeloven.

Den gældende bestemmelse i retsplejelovens § 783, stk. 1, 2. pkt., blev som nævnt i pkt. 4.1.1. affattet ved lov nr. 227 af 6. juni 1985 om ændring af retsplejeloven (Telefonaflytning mv.), hvor der i retsplejeloven blev indsat et nyt kapitel 71 med regler om indgreb i meddelelseshemmeligheden.

Om baggrunden for bestemmelsen blev i de almindelige bemærkninger til lovforslaget anført følgende, jf. Folketingstidende 1984-85, tillæg A, spalte 2974:

»Med hensyn til *formen for rettens afgørelse* foreslås det i § 783, stk. 1, bl.a., at der ligesom i dag skal være tale om en kendelse, hvilket navnlig har den betydning, at rettens beslutning om indgrebets foretagelse skal begrundes, og § 783, stk. 1, foreskriver i den forbindelse, at retten skal anføre de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Udvalgets udkast til § 783 i retsplejeloven indeholder herudover forskellige formkrav vedrørende tidsfrister, angivelse af de pågældende telefonnumre, lokaliteter m.v.«

Lovændringen var baseret på Strafferetsplejeudvalgets betænkning nr. 1023/1984 om indgreb i meddelelseshemmeligheden og anvendelse af agenter, jf. pkt. 4.1.1. ovenfor. I betænkningen side 73 anførte Strafferetsplejeudvalget følgende:

»Ved indgreb i meddelelseshemmeligheden foreslår udvalget yderligere, at indgrebet bliver specificeret i kendelsen ved angivelse af »de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår«, jfr. lovudkastets § 783, stk. 1. Herved sikres, at den bemyndigelse, som kendelsen giver politiet, får en præcis afgrænsning.«

I betænkningen omtaltes bl.a. en analyse vedrørende indgreb i meddelelseshemmeligheden i Hans Gammeltoft-Hansens afhandling »Straffeprocessuelle tvangsindgreb« fra 1981. Denne afhandling indeholdt forslag til nye lovbestemmelser om straffeprocessuelle tvangsindgreb, herunder bl.a. indgreb i meddelelseshemmeligheden. Forslaget til en ny bestemmelse om telefonaflytning (og anden aflytning) var formuleret således, at der kunne foretages aflytning af telefonsamtaler »over for en person«, hvis de foreslåede mistankekrav og kriminalitetskrav var opfyldt, jf. Gammeltoft-Hansen, »Straffeprocessuelle tvangsindgreb«, 1981, side 306.

I bemærkningerne til forslaget til en ny bestemmelse om aflytning anførte Gammeltoft-Hansen bl.a., at ordene » over for en person .« tilkendegiver, at alle telefonapparater, hvor der er tilstrækkelig anledning til at antage, at meddelelser gives til eller fra en mistænkt, er omfattet af den foreslåede bestemmelse, jf. side 314 i afhandlingen.

Som det fremgår af bestemmelsen i retsplejelovens § 783, stk. 1, 2. pkt., bygger den gældende ordning ikke på dette forslag, men derimod på et krav om anførelse af de enkelte telefonnumre i kendelsen.

Hvad angår spørgsmålet om, *hvilke personers telefoner* som vil kunne aflyttes, anførte Strafferetsplejeudvalget følgende i betænkning nr. 1023/1984, side 98 f:

»Endvidere foreslås kravet om sammenhængen mellem den mistænkte person og kommunikationen beskrevet således, at der skal være »bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt«. Denne udformning giver adgang til at gribe ind i kommunikation, hvori en mistænkt direkte er part f.eks. som afsender eller modtager af et brev eller som deltager i en telefonsamtale eller anden samtale. Udformningen giver også mulighed for at gribe ind, hvis samtalen eller brevvekslingen føres mellem personer, der ikke er mistænkt, såfremt der er bestemte grunde til at antage, at de pågældende formidler meddelelser til eller fra en mistænkt og altså virker som budbringere for denne.

Det må i denne forbindelse erindres, at de gældende regler om telefonaflytning er indrettet således, at der gives politiet en generel tilladelse til at aflytte samtaler til og fra en bestemt telefon, når det må antages, at der over denne formidles samtaler til eller fra en mistænkt. Det er altså ikke nødvendigvis den mistænktes telefon, der aflyttes. F.eks. vil den mistænkte i narkotikasager undertiden befinde sig i udlandet. For at skaffe oplysning om tid og sted for hans hjemkomst – evt. i forbindelse med en narkotikaleverance – kan det være nødvendigt at aflytte telefoner hos ham nærtstående personer i Danmark. Det kan også undertiden være nødvendigt at aflytte offentlige telefoner, eventuelt telefonautomater, f.eks. i og omkring værtshuse, hvor der er mistanke om handel med narkotika.«

I praksis vil politiet således ofte indhente retskendelse om aflytning af telefoner, der tilhører andre personer end den mistænkte - f.eks. kæresten, arbejdspladsen, forældrene eller en nær ven – fordi der er bestemte grunde til at antage, at der gives meddelelser til eller fra den mistænkte fra disse personers telefoner.

Med hensyn til *hvilke samtaler* som vil kunne aflyttes, anførte Strafferetsplejeudvalget følgende på side 59 i betænkning nr. 1023/1984:

» Om den praktiske gennemførelse af telefonaflytning bemærkes, at indgrebet såvel efter de gældende regler som efter udvalgets lovudkast rettes mod alle telefonsamtaler, der inden for en bestemt periode føres fra en nærmere angivet telefon, som politiet har en særlig mistanke om vil blive benyttet i forbindelse med en forbrydelse. Herved rammer indgrebet altså også alle de personer, der – uden at have nogen forbindelse med forbrydelsen – tilfældigvis ringer op til eller fra den pågældende telefon. At indgrebet på denne måde rammer en række helt udenforstående personer, er uundgåeligt, da en snævrere afgrænsning af det tilladelige »lytteområde« end de samtaler, der føres over en bestemt telefon, ikke lader sig drage.«

4.2. Kendelse på person

4.2.1. Arbejdsgruppens overvejelser og anbefalinger

Den tværministerielle arbejdsgruppe om terrorbekæmpelse har i anbefaling nr. 26 i rapporten om det danske samfunds indsats og beredskab mod terror foreslået, at der skabes mulighed for, at en retskendelse om indgreb i meddelelseshemmeligheden kan være rettet mod personen og ikke kommunikationsmidlerne.

Om baggrunden for anbefalingen anfører arbejdsgruppen bl.a., at erfaringen viser, at en del mistænkte forsøger at sløre deres handlinger ved at anvende flere forskellige kommunikationsmidler. Det kan f.eks. være forskellige mobiltelefoner eller SIM-kort, som udskiftes løbende. Arbejdsgruppen peger i den forbindelse på, at den teknologiske udvikling gennem de senere år har betydet, at såvel antallet som tilgængeligheden af de til rådighed stående kommunikationsmidler er øget betydeligt.

Det anføres videre i rapporten, at hvis en mistænkt anvender flere forskellige kommunikationsmidler, skal der indhentes en retskendelse for hvert enkelt kommunikationsmiddel. Det medfører, at der skal holdes et retsmøde hver gang med inddragelse af en dommer og forsvarer, samt at politiet skal forberede sagen forud for retsmødet. Hvis der skabes mulighed for, at retskendelsen vedrører personen og ikke kommunikationsmidlet, vil der efter arbejdsgruppens opfattelse kunne spares ressourcer både hos domstole og politi, hvilket oplyses også at være vist ved erfaringer fra udlandet.

Arbejdsgruppen forudsætter, at politiet over for retten godtgør, at den person, indgrebet retter sig imod, anvender en flerhed af kommunikationsmidler, samt at retten efterfølgende orienteres om, hvilke kommunikationsmidler den person, som kendelsen vedrører, har anvendt.

Som det fremgår af regeringens handlingsplan for terrorbekæmpelse, har regeringen besluttet at arbejde videre med at konkretisere denne anbefaling. Udmøntningen af anbefalingen er indeholdt i dette lovforslag, jf. nedenfor under pkt. 4.2.2.

4.2.2. Justitsministeriets overvejelser

Som beskrevet i pkt. 4.1.2. følger det af retsplejelovens § 783, stk. 1, 2. pkt., at der i en kendelse om indgreb i meddelelseshemmeligheden skal anføres de telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår.

I de godt 20 år, der er forløbet, siden § 783, stk. 1, 2. pkt., trådte i kraft, er der sket en voldsom teknologisk udvikling inden for tele- og internetkommunikation. Omfanget af denne udvikling illustreres ikke mindst af de senere års fremvækst af en mangfoldighed af nye kommunikationsmidler som f.eks. mobiltelefoner, taletidskort, e-mail, internet-chat og IP-telefoner. Disse mange nye former for tele- og internetkommunikation anvendes i dag som helt sædvanlige kommunikationsmidler af en meget stor – og stadigt tiltagende – del af befolkningen. Samtidig udvides udbudet på telemarkedet hele tiden med videreudviklede og helt nye kommunikationsmidler.

Den hastige teknologiske udvikling indebærer i sagens natur betydelige udfordringer for politiet i forbindelse med efterforskning af de mange former for kriminalitet, hvor der kan være behov for at skaffe sig oplysninger om en mistænkts kommunikation med andre. Politiet må således i dag ofte indhente et større antal retskendelser vedrørende samme mistænkte person, herunder kendelser på andre personers – f.eks. familiemedlemmers eller arbejdsgiveres – telefonnumre, som den mistænkte har adgang til.

Som anført af den tværministerielle arbejdsgruppe om terrorbekæmpelse er det i den forbindelse politiets erfaring, at mange mistænkte forsøger at sløre deres handlinger ved at anvende flere forskellige kommunikationsmidler og f.eks. løbende udskifte mobiltelefoner eller SIM-kort. Politiets Efterretningstjeneste har over for Justitsministeriet oplyst, at det ikke er usædvanligt, at mistænkte, som tjenesten har behov for at overvåge, benytter sig af et stort antal forskellige telefoner eller taletidskort på samme tid. Der har således været tilfælde, hvor det har været nødvendigt at indhente et endog meget betydeligt antal retskendelser om telefonaflytning i en enkelt sag.

Den beskrevne udvikling gør det vanskeligt for politiet at være tilstrækkelig på forkant med, hvilke telefonnumre en mistænkt benytter, til, at politiet kan nå – løbende – at indhente forudgående retskendelser på alle relevante telefonnumre. Når det opdages, at en mistænkt benytter sig af (endnu) et telefonnummer, som politiet ikke hidtil har haft kendskab til, vil formålet med aflytningen af den pågældende ofte blive forspildt, hvis politiet herefter skal afvente, at der indhentes en ny retskendelse. Det er derfor ikke sjældent nødvendigt for politiet straks at iværksætte aflytning af det nye telefonnummer, jf. retsplejelovens § 783, stk. 3, om politiets adgang til selv at træffe beslutning om indgreb i meddelelseshemmeligheden, når indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes. Som beskrevet i pkt. 4.1.1. skal politiet herefter snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten.

Det samme gør sig endvidere gældende med hensyn til teleoplysning efter retsplejelovens § 780, stk. 1, nr. 3, det vil sige, hvor politiet – uanset om det sker i tilknytning til en aflytning eller ej – har behov for oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat. I sådanne tilfælde giver det således anledning til tilsvarende vanskeligheder for politiet på forhånd at angive de konkrete telefonnumre, hvor der er behov for at iværksætte teleoplysning.

Om arbejdsgruppens forslag bemærkes herefter følgende:

Som anført i forarbejderne til den gældende bestemmelse i retsplejelovens § 783, stk. 1, 2. pkt., bygger kravet om, at kendelsen skal angive de telefonnumre, som indgrebet vedrører, på hensynet til, at den bemyndigelse, som rettens kendelse giver politiet, er præcist afgrænset. Herved undgås det, at der opstår tvivl om, hvorvidt politiet ved den efterfølgende aflytning har holdt sig inden for de grænser, som retten har fastsat.

Heroverfor står – som nærmere beskrevet ovenfor og i arbejdsgruppens rapport – at den teknologiske udvikling på området i stigende grad vanskeliggør politiets efterforskning mv., ligesom den gældende ordning efter omstændighederne kan medføre en meget væsentlig ressourcemæssig belastning af såvel politiet som domstolene. Særligt med hensyn til terrorområdet bemærkes, at det som omtalt ovenfor er Politiets Efterretningstjenestes erfaring, at de kredse, der mistænkes for forbindelse med mulig terrorvirksomhed, i væsentlig grad søger at udnytte den teknologiske udvikling inden for tele- og internetkommunikation til at undgå overvågning fra myndighedernes side. Bl.a. derfor er det som ligeledes beskrevet ovenfor i mange tilfælde nødvendigt at iværksætte aflytning uden retskendelse i medfør af retsplejelovens § 783, stk. 3, (på øjemedet).

På den baggrund er Justitsministeriet enig med arbejdsgruppen i, at der kan være anledning til – i hvert fald på terrorområdet og inden for rammerne af efterfølgende kontrol fra rettens side, jf. nærmere nedenfor – at tilpasse bestemmelsen i retsplejelovens § 783, stk. 1, 2. pkt., til den teknologiske udvikling.

Det foreslås derfor i lovforslagets § 2, nr. 4, at der i § 783 indsættes et nyt stk. 2, hvorefter retten ved kendelse om telefonaflytning (det vil sige aflytning af telefonsamtaler eller anden tilsvarende telekommunikation) eller teleoplysning i forbindelse med efterforskning af en overtrædelse af straffelovens kapitel 12 eller 13 i stedet for bestemte telefonnumre kan anføre den person, som indgrebet angår. Den foreslåede bestemmelse omfatter således alle de indgreb i meddelelseshemmeligheden, der er omfattet af retsplejelovens § 780, stk. 1, nr. 1 og 3, uanset om der er tale om egentlig telefonkommunikation eller anden tilsvarende telekommunikation, f.eks. e-mail-, internet- eller telefaxkommunikation.

For så vidt angår teleoplysning skal det bemærkes, at den foreslåede bestemmelse alene omfatter fremadrettet teleoplysning i medfør af retsplejelovens § 780, stk. 1, nr. 3, og ikke bagudrettet teleoplysning i medfør af editionsreglerne, jf. Højesterets kendelse gengivet i UfR 1993, side 1. Der vil således ikke på grundlag af en kendelse på person kunne indhentes historiske teleoplysninger.

Kendelse på en person i medfør af den foreslåede affattelse af retsplejelovens § 783, stk. 2, 1. pkt., forudsætter naturligvis, at de øvrige betingelser for henholdsvis telefonaflytning eller teleoplysning er opfyldt. Den foreslåede bestemmelse vil ikke udvide politiets adgang til at iværksætte telefonaflytning eller teleoplysning, men derimod alene forenkle den formelle procedure, så politiet kun behøver at indhente én forudgående retskendelse. De almindelige betingelser for, hvornår telefonaflytning mv. kan foretages, videreføres således uændret.

Det skal i den forbindelse understreges, at indgreb i meddelelseshemmeligheden efter retsplejelovens § 781, stk. 1, nr. 1, ligesom i dag kun vil kunne foretages, hvis der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt. Der vil således kun kunne foretages aflytning af et telefonnummer eller indhentes teleoplysninger om, hvilke telefoner der sættes i forbindelse med et bestemt telefonnummer, når der er bestemte grunde til at antage, at der over denne telefon formidles samtaler til eller fra den mistænkte person. Der henvises til pkt. 1.1., 4.1.1. og 4.1.2. samt Strafferetsplejeudvalgets betænkning nr. 1023/1984, side 98.

Betingelsen i § 781, stk. 1, nr. 1, vil således skulle være opfyldt i relation til hvert enkelt telefonnummer, der aflyttes eller indhentes teleoplysninger om på grundlag af en retskendelse på personen i medfør af den foreslåede nye bestemmelse i § 783, stk. 2, 1. pkt. Som nærmere beskrevet nedenfor skal der endvidere ske en efterfølgende underretning af retten om bl.a. de konkrete omstændigheder i sagen, hvorpå det støttes, at der er bestemte grunde til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den person, som indgrebet angår.

Udover kravet i § 781, stk. 1, nr. 1, vil det være en forudsætning for at få en retskendelse på personen, at de øvrige almindelige betingelser for indgreb i meddelelseshemmeligheden er opfyldt. Det gælder f.eks. indikationskravet i § 781, stk. 1, nr. 2, proportionalitetskravet i § 782, stk. 1, og kravet om, at der i kendelsen skal fastsættes det tidsrum, inden for hvilket indgrebet må foretages, jf. § 783, stk. 2, (der efter forslaget bliver § 783, stk. 3). Der henvises i øvrigt til beskrivelsen af gældende ret i pkt. 4.1.1.

Arbejdsgruppen har som anført i pkt. 4.2.1. forudsat, at politiet som betingelse for, at den foreslåede bestemmelse kan anvendes, over for retten godtgør, at den person, indgrebet retter sig imod, anvender en flerhed af kommunikationsmidler. Om dette spørgsmål bemærkes følgende:

Som beskrevet ovenfor er det en forudsætning både for at få en kendelse på personen og for at iværksætte aflytning eller teleoplysning på grundlag af en sådan kendelse, at de almindelige betingelser for telefonaflytning eller teleoplysning er opfyldt i forhold til hvert enkelt telefonnummer.

Den foreslåede bestemmelse vil imidlertid forenkle proceduren, så politiet kun behøver at indhente én forudgående retskendelse. En sådan retskendelse om telefonaflytning af personen vil give mulighed for at aflytte den mistænkte person, uanset hvilke telekommunikationsmidler den pågældende måtte vælge at benytte sig af. Med hjemmel i en sådan forudgående retskendelse vil politiet løbende kunne iværksætte aflytning af alle

de telefonnumre, der er bestemte grunde til at antage bliver benyttet af en person, som er mistænkt for overtrædelse af straffelovens kapitel 12 eller 13. Tilsvarende vil en retskendelse om teleoplysning på personen give mulighed for løbende at indhente oplysninger om, hvilke telefonnumre der sættes i forbindelse med de telefoner, som der er bestemte grunde til at antage, at den mistænkte person benytter.

Efter Justitsministeriets opfattelse bør det ikke herudover være en særlig betingelse, at politiet i de konkrete tilfælde godtgør, at den person, indgrebet retter sig imod, anvender en flerhed af kommunikationsmidler. Justitsministeriet har i den forbindelse lagt vægt på, at formålet med den foreslåede adgang til retskendelse på en person i sager om overtrædelse af straffelovens kapitel 12 og 13 som anført er at forenkle proceduren, og at det som nævnt er Politiets Efterretningstjenestes generelle erfaring, at netop de kredse, der mistænkes for forbindelse med mulig terrorvirksomhed, i væsentlig grad søger at udnytte den teknologiske udvikling inden for tele- og internetkommunikation til at undgå overvågning fra myndighedernes side.

Det fremgår af pkt. IV i Justitsministeriets instruks af 9. maj 1996 om Politiets Efterretningstjeneste, at indgribende efterforskningsskridt, herunder indgreb i meddelelseshemmeligheden, i hvert enkelt tilfælde skal godkendes af chefen for tjenesten eller i dennes fravær af chefens stedfortræder. Såfremt det pågældende efterforskningsskridt kræver retskendelse, skal denne godkendelse finde sted, forinden sagen forelægges for retten i overensstemmelse med retsplejelovens regler.

I overensstemmelse hermed forudsættes det, at den praktiske iværksættelse af telefonaflytning eller teleoplysning, der sker på grundlag af en retskendelse på personen, for hvert enkelt telefonnummers vedkommende skal forelægges til forudgående godkendelse hos chefen for Politiets Efterretningstjeneste eller dennes stedfortræder.

I medfør af den foreslåede affattelse af § 783, stk. 2, 2. pkt., skal politiet snarest muligt efter udløbet af det tidsrum, inden for hvilket indgrebet kan foretages, underrette retten om de telefonnumre – herunder f.eks. IMSI- eller IMEI-numre – som indgrebet har været rettet imod (det vil sige de telefonnumre, som er blevet aflyttet, eller hvor der har været iværksat teleoplysning), samt om de bestemte grunde, der er til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte, jf. kravet i § 781, stk. 1, nr. 1.

Det forudsættes, at denne underretning af retten indeholder oplysninger svarende til dem, som skal medtages, når indgreb, der er iværksat af politiet uden forudgående retskendelse (på øjemedet), efterfølgende skal forelægges for retten til godkendelse, jf. § 783, stk. 3 (der efter forslaget bliver § 783, stk. 4).

Politiets underretning til retten sker med henblik på, at retten herefter underretter den advokat, som er beskikket i sagen i medfør af retsplejelovens § 784, stk. 1, jf. den foreslåede bestemmelse i § 783, stk. 2, 3. pkt. I praksis vil retten ofte kunne foretage denne underretning samtidig med den underretning af den beskikkede advokat, som retten allerede i dag skal foretage efter § 788, stk. 3, 3. pkt., jf. stk. 4, 2. pkt. En efterprøvelse af lovligheden af indgrebet forudsættes ikke foretaget på dette tidspunkt, hvor retten alene ville have politiets fremstilling som grundlag. Den beskikkede advokat vil imidlertid efter at have modtaget underretningen kunne indbringe spørgsmålet for retten, jf. herom nedenfor.

Den advokat, der efter § 784, stk. 1, skal beskikkes i sager om indgreb i meddelelseshemmeligheden, skal beskikkes, uanset om der allerede er beskikket en forsvarer for den mistænkte, som kan varetage dennes interesser. Den beskikkede advokat skal således varetage interesserne for ikke blot den mistænkte, men også for indehaverne af de telefoner, som f.eks. aflyttes, og de personer, der mere eller mindre tilfældigt kommer til at tale i en sådan telefon, eller som på anden måde bliver berørt af indgrebet.

Underretningen af den beskikkede advokat om, hvilke telefonnumre der er blevet aflyttet, eller hvor der har været iværksat teleoplysning – og om de bestemte grunde, der er til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte – skal gøre det muligt for advokaten at tage stilling til, om spørgsmålet om lovligheden af indgrebet skal indbringes for retten.

Spørgsmålet om lovligheden af aflytning eller teleoplysning gennemført på grundlag af en forudgående retskendelse på personen kan således indbringes for retten i medfør af den foreslåede bestemmelse i § 783, stk. 2, 3. pkt. Formålet hermed er at sikre en adgang til kontrol ved domstolene med hensyn til de konkrete telefonnumre, som politiet har aflyttet eller indhentet teleoplysninger om på grundlag af en retskendelse på personen. Hvis sagen indbringes for retten af den beskikkede advokat, afgør retten ved kendelse, om indgrebet er sket inden for rammerne af den forudgående retskendelse på personen og i øvrigt i overensstemmelse med retsplejelovens almindelige betingelser for telefonaflytning og teleoplysning, jf. bl.a. § 781, stk. 1, nr. 1.

Finder retten i den forbindelse, at politiet har foretaget et indgreb, som ikke burde være foretaget, skal retten give meddelelse herom til Justitsministeriet, jf. den foreslåede bestemmelse i § 783, stk. 2, 5. pkt. Dette svarer til, hvad der i dag gælder efter retsplejelovens § 783, stk. 3, 4. pkt., i de tilfælde, hvor politiet har iværksat et indgreb i meddelelseshemmeligheden uden forudgående retskendelse (på øjemedet), og retten får forelagt sagen med henblik på efterfølgende godkendelse, men ikke godkender indgrebet.

I lyset af den beskrevne teknologiske udvikling har Justitsministeriet overvejet, om der kunne være anledning til udstrække den foreslåede ændring af retsplejelovens § 783 til at gælde generelt og ikke kun på terrorområdet. De vanskeligheder, som udviklingen på tele- og internetkommunikationsområdet medfører for politiet, og som er nærmere beskrevet ovenfor, gør sig således også gældende med hensyn til en række andre kriminalitetsformer, herunder f.eks. narkotikakriminalitet.

Heroverfor står, at den foreslåede ændring kan siges at have en vis principiel karakter, og at en ordning, hvorefter den udstrækkes til at gælde generelt, derfor bør overvejes i en bredere sammenhæng.

På denne baggrund er det Justitsministeriets opfattelse, at den foreslåede ændring på nuværende tidspunkt bør afgrænses til at vedrøre sager om overtrædelse af straffelovens kapitel 12 og 13, således at en mere generel ændring på området i givet fald tages op til nærmere overvejelse på et senere tidspunkt.

4.3. Undladelse af underretning

4.3.1. Arbejdsgruppens overvejelser og anbefalinger

Den tværministerielle arbejdsgruppe om terrorbekæmpelse har i anbefaling nr. 27 i rapporten om det danske samfunds indsats og beredskab mod terror foreslået, at undladelse af underretning, jf. retsplejelovens § 788, stk. 4, kan ske på baggrund af hensyn til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder.

Arbejdsgruppen har i den forbindelse henvist til, at det følger af retsplejelovens § 729 c, stk. 1, nr. 6, at retten efter anmodning fra politiet kan bestemme, at reglerne om forsvarerens og sigtedes ret til aktindsigt fraviges, hvis det er påkrævet af hensyn til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder. Efter arbejdsgruppens opfattelse gør disse hensyn sig ligeledes gældende ved indgreb i meddelelseshemmeligheden, da der kan forekomme situationer, hvor politiet anvender teknikker, som ikke er kendt i en bredere kreds, herunder det kriminelle miljø, og hvor en underretning om indgrebet vil kunne ødelægge politiets mulighed for at anvende denne efterforskningsteknik fremover.

Som det fremgår af regeringens handlingsplan for terrorbekæmpelse, har regeringen besluttet at arbejde videre med at konkretisere denne anbefaling. Dette lovforslag udmønter den pågældende anbefaling, jf. nedenfor under pkt. 4.3.2.

4.3.2. Justitsministeriets overvejelser

Som beskrevet i pkt. 4.1.1. følger det af den gældende bestemmelse i retsplejelovens § 788, stk. 4, at retten efter begæring fra politiet kan beslutte, at underretning i medfør af § 788, stk. 1-3, om et afsluttet indgreb i meddelelseshemmeligheden skal undlades eller udsættes i et nærmere fastsat tidsrum, hvis underretningen vil være til skade for efterforskningen eller til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller hvis omstændighederne i øvrigt taler imod underretning.

Justitsministeriet kan tilslutte sig arbejdsgruppens anbefaling om, at der fastsættes en udtrykkelig hjemmel til at undlade underretning på grundlag af hensynet til at beskytte fortrolige oplysninger om politiets efterforskningsmetoder. Det vil således kunne skabe betydelige problemer for politiets fremtidige efterforskningsmuligheder, hvis sådanne oplysninger spredes i kriminelle miljøer.

Det foreslås derfor i lovforslagets § 2, nr. 5, at retsplejelovens § 788, stk. 4, ændres, så det kommer til at fremgå, at hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder taler imod underretning, kan retten efter begæring fra politiet beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum, der kan forlænges.

Underretning om et indgreb i meddelelseshemmeligheden vil således kunne undlades, hvis oplysningen om, at der er gennemført et sådant indgreb, i sig selv vil afsløre ellers fortrolige oplysninger om politiets efterforskningsmetoder.

Det forudsættes, at udtrykket »fortrolige oplysninger om politiets efterforskningsmetoder« har samme anvendelsesområde som den tilsvarende formulering i retsplejelovens § 729 c, stk. stk. 1, nr. 6. Efter denne bestemmelse kan retten efter anmodning fra politiet bestemme, at reglerne om forsvarerens og sigtedes ret til aktindsigt efter §§ 729 a og 729 b fraviges, hvis det er påkrævet af hensyn til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder. § 729 c, stk. 1, nr. 6, (tidligere § 745 b, stk. 1, nr. 6) blev affattet ved lov nr. 436 af 10. juni 2003 om ændring af straffeloven og retsplejeloven (Bekæmpelse af rockerkriminalitet og anden organiseret kriminalitet). Der henvises til Folketingstidende 2002-03, tillæg A, side 6696, tillæg B, side 1663 og 1858, samt Folketingets forhandlinger, side 8417, 10095 og 10510.

I overensstemmelse med forarbejderne til retsplejelovens § 729 c, stk. 1, nr. 6, forudsættes det ved den foreslåede formulering af § 788, stk. 4, at oplysninger om »politiets efterforskningsmetoder« f.eks. vil kunne være tekniske oplysninger om politiets aflytningsudstyr og –metoder mv. Der forudsættes endvidere at være tale om »fortrolige oplysninger«, hvis politiet har en særlig interesse i at holde oplysningerne hemmelige, og oplysningerne ikke er almindeligt kendt.

5. Teleobservation

9, jf. artikel 5, idet Justitsministeriet agter at udnytte forbeholdsadgangen i artikel 20, stk. 2, i forhold til disse bestemmelser.

Det skal endelig fremhæves, at der fortsat vil være adgang til at nægte udlevering efter de øvrige nægtelsesgrunde i udleveringsloven, herunder reglerne i § 6 om risiko for politisk forfølgning, tortur mv. i det anmodende land, reglerne i § 7 om humanitære hensyn samt reglerne i §§ 8-9 om »ne bis in idem«-princippet og forældelse. Desuden må udlevering fortsat kun ske på vilkår af, at en eventuel dødsstraf for den pågældende handling i givet fald ikke fuldbyrdes.

Europarådets konvention om forebyggelse af terrorisme træder ifølge konventionens artikel 23 i kraft den første dag i den måned, der følger efter udløbet af en periode på 3 måneder efter den dato, hvor 6 undertegnende parter, herunder mindst 4 af Europarådets medlemsstater, har udtrykt deres samtykke til at være bundet af konventionen. Konventionen er endnu ikke trådt i kraft.

FN's konvention om nuklear terrorisme træder ifølge konventionens artikel 25 i kraft den 30. dag efter datoen for deponeringen af det 22. ratifikations-, accept-, godkendelses- eller tiltrædelsesinstrument hos De Forenedes Nationers generalsekretær. Konventionen er endnu ikke trådt i kraft.

Ikraftsættelse af den danske gennemførelsesbestemmelse om udlevering for politiske lovovertrædelser, jf. lovforslagets § 5, kunne derfor medføre, at der i en periode, hvor konventionerne endnu ikke er trådt i kraft, kunne ske udlevering for handlinger i videre omfang, end Danmark er konventionsmæssigt forpligtet til.

På den baggrund har Justitsministeriet overvejet, om ikrafttrædelsesbestemmelsen bør udformes således, at ændringen først finder anvendelse på anmodninger om udlevering, der fremsættes efter, at de pågældende konventioner er trådt i kraft mellem Danmark og vedkommende fremmede stat.

En lignende fremgangsmåde er benyttet ved lov nr. 280 af 25. april 2001 (Gennemførelse af FN's terrorbombekonvention mv.), lov nr. 378 af 6. juni 2002 (anti-terrorpakken) og lov nr. 1160 af 19. december 2003 (Gennemførelse af ændringsprotokollen af 15. maj 2003 til den europæiske konvention om bekæmpelse af terrorisme).

Det er Justitsministeriets opfattelse, at ikrafttrædelsesbestemmelsen i dette lovforslag bør udformes på tilsvarende måde. Det foreslås derfor, at loven finder anvendelse, hvor der fremsættes anmodning om udlevering efter Europarådets konvention om forebyggelse af terrorisme efter, at denne konvention er trådt i kraft mellem Danmark og vedkommende fremmede stat, og tilsvarende hvor der fremsættes anmodning om udlevering efter FN's konvention om nuklear terrorisme efter, at denne konvention er trådt i kraft mellem Danmark og vedkommende fremmede stat.

10. Logning af trafikdata vedrørende telekommunikation

10.1. Gældende ret

Ved lov nr. 378 af 6. juni 2002 vedtog Folketinget den såkaldte anti-terrorpakke. Med loven indførtes bl.a. en ny bestemmelse i retsplejelovens § 786, stk. 4, om opbevaring og registrering af oplysninger om teletrafik. Der henvises til Folketingstidende 2001-01, 2. samling, tillæg A, side 808, og Folketingets forhandlinger, side 1321, 7439 og 7747.

Efter den såkaldte logningsbestemmelse i retsplejelovens § 786, stk. 4, 1. pkt., påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Den nærmere tekniske udmøntning af logningsforpligtelsen fastsættes administrativt af justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling, jf. § 786, stk. 4, 2. pkt. Justitsministeren fastsætter – efter forhandling med ministeren for videnskab, teknologi og udvikling – tidspunktet for logningsforpligtelsens ikrafttræden.

Med § 8 i lov nr. 378 af 6. juni 2002 blev det endvidere fastsat, at justitsministeren i folketingsåret 2005-06 skal fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var, at ordningen med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskningen var en nyskabelse, og at Justitsministeriet derfor fandt det hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse.

10.2. Justitsministeriets overvejelser

Den 24. marts 2004 sendte Justitsministeriet et udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik i høring hos en række myndigheder og organisationer. I lyset af de indkomne høringssvar besluttede Justitsministeriet i september 2004 at nedsætte en arbejdsgruppe med deltagelse af repræsentanter for IT- og telebranchen samt boligforeningerne med henblik på yderligere drøftelser af udkastet til bekendtgørelse og vejledning.

Sideløbende hermed er spørgsmålet om regler om logning af oplysninger om teletrafik blevet drøftet i EU-regi. Som led i EU's samlede indsats mod terrorisme og på baggrund af terrorangrebene i Madrid den 11. marts 2004 fremlagde en række medlemslande (Frankrig, Irland, Storbritannien og Sverige) således den 28. april 2004 et forslag til en rammeafgørelse om opbevaring af data, der behandles og lagres i forbindelse

med levering af offentligt tilgængeligt kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger. Forslaget til rammeafgørelse er blevet drøftet på en række møder i EU-regi, herunder i Rådet.

I lyset af denne udvikling orienterede Justitsministeriet ved brev af 30. september 2004 Folketingets Retsudvalg om de videre overvejelser med hensyn til udformningen af de danske regler på området. Justitsministeriet tilkendegav i den forbindelse, at ministeriet fandt det rigtigst ikke at udstede regler på området, før rammeafgørelsen enten var vedtaget, eller forhandlingerne havde vist, at der ikke var udsigt til, at der på kortere sigt kunne opnås enighed i Rådet.

Kommissionen har efterfølgende den 21. september 2005 fremlagt et forslag til et direktiv på området, og på rådsmødet (retlige og indre anliggender) den 21. februar 2006 blev et direktiv om opbevaring af trafikdata vedtaget med kvalificeret flertal.

Spørgsmålet om gennemførelse af direktivet om opbevaring af trafikdata vil blive behandlet i ekspertgruppen om logning, og det forventes, at arbejdet i ekspertgruppen kan afsluttes i løbet af sommeren 2006 med henblik på udstedelse af en bekendtgørelse om logning i efteråret 2006. Når logningsbekendtgørelsen udstedes, vil forpligtelsen i retsplejelovens § 786, stk. 4, for udbydere af telenet eller teletjenester til at registrere og opbevare oplysninger om teletrafik blive sat i kraft.

Med henblik på at sikre en evaluering af ordningen med logning af oplysninger om teletrafik på et tidspunkt, hvor der har været mulighed for over et relevant tidsrum at indhøste erfaringer med en sådan forpligtelse, foreslås det at fastsætte et nyt tidspunkt for revisionen af logningsbestemmelsen. Det foreslås således, at justitsministeren i folketingsåret 2009-10 fremsætter forslag om revision af retsplejelovens § 786, stk. 4. Med en forventet udstedelse af logningsbekendtgørelsen og ikrafttræden af retsplejelovens § 786, stk. 4, i efteråret 2006 indebærer dette, at ordningen tages op til fornyet overvejelse efter et tidsrum, der svarer til det oprindelig forudsatte ved vedtagelsen af anti-terrorpakken i sommeren 2002.

11. Lovforslagets økonomiske og administrative konsekvenser mv.

Ved de foreslåede ændringer af retsplejeloven gennemføres en vis tilpasning og forenkling af reglerne om Politiets Efterretningstjenestes indhentelse og videregivelse af oplysninger og af bestemmelserne om indgreb i meddelelseshemmeligheden mv. i overensstemmelse med den teknologiske udvikling og udviklingen i terrortruslen. Ændringerne indebærer herved en vis administrativ lettelse for bl.a. politiet, herunder Politiets Efterretningstjeneste, og for andre forvaltningsmyndigheder i forbindelse med efterretningstjenestens indhentelse af oplysninger.

Den foreslåede bestemmelse i retsplejelovens § 791 a, stk. 5, om teleobservation, giver politiet mulighed for efter rettens kendelse at foretage teleobservation. Det vil efter lovforslagets § 791 a, stk. 6, på samme måde som det er tilfældet ved gennemførelsen af f.eks. indgreb i meddelelseshemmeligheden, påhvile udbydere af telenet og teletjenester at bistå politiet ved gennemførelse af teleobservation, herunder ved at give de oplysninger der er omfattet af den foreslåede § 791 a, stk. 5. Forpligtelsen til at bistå politiet indebærer som udgangspunkt administrative omkostninger for udbyderne i forbindelse med gennemførelse af de konkrete teleobservationer, men omkostningerne herved afholdes af politiet i lighed med, hvad der er tilfældet ved andre lignende straffeprocessuelle tvangsindgreb. Som anført ovenfor under pkt. 5. indebærer lovforslaget, at der i retsplejeloven indsættes en særskilt bestemmelse om teleobservation som efterforskningsskridt. Der er imidlertid tale om et efterforskningsskridt, der også i dag anvendes af politiet, og det skønnes ikke muligt nærmere at vurdere, i hvilket omfang lovforslaget i sig selv vil kunne medføre en stigning i politiets udgifter hertil.

Lovforslaget skønnes ikke i øvrigt at have økonomiske eller administrative konsekvenser for det offentlige af betydning.

Forslaget har været sendt til Erhvervs- og Selskabsstyrelsens Center for Kvalitet i ErhvervsRegulering (CKR) med henblik på en vurdering af, om forslaget skal forelægges Økonomi- og Erhvervsministeriets virksomhedspanel. Styrelsen vurderer, at forslaget om pålæg om kvalitet og opbevaring af tv-optagelser vil medføre administrative konsekvenser for de virksomheder, der modtager et sådan pålæg. Da det endnu ikke vides, hvor ofte politiet vil gøre brug af disse muligheder, kan CKR først kvantificere konsekvenserne, når forslagene er trådt i kraft. Kvantificeringen vil finde sted i forbindelse med opdateringen af Justitsministeriets AMVAB-måling. Forslaget om, at luftfartselskaber skal foretage registrering og opbevaring i 1 år af oplysninger om passagerer og besætningsmedlemmer på luftfartøjer vurderes at medføre store løbende administrative konsekvenser for de 23 omfattede virksomheder. De nærmere krav til registrering og opbevaring fastsættes i en bekendtgørelse, og det anbefales således, at denne bekendtgørelse oversendes til CKR så hurtigt som muligt, med henblik på en vurdering af de administrative konsekvenser.

Samlet set vurderes det ikke, at de konkrete bestemmelser i lovforslaget indeholder administrative konsekvenser for erhvervslivet i et omfang, der berettiger, at det bliver forelagt virksomhedspanelet. Forslaget har derfor ikke været forelagt Økonomi- og Erhvervsministeriets virksomhedspanel.

Lovforslaget skønnes ikke i sig selv at have økonomiske konsekvenser for erhvervslivet af betydning. Der henvises til det samtidig hermed fremsatte forslag til lov om ændring af lov om konkurrence- og forbrugerforhold på telemarkedet, lov om radiofrekvenser og lov om radio- og terminaludstyr og elektromagnetiske forhold (Opfølgning på regeringens handlingsplan for terrorbekæmpelse).

Lovforslaget har ingen miljømæssige konsekvenser og indeholder ikke EU-retlige aspekter.

	Positive konsekvenser/ mindreudgifter	Negative konsekvenser/ merudgifter
Økonomiske konsekvenser for stat, kommuner og amtskommuner	Ingen	Ingen af betydning. Det skønnes ikke muligt nærmere at vurdere, i hvilket omfang lovforslaget i sig selv vil kunne medføre en stigning i politiets udgifter til teleobservation.
Administrative konsekvenser for stat, kommuner og amtskommuner	Lovforslaget skønnes at indebære visse administrative lettelser	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen af betydning
Administrative konsekvenser for erhvervslivet	Ingen	Lovforslaget, navnlig de foreslåede ændringer i luftfartsloven og indførelsen af nye regler om luftfartsselskabernes registrering og opbevaring af passageroplysninger, skønnes at have administrative omkostninger for erhvervslivet.
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter	

12. Hørte myndigheder mv.

Straffelovrådets betænkning nr. 1474/2006 om det strafferetlige værn mod terrorisme har – sammen med et udkast til forslag til ændring af udleveringsloven – været sendt i høring hos følgende myndigheder og organisationer mv.:

Præsidenterne for Østre og Vestre Landsret, præsidenterne for Københavns Byret og for retterne i Århus, Odense, Ålborg og Roskilde, Den Danske Dommerforening, Domstolsstyrelsen, Dommerfuldmægtigforeningen, Rigsadvokaten, Rigspolitichefen, Politidirektøren i København, Foreningen af Politimestre i Danmark, Politifuldmægtigforeningen, Politiforbundet i Danmark, Advokatrådet, Landsforeningen af beskikkede advokater, Institut for Menneskerettigheder, Dansk Retspolitisk Forening, Retssikkerhedsfonden, Energistyrelsen og Statens Institut for Strålehygiejne.

Den øvrige del af lovforslaget har – bortset fra lovforslagets § 6 – forud for fremsættelsen været i høring hos følgende myndigheder og organisationer mv.:

Præsidenterne for Østre og Vestre Landsret, præsidenterne for Københavns Byret og for retterne i Århus, Odense, Ålborg og Roskilde, Den Danske Dommerforening, Domstolsstyrelsen, Dommerfuldmægtigforeningen, Rigsadvokaten, Rigspolitichefen, Politidirektøren i København, Foreningen af Politimestre i Danmark, Politifuldmægtigforeningen, Politiforbundet i Danmark, Advokatrådet, Landsforeningen af beskikkede advokater, Institut for Menneskerettigheder, Det Kriminalpræventive Råd, Finansforbundet, Finansrådet, Kommunernes Landsforening, Dansk Handel & Service, Forbrugerrådet, Datatilsynet, Den Danske Brancheforening for Sikkerhed og Sikring, Dansk Industri, Dansk Retspolitisk Forening, Retssikkerhedsfonden, Brancheforeningen Telekommunikationsindustrien, Brancheorganisationen ForbrugerElektronik, Canal Digital Danmark A/S, Viasat A/S, Dansk IT, ISPA DK (Foreningen af Internetleverandører), Foreningen af Danske InternetMedier, IT-Brancheforeningen, ITEK/Dansk Industri, PROSA, SAM-DATA (HK), IFPI Danmark, Business Software Alliance Danmark, Multimedieforeningen, CSC Danmark A/S, Grossistforeningen for Radio og Elektronik, Kommunedata KMD, Sonofon I/S, Tele 2 A/S, TDC A/S, Telia A/S, Realkreditrådet, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Leverandørforeningen for Radiokommunikation, Air Greenland A/S, Airport Coordination Denmark A/S, AOPA Danmark, Atlantic Airways, Billund Lufthavn, Cabin Union Denmark, Cimber Air A/S, Danish Air Transport ApS, Dansam c/o Lufthavnschef Peter Bay, Dansk Arbejdsgiverforening, Dansk Flyvelederforening, Københavns Lufthavn, DALPA, Erhvervsflyvningens Sammenslutning, Flyvesikringstjenensten/Naviair, Forbrugerrådet, Havarikommissionen for Civil Luftfart, Konkurrencestyrelsen, Københavns Lufthavne A/S, KZ & Veteranfly Klubben, LSG Sky Chefs, Kongelig Dansk Aeroklub, My Travel Airways A/S, Nordisk Flyforsikringsgruppe (NFG), North Flying A/S, Novia, Rådet for Større Flysikkerhed, SAS - afdeling AX, SAS - Head Office - afd. DX, Servisair Danmark A/S, Star Air A/S, Statens Luftfartsvæsen, Sterling Airlines A/S, Sun-Air of Scandinavia, Association of Travel Managers in Denmark, Dansk Handicap Forbund, De Samvirkende Invalideorganisationer, Foreningen af Rejsearrangører I Danmark (RiD), Danmarks Rejsebureau Forening.

Bemærkninger til lovforslagets enkelte bestemmelser

I *bilag 3* til lovforslaget er de foreslåede bestemmelser sammenholdt med de nugældende regler.

Til § 1

Til nr. 1 (straffelovens § 110 d)

Efter straffelovens § 110 d kan den foreskrevne straf forhøjes med indtil det halve, når nogen af de i kapitlerne 25 (legemskrænkelser), 26 (frihedskrænkelser) og 27 (freds- og ærekrænkelser) omhandlede forbrydelser begås mod et fremmed statsoverhoved eller lederen af en fremmed diplomatisk mission. Med den foreslåede ændring undtages forbrydelser omfattet af straffelovens kapitel 13 fra bestemmelsens anvendelsesområde. Ændringen skal ses i sammenhæng med de nye bestemmelser i kapitel 13 om terrorisme mv., der fastsætter forhøjede strafmaksima for en række af de forbrydelser, der indgår i § 110 d. Hvor en forbrydelse er omfattet af såvel § 110 d som en bestemmelse i kapitel 13, f.eks. den foreslåede bestemmelse i § 114 a, nr. 2, indebærer ændringen, at strafforhøjelse sker efter § 114 a uden samtidig anvendelse af § 110 d.

Til nr. 2 (Overskriften til 13. kapitel)

Der foreslås en ny overskrift til kapitel 13, der er mere dækkende for kapitlets indhold efter indføjelsen af bestemmelserne om terrorhandlinger mv.

Til nr. 3 (straffelovens § 114, stk. 1, nr. 8)

Med den foreslåede bestemmelse i § 114, stk. 1, nr. 8, udvides den særlige terrorismebestemmelse i straffelovens § 114 med besiddelse og anvendelse mv. af radioaktive stoffer efter § 192 b, sml. lovforslagets § 1, nr. 7, med tilhørende bemærkninger.

Til nr. 4 (straffelovens §§ 114 a-114 e)

Til § 114 a

Forslaget til en ny § 114 a omfatter handlinger, der efter Europarådskonventionen skal anses som terrorhandlinger, og som ikke allerede er omfattet af § 114.

Det foreslås, at straffen kan overstige den højeste for lovovertrædelsen foreskrevne straf med indtil det halve, når handlingen er omfattet af vedkommende artikel i en af de opregnede konventioner. Hvis den højeste straf, der er foreskrevet for den pågældende handling, er mindre end 4 års fængsel, kan straffen dog stige til fængsel indtil 6 år. Med den sidstnævnte bestemmelse sigtes til forbrydelser, der har strafmaksima på under 4 års fængsel, f.eks. straffelovens § 260 om ulovlig tvang og § 266 om trusler. Den foreslåede bestemmelse er subsidiær i forhold til § 114.

Med § 114 a tilsigtes ingen nykriminalisering. Formålet med bestemmelsen er derimod at indføje en sidestrafferamme med mulighed for strafforhøjelse, når overtrædelse af visse bestemmelser i straffeloven er begået under omstændigheder omfattet af de berørte artikler i de nævnte internationale konventioner, f.eks. § 114 a, nr. 4, sammenholdt med straffelovens § 276, jf. § 285, stk. 1, eller § 286.

§ 192 b, stk. 2, nr. 2, vedrører fjernelse, ændring eller beskadigelse af en nødvendig beskyttelse mod spredning af radioaktive stoffer eller mod ioniserende stråling. Hermed sigtes til tilfælde, hvor en nødvendig indkapsling af et radioaktivt stof eller afskærmning af en anordning, der kan udsende ioniserende stråling, fjernes, eksempelvis hvor afskærmningen ved et røntgenanlæg beskadiges, så strålingen rammer forbipasserende. Bestemmelsen kræver, at beskyttelsen mod spredning af radioaktive stoffer eller mod ioniserende stråling er nødvendig, f.eks. fordi de radioaktive stoffer eller den ioniserende stråling uden beskyttelsen vil gøre skade på personer, ting eller miljø på kortere eller længere sigt.

§ 192 b, stk. 2, nr. 3, retter sig mod anvendelse eller beskadigelse af et nukleart anlæg med den følge, at der sker udslip af radioaktive stoffer eller fremkaldes fare derfor. Bestemmelsen kan f.eks. finde anvendelse i tilfælde, hvor et atomkraftværk beskadiges på en sådan måde, at der sker udslip af radioaktive stoffer, eller hvor der fremkaldes fare herfor.

Forbrydelsen i § 192 b fuldbyrdes ved henholdsvis besiddelsen mv. og anvendelsen mv. af de omhandlede radioaktive stoffer og anordninger m.fl.

Subjektivt kræves efter § 192, stk. 1, at besiddelsen mv. sker med forsæt til skade på andres person eller til betydelig skade på andres ting eller på miljøet. Foruden forsæt til besiddelsen mv. kræves således forsæt til, at det stof eller den anordning, der besiddes mv., skal anvendes til at forvolde skade. Det forudsættes, at bestemmelsen alene finder anvendelse i tilfælde, hvor der er forsæt til strålingsskader, men derimod ikke i tilfælde, hvor en sådan anordning anvendes til f.eks. almindelig vold. Det er for så vidt angår andres person tilstrækkeligt, at der foreligger forsæt til skade. Der kræves således ikke, at der foreligger forsæt til at forårsage f.eks. død eller alvorlig personskade. For så vidt angår tings- og miljøskade kræves forsæt til, at skaden er betydelig. Der skal således være tale om forsæt til skade af et vist omfang, når det drejer sig om skade på andres ting eller skade på miljøet. Skade kan efter omstændighederne f.eks. bestå i, at celler i den menneskelige organisme udsættes for skadelig påvirkning, der indebærer risiko for senere udvikling af cancer eller genskader, der først kan spores mange år efter hændelsen.

Efter § 192, stk. 2, kræves, at anvendelsen mv. sker med forsæt til skade som nævnt i stk. 1 eller til at tvinge nogen til at foretage eller undlade at foretage en handling, f.eks. udbetaling af penge eller fremskaffelse af fortrolige oplysninger.

§ 192, stk. 3, 1. led, er affattet på samme måde som den gældende straffelovs § 183, stk. 2, om forvoldelse af sprængning og spredning af skadevoldende luftarter mv. under de i § 180 angivne omstændigheder.

Der kræves alene uagtsomhed, jf. straffelovens § 20, med hensyn til den følge, der består i radioaktivt udslip eller fare herfor i § 192 b, stk. 2, nr. 3, eller omfattende miljøskade eller nærliggende fare herfor i § 192 b, stk. 3, 2. led. Bestemmelsen svarer på dette punkt til den gældende straffelovs § 196.

Til § 2

Retsplejeloven

Til nr. 1 (retsplejelovens § 110 a)

Formålet med bestemmelsen i *stk. 1* er at skabe grundlag for, at Politiets Efterretningstjeneste kan videregive oplysninger til Forsvarets Efterretningstjeneste, uden at der i hvert enkelt tilfælde skal foretages en nærmere konkret vurdering i forhold til den enkelte oplysning.

Bestemmelsen omfatter både ikke-fortrolige og fortrolige oplysninger, herunder oplysninger om enkeltpersoners rent private forhold.

Videregivelse af oplysninger efter bestemmelsen i stk. 1 kan ske på den betingelse, at oplysningerne kan have betydning for varetagelse af *Forsvarets Efterretningstjenestes opgaver* eller *Politiets Efterretningstjenestes opgaver*. Der henvises herom til pkt. 3.4.2.2. ovenfor.

Med bestemmelsen i *stk. 2* etableres et særligt lovgrundlag for Politiets Efterretningstjenestes indhentelse af oplysninger fra andre forvaltningsmyndigheder.

På samme måde som bestemmelsen i stk. 1 omfatter stk. 2 både ikke-fortrolige og fortrolige oplysninger.

Oplysningerne vil kunne indhentes fra andre forvaltningsmyndigheder. Dette omfatter de myndigheder og institutioner, der er omfattet af det almindelige anvendelsesområde for forvaltningsloven og lov om offentlighed i forvaltningen. Det vil sige, at der kan indhentes oplysninger fra andre forvaltningsmyndigheder, hvad enten de hører under den statslige, kommunale eller (fremtidige) regionale forvaltning, og uanset om der er tale om almindelige forvaltningsmyndigheder, særlige nævn eller råd eller særlige forvaltningsmyndigheder. Det bemærkes, at Politiets Efterretningstjenestes adgang til at indhente oplysninger fra Forsvarets Efterretningstjeneste ikke reguleres af § 110 a, stk. 2, men derimod af den bestemmelse, der ved det lovforslag, som forsvarsministeren samtidig har fremsat, foreslås indsat i forsvarsloven.

Det er en betingelse for, at Politiets Efterretningstjeneste kan indhente oplysninger, at oplysningerne må antages at have betydning for Politiets Efterretningstjenestes opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13. I betingelsen om, at oplysningerne "må antages at have betydning", ligger, at der skal være en mere konkret formodning for, at de oplysninger, som Politiets Efterretningstjeneste ønsker at indhente fra en anden forvaltningsmyndighed, vil have betydning for varetagelsen af de nævnte opgaver. Der henvises til pkt. 3.4.2.3. ovenfor.

Det vil være Politiets Efterretningstjeneste, der i forbindelse med indhentelsen af oplysningerne skal vurdere, om betingelsen i § 110 a, stk. 2, er opfyldt. Lovforslaget bygger således på, at den forvaltningsmyndighed, der på grundlag af den foreslåede bestemmelse modtager en anmodning om oplysninger fra Politiets Efterretningstjeneste, vil kunne lægge til grund, at de pågældende oplysninger må antages at have betydning for varetagelse af Politiets Efterretningstjenestes opgaver vedrørende forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.

Det bemærkes dog, at en forvaltningsmyndighed bør rette henvendelse til Politiets Efterretningstjeneste, hvis den pågældende myndighed er i tvivl om, hvilke nærmere oplysninger tjenesten har brug for, jf. herved princippet i forvaltningslovens § 32, hvorefter den, der virker inden for den offentlige forvaltning, ikke må skaffe sig fortrolige oplysninger, som ikke er af betydning for udførelsen den pågældendes opgaver.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger, pkt. 3.3.

Til nr. 2 (overskriften til retsplejelovens kapitel 71)

Ændringen af overskriften til kapitel 71 er en konsekvens af den foreslåede nye regel i § 791 c om forstyrrelse eller afbrydelse af radio- eller telekommunikation, jf. forslagets § 2, nr. 8.

Til nr. 3 (retsplejelovens § 783, stk. 1)

Der er tale om en tilføjelse af redaktionel karakter, som har sammenhæng med forslaget i lovforslagets § 2, nr. 4, jf. nedenfor.

Til nr. 4 (retsplejelovens § 783, stk. 2)

Med forslaget indsættes der i retsplejelovens § 783 et nyt stk. 2, hvorefter retten ved kendelse om telefonaflytning eller teleoplysning i forbindelse med efterforskning af en overtrædelse af straffelovens kapitel 12 eller 13 i stedet for bestemte telefonnumre kan anføre den person, som indgrebet angår (den mistænkte person), jf. § 783, stk. 1, 2. pkt. Den foreslåede bestemmelse omfatter således alle de indgreb i meddelelseshemmeligheden, der er omfattet af retsplejelovens § 780, stk. 1, nr. 1 og 3, uanset om der er tale om egentlig telefonkommunikation eller anden tilsvarende telekommunikation, f.eks. e-mail-, internet- eller telefaxkommunikation. Den foreslåede bestemmelse omfatter alene fremadrettet teleoplysning i medfør af retsplejelovens § 780, stk. 1, nr. 3, og ikke bagudrettet teleoplysning i medfør af editionsreglerne.

For at retten kan udstede en kendelse på personen i medfør af den foreslåede affattelse af retsplejelovens § 783, stk. 2, 1. pkt., skal de sædvanlige betingelser for telefonaflytning eller teleoplysning være opfyldt, herunder navnlig kravet i § 781, stk. 1, nr. 1, om, at der skal være bestemte grunde til at antage, at der på den pågældende måde gives meddelelser til eller fra den mistænkte. Det samme gælder f.eks. indikationskravet i § 781, stk. 1, nr. 2, proportionalitetskravet i § 782, stk. 1, og kravet om, at der i kendelsen skal fastsættes det tidsrum, inden for hvilket indgrebet må foretages, jf. § 783, stk. 2, (der efter forslaget bliver § 783, stk. 3).

Den foreslåede bestemmelse i retsplejelovens § 783, stk. 2, vil således alene forenkle den formelle procedure, så politiet kun behøver at indhente én forudgående retskendelse. En retskendelse om telefonaflytning af personen vil give mulighed for at aflytte den mistænkte person, uanset hvilke telekommunikationsmidler den pågældende måtte vælge at benytte sig af. Med hjemmel i en sådan forudgående retskendelse vil politiet løbende kunne iværksætte aflytning af alle de telefonnumre, der er bestemte grunde til at antage bliver benyttet af en person, som er mistænkt for overtrædelse af straffelovens kapitel 12 eller 13. Tilsvarende vil en retskendelse om teleoplysning på personen give mulighed for løbende at indhente oplysninger om, hvilke telefonnumre der sættes i forbindelse med de telefoner, som der er bestemte grunde til at antage benyttes til at give meddelelser til eller fra den mistænkte.

I medfør af den foreslåede affattelse af § 783, stk. 2, 2. pkt., skal politiet snarest muligt efter udløbet af det tidsrum, inden for hvilket indgrebet kan foretages, underrette retten om de telefonnumre, som er blevet aflyttet, eller hvor der har været iværksat teleoplysning, samt om de bestemte grunde, der er til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte person.

Politiets underretning til retten sker med henblik på, at retten herefter underretter den advokat, som er beskikket i sagen i medfør af retsplejelovens § 784, stk. 1, jf. den foreslåede bestemmelse i § 783, stk. 2, 3. pkt. Underretningen skal gøre det muligt for den beskikkede advokat at tage stilling til, om spørgsmålet om lovligheden af indgrebet skal indbringes for retten.

Spørgsmålet om lovligheden af indgrebet kan således indbringes for retten i medfør af den foreslåede bestemmelse i § 783, stk. 2, 3. pkt. Formålet med denne bestemmelse er at sikre en adgang til kontrol ved domstolene med hensyn til de konkrete telefonnumre, som politiet har aflyttet eller foretaget teleoplysning på efter en retskendelse på personen. Hvis sagen indbringes for retten af den beskikkede advokat, afgør retten ved kendelse, om indgrebet er sket inden for rammerne af den forudgående retskendelse på personen og i øvrigt i overensstemmelse med retsplejelovens almindelige betingelser for telefonaflytning og teleoplysning, jf. bl.a. § 781, stk. 1, nr. 1.

Finder retten i den forbindelse, at der er foretaget et indgreb, som ikke burde være foretaget, skal retten give meddelelse herom til Justitsministeriet, jf. den foreslåede bestemmelse i § 783, stk. 2, 5. pkt.

Der henvises i øvrigt til pkt. 4.2. i de almindelige bemærkninger til lovforslaget.

Til nr. 5 (retsplejelovens § 788, stk. 4)

Det foreslås, at retsplejelovens § 788, stk. 4, ændres, så det kommer til at fremgå udtrykkeligt, at hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder taler imod underretning, kan retten efter begæring fra politiet beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum, der kan forlænges.

Det forudsættes i den forbindelse, at udtrykket »fortrolige oplysninger om politiets efterforskningsmetoder« har samme anvendelsesområde som den tilsvarende formulering i retsplejelovens § 729 c, stk. 1, nr. 6.

Der henvises i øvrigt til pkt. 4.3. i de almindelige bemærkninger til lovforslaget.

Til nr. 6 (retsplejelovens § 791 a, stk. 5 og 6)

Bestemmelsen indeholder en udtrykkelig hjemmel for politiet til under nærmere angivne betingelser at foretage teleobservation. Ved teleobservation forstås indhentelse af oplysninger, der gør det muligt løbende at stedfæste en tændt mobiltelefon. Det vil navnlig dreje sig om oplysninger om, hvilke mobiltelefonmaster den pågældende mobiltelefon er i forbindelse med ved opdateringer, hvilken celle der er anvendt ved opdateringen, samt – ved mobiltelefonens anvendelse til kommunikation – oplysninger om i hvilken afstand fra masten mobiltelefonen befinder sig.

Teleobservation kan foretages, hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og hvis efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.

Anvendelse af teleobservation vil endvidere kun kunne foretages, hvis dette vil være foreneligt med almindelige principper om proportionalitet. Bestemmelsen i § 791 a, stk. 5, (der efter forslaget bliver stk. 7), hvorefter et indgreb ikke må foretages, hvis det – efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den person, som det rammer – vil være uforholdsmæssigt, vil således finde tilsvarende anvendelse ved teleobservation.

Der henvises i øvrigt til pkt. 5.3. i de almindelige bemærkninger.

Den foreslåede § 791 a, stk. 6, indebærer en forpligtelse for udbydere af telenet eller teletjenester til at bistå politiet ved gennemførelse af teleobservation, herunder ved udlevering af de oplysninger, der er omfattet af den foreslåede nye bestemmelse i § 791 a, stk. 5.

Der henvises i øvrigt til pkt. 5.3. i de almindelige bemærkninger.

Til nr. 7 (retsplejelovens § 791 a, stk. 8, 2. pkt.)

Den foreslåede tilføjelse indebærer, at visse nærmere opregnede bestemmelser vedrørende indgreb i meddelelseshemmeligheden finder tilsvarende anvendelse ved indgreb efter den foreslåede bestemmelse i § 791 a, stk. 5, om teleobservation.

Teleobservation kan således som udgangspunkt alene iværksættes efter rettens forudgående kendelse. I kendelsen skal bl.a. angives det mobiltelefonnummer eller anden identifikation, f.eks. IMEI- eller IMSI-nummer, som indgrebet angår, samt det tidsrum, inden for hvilket indgrebet kan foretages, jf. henvisningen til retsplejelovens § 783. I tilfælde, hvor kendelsen indhentes med henblik på efterforskning af en overtrædelse af straffelovens kapitel 12 eller 13, vil der i kraft af den foreslåede nye bestemmelse i retsplejelovens § 783, stk. 2, jf. lovforslagets § 2, nr. 4, i stedet kunne anføres den person, som indgrebet angår.

Hvis øjemedet ville forspildes, hvis rettens kendelse skulle afventes, kan politiet træffe beslutning om teleobservation. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten, jf. § 783, stk. 3.

Endvidere er visse øvrige bestemmelser om indgreb i meddelelseshemmeligheden gjort tilsvarende anvendelige ved teleobservation, herunder bestemmelserne om advokatbeskikkelse, jf. § 784 og § 785, om underretning ved indgrebets ophør, jf. § 788, og § 791, der omhandler politiets efterfølgende tilintetgørelse af materiale, der er kommet til politiets kendskab i forbindelse med indgrebet.

Der henvises i øvrigt til pkt. 5.3. i de almindelige bemærkninger.

Til nr. 8 (retsplejelovens § 791 b, stk. 3)

Der er tale om en redaktionel ændring som konsekvens af lovforslagets § 2, nr. 4.

Til nr. 9 (retsplejelovens § 791 c)

Bestemmelsen indebærer, at politiet under nærmere angivne betingelser kan forstyrre eller afbryde radio- eller telekommunikation.

Det foreslås i *stk. 1* som betingelse for forstyrrelse eller afbrydelse af radio- eller telekommunikation i et område, at der er afgørende grunde til det med henblik på at forebygge, at der i det pågældende område vil blive begået en lovovertrædelse, der efter loven kan straffes med fængsel i 6 år eller derover, eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, og som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.

Det er således en betingelse for at iværksætte forstyrrelse eller afbrydelse af radio- eller telekommunikation efter den foreslåede bestemmelse, at der er afgørende grunde til det med henblik på at forebygge f.eks. terrorhandlinger. Dette indebærer, at der skal være en markant øget risiko for, at der i det pågældende område vil blive begået f.eks. en terrorhandling. Det vil afhænge af en konkret, samlet vurdering, om der foreligger en markant øget risiko. Dette kan f.eks. være tilfældet, hvor der foreligger konkrete oplysninger om, at et terrorangreb er nært forestående i et bestemt område.

Endvidere vil bestemmelsen i helt særlige tilfælde kunne anvendes, hvor der ikke foreligger sådanne konkrete oplysninger, men hvor der er tale om en begivenhed, som efter en generel vurdering kan indebære en markant øget risiko for f.eks. terrorangreb. Der kan bl.a. være tale om besøg af særligt udsatte udenlandske statsoverhoveder mv., som f.eks. skal optræde offentligt i forbindelse med taler til offentligheden, og hvor politiet finder, at den fornødne beskyttelse alene kan etableres ved midlertidigt at afbryde radio- eller telekommunikationen i et område.

Den foreslåede bestemmelse tager navnlig sigte på at forebygge terror, men bestemmelsen er ikke begrænset hertil. Når betingelserne for at iværksætte indgrebet i øvrigt er opfyldt, kan politiet forstyrre eller afbryde radio- eller telekommunikation i et område med henblik på at forebygge anden alvorlig kriminalitet. Det kan f.eks. være retsstridige forstyrrelser i driften af almindelige samfærdselsmidler mv. eller gidsels- og kidnapningssituationer.

Det er endvidere en betingelse for indgrebet, at lovovertrædelsen kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Adgangen til at foretage indgreb i form af forstyrrelse eller afbrydelse af radio- eller telekommunikation vil således være begrænset til helt særlige situationer.

Stk. 2 indeholder en almindelig proportionalitetsregel.

Efter *stk. 3, 1. pkt.*, skal kompetencen til at træffe bestemmelse om forstyrrelse eller afbrydelse af radio- eller telekommunikation henhøre under retten.

I en kendelse, der tillader forstyrrelse eller afbrydelse af radio- eller telekommunikation, skal det angives, hvilket område indgrebet angår, jf. den foreslåede bestemmelse i stk. 3, 2. pkt. Den nærmere afgrænsning af området vil bero på en konkret vurdering i det enkelte tilfælde, og området for den konkrete forstyrrelse eller afbrydelse af radio- eller telekommunikation må fastlægges på baggrund af de forhold, som begrunder vurderingen af, at der f.eks. er en markant øget risiko for et terrorangreb i det pågældende område. Udstrækningen af det pågældende område skal – i overensstemmelse med almindelige principper om proportionalitet – være så begrænset som muligt. Udstrækningen heraf må også konkret ses i lyset af de tekniske forhold, herunder frekvens, sendeeffekt og antenneforhold. Medmindre helt særlige omstændigheder gør sig gældende, vil der ikke være grundlag for at forstyrre eller afbryde radio- eller telekommunikation udover et område med en radius af nogle hundrede meter.

Endvidere skal det i kendelsen anføres, hvilke konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt, jf. den foreslåede bestemmelse i stk. 3, 2. pkt.

I kendelsen skal endvidere fastsættes det tidsrum, inden for hvilket indgrebet kan foretages, jf. stk. 3, 4. pkt. Tidsrummet skal – i overensstemmelse med almindelige principper om proportionalitet – være så kort som muligt. Medmindre helt særlige omstændigheder gør sig gældende, vil der ikke være grundlag for at fastsætte et længere tidsrum end nogle timer. Tidsrummet kan forlænges ved en ny kendelse.

Efter *stk. 4* kan politiet træffe en foreløbig beslutning om at foretage forstyrrelse eller afbrydelse af radio- eller telekommunikation, hvis indgrebets øjemed ville forspildes ved at afvente en retskendelse (på øjemedet). Dette kan f.eks. være relevant, hvor politiet har behov for øjeblikkelig at forstyrre eller afbryde radio- eller telekommunikation i et område. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes, samt om det kan opretholdes, og i bekræftende fald for hvilket tidsrum. Burde indgrebet efter rettens opfattelse ikke have været foretaget, skal retten give meddelelse herom til Justitsministeriet.

Efter *stk. 5* finder reglerne i §§ 784 og 785 om advokatbeskikkelse tilsvarende anvendelse ved indgreb i form af forstyrrelse eller afbrydelse af radio- eller telekommunikation.

Efter retsplejelovens § 784, stk. 1, 2. pkt., skal der beskikkes en advokat fra den særlige kreds af advokater, som er nævnt i stk. 2, hvis efterforskningen angår en overtrædelse af straffelovens kapitel 12 eller 13. Denne bestemmelse finder tilsvarende anvendelse ved indgreb i form af forstyrrelse eller afbrydelse af radio- eller telekommunikation. Det indebærer, at der også ved forstyrrelse eller afbrydelse af radio- eller telekommunikation med henblik på at forebygge terrorhandlinger skal beskikkes en advokat fra den særlige kreds af advokater.

Der henvises i øvrigt til pkt. 6.3. i de almindelige bemærkninger.

Til § 3

Lov om forbud mod tv-overvågning m.v.

Til nr. 1 (§§ 4 a og 4 b)

Til § 4 a

Bestemmelsen er ny og indebærer en udtrykkelig adgang for politimesteren til at henstille, at offentlige myndigheder eller private foretager tv-overvågning, som de efter gældende lovgivning har mulighed for at foretage.

Bestemmelsen udvider ikke adgangen til at foretage tv-overvågning. En henstilling kan således alene gives inden for rammerne af gældende lovgivning, navnlig tv-overvågningsloven, persondataloven og retsplejeloven.

En henstilling om at iværksætte tv-overvågning forudsættes navnlig anvendt, hvor tv-overvågning vurderes at kunne være af betydning for politiets muligheder for at forebygge og efterforske eventuelle terrorangreb.

Politiets henstilling er ikke bindende for modtageren, men det forudsættes, at offentlige myndigheder i almindelighed efterkommer henstillingen, medmindre der foreligger helt særlige forhold.

Kompetencen til at henstille, at der foretages tv-overvågning, ligger hos politimesteren.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger, pkt. 7.3.

Til § 4 b

Bestemmelsen er ny og indebærer en adgang for politimesteren til at meddele pålæg til offentlige myndigheder og private, som foretager eller planlægger at iværksætte tv-overvågning efter gældende lovgivning, med hensyn til kvaliteten af optagelser af billeder på videobånd, film eller lignende samt med hensyn til opbevaringen af sådanne optagelser.

Pålægget kan for det første indeholde tekniske specifikationer, som optagelserne skal overholde med henblik på at sikre, at optagelserne er af en sådan kvalitet, at de vil kunne anvendes ved en senere efterforskning.

Bestemmelsen giver derimod ikke mulighed for at pålægge en offentlig myndighed eller en privat f.eks. at opsætte et ekstra kamera med henblik på at dække et bestemt område bedre. Hvis politimesteren finder, at dette vil være af betydning for bekæmpelsen af terrorisme, vil politimesteren i et sådant tilfælde i stedet kunne *henstille* , at det pågældende kamera opsættes, jf. den foreslåede bestemmelse i § 4 a.

Pålægget kan for det andet indeholde krav vedrørende opbevaringen af optagelserne. Der kan både være tale om krav til, hvordan opbevaring skal ske med henblik på at sikre, at optagelserne bevarer deres kvalitet, og krav til, hvor længe optagelserne skal opbevares.

I alle tilfælde kan der alene gives pålæg inden for rammerne af de betingelser for at foretage tv-overvågning, som er fastsat i gældende lovgivning, navnlig tv-overvågningsloven, persondataloven og retsplejeloven. Politimesteren kan således ikke med et pålæg efter den foreslåede bestemmelse udvide området for, hvor eller hvordan der kan foretages tv-overvågning, eller hvor længe optagelserne må opbevares.

Der henvises i øvrigt til pkt. 7.3. i lovforslagets almindelige bemærkninger.

Til nr. 2 (§ 5, stk. 2)

Bestemmelsen er ny og har til formål at give mulighed for bødestraf, hvis et pålæg meddelt i medfør af § 4 b ikke efterkommes.

Såvel offentlige myndigheder som private vil kunne ifalde strafansvar efter den foreslåede bestemmelse.

Til § 4

Lov om luftfart

Til nr. 1 (luftfartslovens § 148 a)

Der foreslås indsat et nyt *kapitel 12 a* i luftfartsloven med en bestemmelse om passageroplysninger. Den foreslåede bestemmelse medfører en forpligtelse for luftfartsselskaber til at registrere, opbevare og udlevere passageroplysninger til Politiets Efterretningstjeneste. Bestemmelsen omfatter luftfartsselskaber, der udfører erhvervsmæssig befordring af passagerer, og omfatter både udenrigs- og indenrigsflyvninger.

Efter *stk. 1* skal luftfartsselskaber foretage registrering og opbevaring i 1 år af oplysninger om passagerer og besætningsmedlemmer på luftfartøjer, der ankommer til eller afgår fra Danmark.

I medfør af *stk. 2* skal luftfartsselskaber endvidere på begæring af Politiets Efterretningstjeneste udlevere de i stk. 1 nævnte oplysninger til brug for forebyggelse og efterforskning overtrædelser af straffelovens kapitel 12 og 13. Efter denne bestemmelse har tjenesten adgang til luftfartsselskabernes aktuelle og historiske passageroplysninger, uden at der foreligger retskendelse eller beslutning om edition. Bestemmelsen giver ligeledes tjenesten mulighed for løbende at indhente passagerlister på udvalgte ruter, der er særligt relevante i terrorsammenhæng. Det forudsættes, at luftfartsselskaberne udleverer oplysningerne hurtigst muligt og uden ugrundet ophold.

Det følger af *stk. 3* , at transport- og energiministeren efter forhandling med justitsministeren fastsætter nærmere regler om registrering og opbevaring af passageroplysninger samt om luftfartsselskabernes praktiske bistand til politiet. Det forudsættes således bl.a., at der fastsættes nærmere regler om, hvilke typer oplysninger der omfattes af luftfartsselskabernes forpligtelse til at registrere, opbevare og udlevere passageroplysninger, jf. stk. 1 og stk. 2.

I medfør af *stk. 4* kan transport- og energiministeren endvidere efter forhandling med justitsministeren fastsætte nærmere regler om Politiets Efterretningstjenestes adgang til luftfartsselskabernes bookingsystemer til brug for forebyggelse og efterforskning af overtrædelser af straffelovens kapitel 12 og 13.

Der henvises til pkt. 8.3. i de almindelige bemærkninger til lovforslaget.

Til nr. 2 (luftfartslovens § 149, stk. 5)

Ændringen indebærer, at overtrædelse af de foreslåede bestemmelser i luftfartslovens § 148 a, stk. 1 og 2, jf. lovforslagets § 4, nr. 1, omfattes af straffebestemmelsen i luftfartslovens § 149, stk. 5. Overtrædelse af luftfartslovens § 148 a, stk. 1 og 2, vil herefter kunne straffes med bøde.

Det bemærkes, at det følger af luftfartslovens § 149, stk. 10, at det i de forskrifter, der fastsættes i medfør af loven, kan bestemmes, at overtrædelser af forskrifterne medfører straf af bøde eller fængsel indtil 4 måneder. I medfør af denne bestemmelse kan der ligeledes fastsættes straffebestemmelser i de forskrifter, der udstedes med hjemmel i de foreslåede bestemmelser i luftfartslovens § 148 a, stk. 3 og 4, jf. lovforslagets § 4, nr. 1.

Til § 5

Til nr. 1 (udleveringslovens § 5, stk. 3)

Efter udleveringslovens § 5, stk. 3, finder forbudet mod at nægte udlevering for politiske lovovertrædelser mv. ikke anvendelse, når handlingen er omfattet af artikel 1 eller 2 i den europæiske konvention om bekæmpelse af terrorisme som ændret ved ændringsprotokol af 15. maj 2003 til den europæiske konvention om bekæmpelse af terrorisme, artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af terrorbombninger eller artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af finansiering af terrorisme.

Med den foreslåede bestemmelse udvides denne undtagelse til også at omfatte handlinger omfattet af artikel 6 og 7 og artikel 9, jf. artikel 6 og 7, i Europarådets konvention om forebyggelse af terrorisme og artikel 2, jf. artikel 1, i FN-konventionen til bekæmpelse af nuklear terrorisme.

Der tilsigtes ikke i øvrigt ændringer i anvendelsesområdet for § 5, stk. 3. Der henvises til bemærkningerne til lov nr. 378 af 6. juni 2002, jf. Folketingstidende 2001-02, side 885, samt til pkt. 9 i de almindelige bemærkninger.

Til nr. 2 (udleveringslovens § 5, stk. 4)

Bestemmelsen er ny. Bestemmelsen tilsigter at tydeliggøre, at der i medfør af Europarådets konvention om forebyggelse af terrorisme ikke består en ubetinget pligt til udlevering for en politisk forbrydelse, når handlingen er omfattet af konventionens artikel 5 eller artikel 9, jf. artikel 5, sådan som det er tilfældet, hvis handlingen er omfattet af konventionens artikel 6 eller 7 eller artikel 9, jf. artikel 6 og 7.

Bestemmelsen indebærer således, at de danske myndigheder ikke vil være afskåret fra efter en konkret vurdering at anse en overtrædelse af konventionens artikel 5 eller af artikel 9, jf. artikel 5, for en politisk lovovertrædelse, ligesom de danske myndigheder i en sådan situation ikke vil være afskåret fra at nægte udlevering med denne begrundelse.

Med formuleringen »i særlige tilfælde« sigtes til, at en offentlig opfordring til at begå en terrorhandling som udgangspunkt må antages ikke at være en politisk forbrydelse, medmindre der foreligger holdepunkter for det modsatte.

Til § 6

Til nr. 1

Bestemmelsen fastsætter, at justitsministeren i folketingsåret 2009-10 skal fremsætte forslag om revision af bestemmelsen i retsplejelovens § 786, stk. 4, om logning af trafikdata.

Der henvises til lovforslagets almindelige bemærkninger pkt. 10.2.

Til § 7

Det foreslås, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Lovens § 5 finder anvendelse på anmodninger om udlevering efter Europarådets konvention om forebyggelse af terrorisme, henholdsvis FN-konventionen til bekæmpelse af nuklear terrorisme, der fremsættes efter, at den pågældende konvention er trådt i kraft mellem Danmark og vedkommende fremmede stat.

Lovens § 1 har virkning for lovovertrædelser, der begås efter lovens ikrafttræden, jf. straffelovens § 3, stk. 1.

I *stk. 2* foreslås det dog, at tidspunktet for ikrafttræden af den foreslåede nye bestemmelse i retsplejelovens § 791 a, stk. 6, hvorefter udbydere af telenet- eller teletjenester er forpligtet til at bistå politiet ved gennemførelse af teleobservation, fastsættes af justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling. Herved sikres det, at forpligtelsen til i disse sager at bistå politiet træder i kraft samtidig med, at udbydere af telenet eller teletjenester efter et lovforslag, der fremsættes af ministeren for videnskab, teknologi og udvikling, bliver forpligtet til at indrette deres systemer således, at disse oplysninger fremadrettet kan leveres til politiet, jf. også lovforslagets almindelige bemærkninger, pkt. 5.2. Den foreslåede bestemmelse i retsplejelovens § 791 a, stk. 5, der giver hjemmel til, at politiet under nærmere angivne betingelser kan iværksætte teleobservation, træder derimod i kraft dagen efter bekendtgørelsen i Lovtidende.

Endvidere foreslås i *stk. 3* , at den foreslåede nye bestemmelse i retsplejelovens § 791 c om forstyrrelse eller afbrydelse af radio- eller telekommunikation træder i kraft den 1. juli 2006. Dette svarer til ikrafttrædelsestidspunktet for de konsekvensændringer i lov om radio- og teleterminaludstyr og elektromagnetiske forhold og lov om radiofrekvenser, der er indeholdt i lovforslaget fra ministeren for videnskab, teknologi og udvikling.

I *stk. 4* foreslås det herudover, at tidspunktet for ikrafttræden af den foreslåede bestemmelse i luftfartslovens § 148 a (luftfartsselskabers pligt til at registrere, opbevare og udlevere passageroplysninger) fastsættes af transport- og energiministeren efter forhandling med justitsministeren.

Til § 8

Bestemmelsen fastsætter lovens territoriale gyldighedsområde.

Bestemmelsen indebærer, at lovens § 1 kan sættes i kraft for Færøerne ved kongelig anordning. Da der gælder en særlig kriminallov for Grønland, er der ikke foreslået en tilsvarende hjemmel til at sætte loven i kraft for Grønland.

Endvidere kan lovens §§ 3-5 sættes i kraft for Færøerne og Grønland ved kongelig anordning.

Lov om forbud mod privates tv-overvågning er sat i kraft for Færøerne ved kgl. anordning nr. 155 af 21. marts 1988 med virkning fra den 1. april 1988. Ændringerne af loven, jf. lov nr. 1016 af 23. december 1998, lov nr. 939 af 20. december 1999 og lov nr. 257 af 8. maj 2002, er ikke sat i kraft for Færøerne. Lov om forbud mod privates tv-overvågning er ikke sat i kraft for Grønland.

Luftfartsloven gælder kun for Grønland med de af den særlige grønlandske lovgivning flydende lempelser. Ved kgl. anordning nr. 130 af 3. marts 1989 er luftfartsloven sat i kraft for Færøerne med virkning fra den 1. maj 1989.

Det bemærkes, at udleveringsloven har gyldighed for Færøerne og Grønland med de afvigelser, som følger af den færøske og grønlandske retsplejelov.

2009/1 LSF 180 (Gældende)

Forslag til Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af

Ministerium: Justitsministeriet

Journalnummer: Justitsmin., sagsnr. 2005-730-0215

Fremsat den 24. marts 2010 af justitsministeren (Lars Barfoed)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, foretages følgende ændring:

1. I *§ 8* ændres »2009-10« til: »2011-12«.

§ 2

Loven træder i kraft den 1. juli 2010.

§ 3

Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning og baggrund

1.1. Formålet med lovforslaget er at ændre revisionsklausulen vedrørende retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, således at justitsministeren fremsætter forslag om revision af bestemmelsen i folketingsåret 2011-12 frem for 2009-10.

1.2. Efter § 8 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (terrorpakke I) skulle justitsministeren i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Ved § 7 i lov nr. 542 af 8. juni 2006 om ændring af straffeloven, retsplejeloven og forskellige andre love (Styrkelse af indsatsen for at bekæmpe terrorisme m.v.) (terrorpakke II) blev revisionen udskudt til folketingsåret 2009-10. Det skyldtes, at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af bestemmelsen, idet retsplejelovens § 786, stk. 4, først blev sat i kraft den 15. september 2007. Der blev med virkning fra samme dato administrativt fastsat nærmere regler om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

1.3. Bestemmelsen i retsplejelovens § 786, stk. 4, blev indført for at sikre, at oplysninger om teletrafik er tilgængelige, når politiet til brug for en konkret efterforskning eller retsforfølgning af alvorlig kriminalitet har indhentet en retskendelse med henblik på et indgreb i meddelelseshemmeligheden.

Det fremgår således af retsplejelovens § 786, stk. 4, at det påhviler udbydere af telenet- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Det fremgår endvidere, at justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler om denne registrering og opbevaring.

Regler herom er fastsat i bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen), der trådte i kraft den 15. september 2007. Logningsbekendtgørelsen indeholder bestemmelser, der gennemfører væsentlige dele af Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet). I tilknytning til logningsbekendtgørelsen har Justitsministeriet udstedt vejledning nr. 74 af 28. september 2006 til bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

1.4. Baggrunden for indsættelsen af en revisionsbestemmelse i 2002 – og som nævnt forlænget i 2006 – var, at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse, jf. Folketingstidende 2001-02, tillæg A, s. 886.

Ved terrorpakke II blev revisionen af retsplejelovens § 786, stk. 4, udskudt til folketingsåret 2009-10, fordi bestemmelsen endnu ikke var sat i kraft, og hjemlen til at fastsætte nærmere regler om logning ikke var udnyttet, således at der ikke forelå erfaringer med anvendelse af bestemmelsen, jf. Folketingstidende 2005-06, tillæg A, s. 7216-7217.

1.5. Justitsministeriet har indhentet udtalelser fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste vedrørende de praktiske erfaringer, der på nuværende tidspunkt foreligger med hensyn til retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Disse myndigheder har oplyst, at de oplysninger om teletrafik, der registreres og opbevares i medfør af logningsbekendtgørelsen, i en lang række tilfælde har været af væsentlig eller afgørende betydning for efterforskning og retsforfølgning af alvorlige forbrydelser, herunder bl.a. i sager om drab, terror, bandekriminalitet, narkokriminalitet, hjemmerøverier og seksuelle overgreb mod børn, og at der derfor ikke bør ske ændringer af pligten til at foretage registrering og opbevaring af oplysninger om teletrafik efter retsplejelovens § 786, stk. 4.

Rigsadvokaten og Rigspolitiet har endvidere anført, at der ud fra hensynet til strafforfølgning kan være behov for at forlænge den gældende opbevaringsperiode på 1 år og behov for at registrere og opbevare flere typer af data. Rigsadvokaten har foreslået, at nærmere overvejelser herom i givet fald sker i lyset af resultatet af det igangværende arbejde i EU-regi med evaluering af det såkaldte logningsdirektiv, jf. pkt. 2.2 nedenfor. Endvidere har Rigspolitiet oplyst, at man vil følge udviklingen på området fremover med henblik på at overveje behovet for en længere opbevaringsperiode og behovet for at registrere og opbevare flere typer af data.

Evalueringen af logningsdirektivet forventes at finde sted i efteråret 2010.

I forbindelse med høringen over et udkast til dette lovforslag har flere organisationer mv., herunder tele- og internetbranchen, bl.a. anført, at revisionsbestemmelsen ikke bør ophæves på nuværende tidspunkt, og at branchens erfaringer mv. bør inddrages ved en kommende revision.

Justitsministeriet foreslår på den anførte baggrund, at revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, ikke ophæves på nuværende tidspunkt, men at revisionen af bestemmelsen udsættes til folketingsåret 2011-12, således at resultatet af den evaluering af logningsdirektivet, der forventes at finde sted i efteråret 2010, også kan indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet er endvidere enig med bl.a. Rigspolitiet i, at det vil være hensigtsmæssigt at indhente yderligere erfaring med reglerne med henblik på at vurdere behovet for eventuelle ændringer.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

2.1.1. Retsplejelovens § 786, stk. 4, blev indført ved lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007, jf. bekendtgørelse nr. 986 af 28. september 2006.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med ministeren for videnskab, teknologi og udvikling nærmere regler om denne registrering og opbevaring.

Retsplejelovens § 786, stk. 4, fastsætter en pligt for udbydere af telenet- og teletjenester til at registre og opbevare oplysninger om teletrafik. Hensigten med bestemmelsen i § 786, stk. 4, er således, at de pågældende oplysninger findes, hvis der bliver brug for dem.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgelse af kriminalitet udgør et indgreb i meddelelseshemmeligheden, og adgangen til at få udleveret oplysninger, som en udbyder har registreret og opbevaret efter bestemmelsen, reguleres derfor af reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71 samt eventuelt også reglerne i kapitel 74 om beslaglæggelse og edition.

2.1.2. Efter retsplejelovens § 786, stk. 4, skal udbydere alene registrere og opbevare oplysninger om, hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var, f.eks. i form af optagelse af en telefonsamtale.

I bemærkningerne til lovforslag nr. L 35 (2001-02) til terrorpakke I fremgår det således, at for så vidt angår *teletrafik* vil de oplysninger, som logningspligten kan omfatte, navnlig være de oplysninger, som politiet har brug for i form af teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4 (Folketingstidende 2001-02, tillæg A, s. 879). Det kan eksempelvis være det kaldende og det kaldte telefonnummer (A- og B-nummer), opkaldstidspunkter og varigheden af samtaler samt – for mobiltelefoners vedkommende – oplysninger om anvendte sendemaster/celler.

For så vidt angår *internettrafik* fremgår det af bemærkningerne til lovforslaget, at der vil kunne fastsættes regler om logning af den dynamiske (skiftende) tildeling af IP-adresser, tidspunkt for opkobling og nedkobling samt opkoblingens varighed.

Samtidig fremgår det, at der *ikke* vil kunne fastsættes regler om, at internetudbydere løbende skal foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger, idet hensigten med bestemmelsen alene er at kunne føre elektroniske spor, der findes på internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

For så vidt angår *e-mail* er det i bemærkningerne til lovforslaget forudsat, at der ikke skal ske en generel logning af indholdsdata, men alene oplysninger svarende til teleoplysninger, dvs. oplysninger om f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen imellem disse.

Det er i bemærkningerne til lovforslaget forudsat, at tele- og internetbranchen inddrages i forbindelse med regelfastsættelsen i forbindelse med udnyttelse af bemyndigelsen bl.a. for at sikre en hensigtsmæssig teknologisk udformning af reglerne, jf. Folketingstidende 2001-02, tillæg A, s. 880.

2.2. Logningsdirektivet

Den 21. februar 2006 blev Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elek-

troniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet) vedtaget.

Det fremgår af direktivets præambel, at baggrunden for direktivet bl.a. er, at det i undersøgelser er blevet påvist, og at medlemsstaterne har praktiske erfaringer for, at trafikdata og lokaliseringsdata har stor betydning i efterforskning, afsløring og retsforfølgning af strafbare handlinger, og at det derfor er nødvendigt på europæisk plan at sikre, at data, som genereres eller behandles af udbydere af elektronisk kommunikation, lagres i en vis periode.

Direktivets artikel 5 opregner de kategorier af data vedrørende telefoni, internettrafik og e-mail, som skal registreres og opbevares.

Af artikel 6 følger, at dataene skal lagres i mindst 6 måneder og højst 2 år regnet fra datoen for gennemførelsen af den omhandlede kommunikation.

Efter artikel 10 skal medlemsstaterne hvert år tilsende Kommissionen statistikker om lagring af data, der er behandlet i forbindelse med levering af offentlige elektroniske kommunikationstjenester.

Det fremgår endvidere af direktivets artikel 14, at Kommissionen senest den 15. september 2010 skal forelægge Europa-Parlamentet og Rådet en evaluering af direktivets anvendelse og dets virkning på de økonomiske aktører og forbrugerne. Evalueringen skal ske under hensynstagen til den udvikling, der er sket inden for elektronisk kommunikationsteknologi, og de statistiske oplysninger, der er tilsendt Kommissionen i medfør af artikel 10. Formålet med evalueringen er at fastslå, om det er nødvendigt at ændre direktivets bestemmelser, særligt for så vidt angår listen over data i artikel 5 og de lagringsperioder, der er fastsat i artikel 6. Resultaterne af evalueringen vil blive offentliggjort.

Fristen for medlemsstaternes gennemførelse af direktivet i national ret var den 15. september 2007, hvilket for Danmarks vedkommende skete bl.a. ved logningsbekendtgørelsen.

2.3. Logningsbekendtgørelsen og vejledningen

2.3.1. Justitsministeriet udstedte den 28. september 2006 logningsbekendtgørelsen med hjemmel i retsplejelovens § 786, stk. 4. Bekendtgørelsen, der trådte i kraft den 15. september 2007, blev ledsaget af vejledning nr. 74 af 28. september 2006, som mere detaljeret redegør for den registrerings- og opbevaringspligt, som følger af logningsbekendtgørelsen.

I overensstemmelse med, hvad der er forudsat i bemærkningerne til retsplejelovens § 786, stk. 4, jf. ovenfor afsnit 2.1, blev det nærmere indhold af de administrative regler om logning fastsat efter dialog med branchen mv. En arbejdsgruppe med deltagelse af repræsentanter for Justitsministeriet, Rigspolitiet, It- og telebranchen, boligforeningerne, Ministeriet for Videnskab, Teknologi og Udvikling samt It- og Telestyrelsen var således tæt inddraget i forbindelse med udfærdigelsen af logningsbekendtgørelsen. Arbejdsgruppen drøftede en række spørgsmål med hensyn til logningsforpligtelsen, herunder spørgsmål af mere teknisk karakter. På baggrund af drøftelserne fandt man frem til en model, som samlet set måtte anses for proportional og afbalanceret samtidig med, at den var økonomisk overkommelig for telebranchen.

I forlængelse af denne arbejdsgruppe har It- og Telestyrelsen, Justitsministeriet og Rigspolitiet etableret et mødeforum bl.a. med henblik på løbende opfølgning på implementeringen af regeringens anti-terrorpakker, herunder logningsbekendtgørelsen.

2.3.2. Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net.

Begrebet "udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere" defineres i logningsbekendtgørelsen på samme måde som i lov om konkurrence- og forbrugerforhold på telemarkedet (lovbekendtgørelse nr. 780 af 28. juni 2007), som hører under Ministeriet for Videnskab, Teknologi og Udvikling. Efter IT- og Telestyrelsens praksis er det en central betingelse for at være omfattet af udbyder-

begrebet, at de elektroniske kommunikationsnet eller -tjenester udbydes til slutbrugere på kommercielt grundlag. Ved vurderingen heraf er det afgørende, om ydelsen sælges eller markedsføres med henblik på at opnå en direkte eller indirekte fortjeneste.

2.3.3. Det fremgår af logningsbekendtgørelsens §§ 4-6, hvilke typer af oplysninger som udbyderne skal registrere. Udbyderne skal således registrere en række nærmere angivne oplysninger om:

– fastnettelefoni,
– mobiltelefoni,
– internettrafik,
– e-mail og
– internettelefoni.

Udbyderne skal bl.a. registrere oplysninger om det opkaldte og det opkaldende nummer i forbindelse med telefonsamtaler, IP-adresser i forbindelse med brug af internettet samt modtagende og afsendende e-mail-adresser i forbindelse med brug af udbyderens egne e-mail-tjenester.

Udbyderne skal derimod ikke registrere og opbevare indholdet af kommunikation, hverken i forbindelse med telefonsamtaler, brug af internettet eller brug af udbyderens e-mail-tjenester.

Efter § 9 i bekendtgørelsen skal de i medfør af §§ 4-6 registrerede oplysninger opbevares i 1 år.

2.3.4. Efter reglerne i logningsbekendtgørelsen er det kun udbydere, der på kommercielt grundlag udbyder elektroniske kommunikationsnet eller -tjenester til slutbrugere, der skal registrere og opbevare oplysninger om teletrafik. Endvidere skal udbyderne alene registrere og opbevare oplysninger om teletrafik, der genereres eller behandles i deres net.

Med henblik på at forbedre politiets mulighed for at sammenholde oplysninger om identiteten på brugere af kommunikationsmidler med oplysninger om de anvendte kommunikationsapparater har Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling nedsat en tværministeriel arbejdsgruppe, som skal overveje, hvordan oplysninger om brugere af taletidskort, internetcaféer, gratis trådløs adgang til internettet (hot spots) og internetadgang på biblioteker mv. kan registreres. Arbejdsgruppen er anmodet om at færdiggøre sit arbejde inden sommerferien 2010. Telebranchen vil blive inddraget i forbindelse med dette arbejde.

2.3.5. Logningsbekendtgørelsen gennemfører store dele af logningsdirektivet og er i vid udstrækning baseret på direktivet, og der anvendes samme terminologi i bekendtgørelsen som i direktivet. Bekendtgørelsen går dog på en række punkter videre end direktivet. Det drejer sig bl.a. om logning af visse oplysninger om hot spots og for så vidt angår mobiltelefoner – logning af oplysninger om den første og sidste mast, som en mobiltelefon er forbundet med som led i kommunikationen.

3. De praktiske erfaringer med retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen

3.1. Som anført i pkt. 1.5 ovenfor har Justitsministeriet til brug for evalueringen af retsplejelovens § 786, stk. 4, indhentet udtalelser fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste om de praktiske erfaringer med bestemmelsen i retsplejelovens § 786, stk. 4, og reglerne fastsat i medfør heraf.

3.2. Rigsadvokaten har på baggrund af udtalelser fra politikredsene og statsadvokaturerne oplyst, at oplysninger om teletrafik, som registreres og opbevares efter bestemmelsen i retsplejelovens § 786, stk. 4, i en række tilfælde har haft væsentlig og i nogle tilfælde afgørende betydning for såvel efterforskning som retsforfølgning i alvorlige straffesager. Det drejer sig bl.a. om sager vedrørende terror, organiseret kriminalitet, drab, hjemmerøverier og grov økonomisk kriminalitet.

Rigsadvokaten har endvidere oplyst, at oplysninger om teletrafik i form af f.eks. teleoplysninger, masteoplysninger og oplysninger om internettrafik bl.a. bidrager til identifikation af mistænkte samt til belysning af kontakt mellem disse indbyrdes eller med den forurettede eller andre personer, der er relevante for sagen. Herudover kan historiske masteoplysninger bidrage til at fastlægge de mistænktes færden f.eks.

i tidsrummet omkring gerningstidspunktet, ligesom oplysninger om internettrafik kan belyse de pågældendes interesse for f.eks. ekstremistiske eller børnepornografiske hjemmesider på internettet. Alle disse oplysninger kan være af særdeles stor betydning for såvel efterforskningen som bevisførelsen i en straffesag.

Det er på den anførte baggrund Rigsadvokatens opfattelse, at oplysninger om teletrafik i dag må anses for en vigtig og til tider afgørende del af efterforskningen og bevisførelsen i alvorlige straffesager. Efter Rigsadvokatens opfattelse bør det derfor også fremover påhvile udbydere af telenet eller teletjenester at foretage registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. retsplejelovens § 786, stk. 4.

Rigsadvokaten har samtidig peget på, at det med hensyn til den periode, hvori de pågældende oplysninger skal opbevares, i visse af udtalelserne er anført, at der er eksempler på sager, hvor det ikke har været muligt at indhente oplysninger om teletrafik til brug for efterforskningen i alvorlige straffesager, idet oplysningerne var blevet slettet efter opbevaringsperiodens udløb på 1 år. Rigsadvokaten har i den forbindelse bemærket, at en forlængelse af opbevaringsperioden antagelig i visse tilfælde ville kunne bidrage til opklaring og domfældelse i straffesager, hvor der efter de gældende regler ikke foreligger oplysninger om teletrafik.

Rigsadvokaten har endvidere anført, at der som led i vurderingen af eventuelt at forlænge den gældende opbevaringsperiode på 1 år bør ske en samlet afvejning af på den ene side hensynet til strafforfølgningen og på den anden side hensynet til privatlivets fred hos abonnenter og brugere af teletjenester og telenet. Rigsadvokaten har derfor foreslået, at de nærmere overvejelser herom i givet fald vil kunne ske i lyset af resultatet af det igangværende arbejde i EU-regi vedrørende evaluering af logningsdirektivet, hvor det bl.a. skal overvejes, om der er behov for at ændre direktivets artikel 6 om opbevaringsperioder, jf. pkt. 2.2 ovenfor.

3.3. Rigspolitiet har oplyst, at oplysninger om teletrafik, der registreres og opbevares i medfør af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen generelt er af væsentlig betydning for politiets opklaring af alvorlige forbrydelser. Flere politikredse har således anvendt oplysninger, som teleselskaberne har registreret og opbevaret i medfør af logningsbekendtgørelsen, i forbindelse med efterforskning og opklaring af sager vedrørende meget alvorlige forbrydelser, herunder sager vedrørende drab, narkotikakriminalitet, røveri mv.

Rigspolitiet har desuden oplyst, at oplysningerne navnlig kan være af afgørende betydning for politiets arbejde i forhold til at kortlægge eventuelle gerningsmænds færden samt kontakt til sagens øvrige personer. Som eksempel nævnes, at oplysninger om teletrafik bl.a. i forbindelse med konflikterne på rocker- og bandeområdet har været anvendt til at underbygge mistanken mod konkrete personer, ligesom oplysningerne undertiden har kunnet benyttes til at udelukke en mistanke mod konkrete personer, idet det har kunnet konstateres, at de pågældende har befundet sig et andet sted end gerningsstedet på gerningstidspunktet.

Rigspolitiet har endvidere oplyst, at Nationalt IT-efterforskningscenter (NITEC) tillige anvender oplysninger, der registreres og opbevares i medfør af logningsbekendtgørelsen, og disse oplysninger er ofte af afgørende betydning for opklaringen af konkrete sager, herunder sager vedrørende seksuelle overgreb mod børn, grooming (internet-relaterede overgreb mod børn) og hacking.

Samlet set er det således Rigspolitiets opfattelse, at de eksisterende regler om registrering og opbevaring af oplysninger om teletrafik er af væsentlig betydning for politiets opklaring af alvorlige forbrydelser, og at der således ikke på nuværende tidspunkt er behov for ændring af reglerne om logning.

Rigspolitiet har samtidig peget på, at der navnlig ud fra efterforskningsmæssige hensyn på længere sigt vil kunne vise sig at være behov for en længere opbevaringsperiode end 1 år, ligesom der kan opstå behov

for at registrere og opbevare flere typer af data. Rigspolitiet vil derfor følge udviklingen på området fremover.

3.4. Politiets Efterretningstjeneste har oplyst, at Politiets Efterretningstjeneste anvender oplysninger om teletrafik i betydeligt omfang navnlig i forbindelse med længerevarende efterforskninger inden for terrorområdet. Oplysninger om teletrafik kan bidrage til at fastlægge, om – og i givet fald i hvilket omfang – en mistænkt person har forbindelser til andre mistænkte personer, ligesom oplysninger om teletrafik kan bidrage til at henlede efterretningstjenestens opmærksomhed på forbindelser mellem en mistænkt og personer, der ikke tidligere har været genstand for efterretningstjenestens opmærksomhed. Oplysninger om teletrafik har således i flere tilfælde været af afgørende betydning for at kunne afdække terrorrelationerne i både ind- og udland. I den forbindelse er det ikke alene af stor betydning at kunne tilvejebringe oplysninger om teletrafik af nyere dato, men tillige at kunne tilvejebringe ældre trafikdata for at konstatere, om der har været tale om en længerevarende forbindelse.

4. Justitsministeriets overvejelser

Som nærmere beskrevet i pkt. 2.2 ovenfor, gennemfører logningsbekendtgørelsen, der er udstedt i medfør af retsplejelovens § 786, stk. 4, væsentlige dele af Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF. Danmarks EU-retlige forpligtelser sætter således visse grænser for, hvilke ændringer der kan foretages af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen, der er fastsat i medfør heraf. Overvejelser om eventuelle ændringer af retsplejelovens § 786, stk. 4, må således ske i lyset af logningsdirektivet, der bl.a. fastsætter, at visse oplysninger om teletrafik *skal* registreres og opbevares i en vis periode.

Som det fremgår af de udtalelser, som Justitsministeriet til brug for udarbejdelsen af dette lovforslag har indhentet fra Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste, er det disse myndigheders vurdering, at de oplysninger om teletrafik, der registreres og opbevares i medfør af logningsbekendtgørelsen, der er fastsat i medfør af retsplejelovens § 786, stk. 4, generelt er af væsentlig betydning og i nogle tilfælde afgørende betydning for efterforskning og retsforfølgning af alvorlige forbrydelser. Det fremgår af udtalelserne, at oplysninger om teletrafik, der er registreret og opbevaret i medfør af logningsbekendtgørelsen, i en lang række tilfælde har haft væsentlig eller afgørende betydning for efterforskningen og retsforfølgningen bl.a. i sager om drab, terror, bandekriminalitet, narkotikakriminalitet, hjemmerøverier, seksuelle overgreb mod børn mv.

Endvidere har Rigsadvokaten og Rigspolitiet anført, at der ud fra hensynet til strafforfølgning kan være behov for at forlænge den gældende opbevaringsperiode på 1 år og behov for at registrere og opbevare flere typer af data. Rigsadvokaten har i den forbindelse foreslået, at nærmere overvejelser herom i givet fald sker i lyset af resultatet af det igangværende arbejde i EU-regi med evaluering af logningsdirektivet, og Rigspolitiet har oplyst, at man vil følge udviklingen på området fremover med henblik på at overveje behovet for at registrere og opbevare flere typer af data.

Evalueringen af logningsdirektivet forventes at finde sted i efteråret 2010.

I forbindelse med høringen over et udkast til dette lovforslag har flere organisationer mv., herunder tele- og internetbranchen, bl.a. anført, at revisionsbestemmelsen ikke bør ophæves på nuværende tidspunkt, og at branchens erfaringer mv. bør inddrages ved en kommende revision.

Justitsministeriet foreslår på den anførte baggrund, at revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, ikke ophæves på nuværende tidspunkt, men at revisionen af bestemmelsen udsættes til folketingsåret 2011-12, således at resultatet af den evaluering af logningsdirektivet, der forventes at finde sted i efteråret 2010, også kan indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet er

endvidere enig med bl.a. Rigspolitiet i, at det vil være hensigtsmæssigt at indhente yderligere erfaring med reglerne med henblik på at vurdere behovet for eventuelle ændringer.

I forbindelse med revisionen vil der så vidt muligt blive taget stilling til, om der er behov for at ændre opbevaringsperioden for loggede data, og om der er behov for at registrere og opbevare flere typer af data. Endvidere vil de synspunkter mv., som fremgår af høringssvarene over et udkast til dette lovforslag, indgå i overvejelserne. Justitsministeriet vil inddrage relevante myndigheder og organisationer mv., herunder tele- og internetbranchen, i forbindelse med revisionen.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4.

5. Lovforslagets økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for stat, kommuner eller regioner.

6. Lovforslagets økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

7. Lovforslagets administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

8. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

9. Forholdet til EU-retten

Lovforslaget indeholder ikke EU-retlige aspekter.

10. Hørte myndigheder mv.

Et udkast til lovforslaget har været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiforbundet i Danmark, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Danske Advokater, Landsforeningen af Forsvarsadvokater, Institut for Menneskerettigheder, Retssikkerhedsfonden, Amnesty International, Dansk Retspolitisk Forening, Dansk Erhverv, Brancheforeningen Telekommunikationsindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, ISPA DK (Foreningen af Internetleverandører), Foreningen af Danske Internet Medier, IT-Branchen, ITEK/Dansk Industri, PROSA, SAM-DATA (HK), IFPI Danmark, Business Software Alliance Danmark, Multimedieforeningen, Kommunedata KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Lejernes LO og Andelsboligforeningernes Fællesrepræsentation.

11. Sammenfattende skema

	Positive konsekvenser/ Mindreudgifter	Negative konsekvenser/ Merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen

Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Bestemmelsen fastsætter, at justitsministeren i folketingsåret 2011-12 skal fremsætte forslag om revision af bestemmelsen i retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2010.

Til § 3

Den foreslåede bestemmelse vedrører lovens territoriale gyldighed. Loven gælder ikke for Færøerne og Grønland, der har egne retsplejelove.

Bilag 1

Lovforslaget sammenholdt med gældende ret

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2009-10 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2009-10« til: »2011-12«.
	§ 2
	Loven træder i kraft den 1. juni 2010.
	§ 3
	Loven gælder ikke for Færøerne og Grønland.

2011/1 LSF 53 (Gældende)

Forslag til Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af revisionsbestemmelse)

Ministerium: Justitsministeriet

Journalnummer: Justitsmin., j.nr. 2011-731-0014

Fremsat den 14. december 2011 af justitsministeren (Morten Bødskov)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006 og lov nr. 650 af 15. juni 2010, foretages følgende ændring:

1. I *§ 8* ændres »2011-12« til: »2013-14«.

§ 2

Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

§ 3

Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Formålet med lovforslaget er at ændre revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, således at justitsministeren fremsætter forslag om revision af bestemmelsen i folketingsåret 2013-14 frem for 2011-12.

Retsplejelovens § 786, stk. 4, blev indført for at sikre, at oplysninger om teletrafik er tilgængelige, når politiet til brug for en konkret efterforskning eller retsforfølgning af alvorlig kriminalitet har indhentet en retskendelse med henblik på et indgreb i meddelelseshemmeligheden.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Regler herom er fastsat i bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

Med logningsbekendtgørelsen gennemføres væsentlige dele af Europa-Parlamentets og Rådets direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

2. Baggrund for revisionsbestemmelsen

2.1. Efter § 8 i lov nr. 378 af 6. juni 2002 (anti-terrorpakke I) skulle justitsministeren i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var, at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 886.

Ved § 7 i lov nr. 542 af 8. juni 2006 (anti-terrorpakke II) blev revisionen udskudt til folketingsåret 2009-10. Det skyldtes, at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af bestemmelsen, idet retsplejelovens § 786, stk. 4, først blev sat i kraft den 15. september 2007. Der blev med virkning fra samme dato med logningsbekendtgørelsen fastsat nærmere regler om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

2.2. Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det vil være hensigtsmæssigt at indhente yderligere erfaring med reglerne om logning med henblik på at vurdere behovet for eventuelle ændringer. Der henvises nærmere til pkt. 4 i de almindelige bemærkninger til det pågældende lovforslag (L 180 – folketingssamlingen 2009-10).

3. Gældende ret

3.1. Retsplejelovens § 786, stk. 4

3.1.1. Retsplejelovens § 786, stk. 4, blev indført ved lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007, jf. bekendtgørelse nr. 986 af 28. september 2006.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Retsplejelovens § 786, stk. 4, fastsætter en pligt for udbydere af telenet- og teletjenester til at registrere og opbevare oplysninger om teletrafik. Hensigten med bestemmelsen er således, at de pågældende oplysninger findes, hvis der bliver brug for dem.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgning af kriminalitet udgør et indgreb i meddelelseshemmeligheden, og adgangen til at få udleveret oplysninger, som en udbyder har registreret og opbevaret efter bestemmelsen, reguleres derfor af reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71 samt eventuelt også reglerne i kapitel 74 om edition.

3.1.2. Efter retsplejelovens § 786, stk. 4, skal udbydere alene registrere og opbevare oplysninger om, hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var, f.eks. i form af optagelse af en telefonsamtale.

I bemærkningerne til lovforslaget om anti-terrorpakke I (L 35, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 879) fremgår det således, at de oplysninger, som logningspligten kan omfatte, for så vidt angår *teletrafik* navnlig vil være de oplysninger, som politiet har brug for i form af teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4. Det kan f.eks. være det kaldende og det kaldte telefonnummer (A- og B-nummer), opkaldstidspunkter og varigheden af samtaler samt – for mobiltelefoners vedkommende – oplysninger om anvendte sendemaster/celler.

For så vidt angår *internettrafik* fremgår det, at der vil kunne fastsættes regler om logning af den dynamiske (skiftende) tildeling af IP-adresser, tidspunkt for opkobling og nedkobling samt opkoblingens varighed.

Samtidig fremgår det, at der *ikke* vil kunne fastsættes regler om, at internetudbydere løbende skal foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger, idet hensigten med bestemmel-

sen alene er at kunne føre elektroniske spor, der findes på internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

For så vidt angår *e-mail* er det med lovforslaget forudsat, at der ikke skal ske en generel logning af indholdsdata, men alene oplysninger svarende til teleoplysninger, det vil sige oplysninger om f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen imellem disse.

3.2. Logningsdirektivet

Af præamblen til logningsdirektivet – Europa-Parlamentets og Rådets direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF – fremgår det, at baggrunden for direktivet bl.a. er, at medlemsstaterne har praktiske erfaringer for, at trafikdata og lokaliseringsdata har stor betydning i efterforskning, afsløring og retsforfølgning af strafbare handlinger, og at det derfor er nødvendigt på europæisk plan at sikre, at data, som genereres eller behandles af udbydere af elektronisk kommunikation, lagres i en vis periode.

Direktivet opregner i artikel 5 de kategorier af data om telefoni, internettrafik og e-mail, som skal registreres og opbevares. Efter artikel 6 skal data lagres i mindst 6 måneder og højst 2 år regnet fra datoen for gennemførelsen af den omhandlede kommunikation. Efter artikel 10 skal medlemsstaterne hvert år give Kommissionen statistikker om lagring af data, der er behandlet i forbindelse med levering af offentlige elektroniske kommunikationstjenester.

Det fremgår af direktivets artikel 14, at Kommissionen senest den 15. september 2010 skal forelægge Europa-Parlamentet og Rådet en evaluering af direktivets anvendelse og dets virkning på de økonomiske aktører og forbrugerne. Evalueringen skal ske under hensyntagen til den udvikling, der er sket inden for elektronisk kommunikationsteknologi, og de statistiske oplysninger, som Kommissionen har modtaget i medfør af artikel 10. Formålet med evalueringen er at fastslå, om det er nødvendigt at ændre direktivet, særligt for så vidt angår listen over data i artikel 5 og de lagringsperioder, der er fastsat i artikel 6.

Kommissionen har den 18. april 2011 offentliggjort en evalueringsrapport om logningsdirektivet, jf. nærmere herom nedenfor under pkt. 4.

Fristen for medlemsstaterne til at gennemføre direktivet i national ret var den 15. september 2007, hvilket for Danmarks vedkommende bl.a. skete ved logningsbekendtgørelsen.

3.3. Logningsbekendtgørelsen og vejledningen hertil

3.3.1. Justitsministeriet udstedte den 28. september 2006 logningsbekendtgørelsen med hjemmel i retsplejelovens § 786, stk. 4. Bekendtgørelsen blev ledsaget af vejledning nr. 74 af 28. september 2006, som mere detaljeret redegør for den registrerings- og opbevaringspligt, som følger af logningsbekendtgørelsen.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net.

Efter logningsbekendtgørelsens §§ 4-6 skal udbyderne registrere en række nærmere angivne oplysninger om fastnettelefoni, mobiltelefoni, internettrafik, e-mail og internettelefoni. Det gælder bl.a. oplysninger om det opkaldte og det opkaldende nummer i forbindelse med telefonsamtaler, IP-adresser i forbindelse med brug af internettet samt modtagende og afsendende e-mail-adresser i forbindelse med brug af udbyderens egne e-mail-tjenester.

Udbyderne skal derimod ikke registrere og opbevare indholdet af kommunikation, hverken i forbindelse med telefonsamtaler, brug af internettet eller brug af udbyderens e-mail-tjenester.

De registrerede oplysninger opbevares i 1 år, jf. bekendtgørelsens § 9.

3.3.2. Logningsbekendtgørelsen gennemfører store dele af logningsdirektivet og er i vid udstrækning

baseret på direktivet, ligesom der anvendes samme terminologi i bekendtgørelsen som i direktivet. Bekendtgørelsen går dog på en række punkter videre end direktivet. Det drejer sig bl.a. om logning af visse oplysninger om hot spots og – for så vidt angår mobiltelefoner – logning af oplysninger om den første og sidste mast, som en mobiltelefon er forbundet med som led i kommunikationen.

3.3.3. Med henblik på at forbedre politiets mulighed for at sammenholde oplysninger om identiteten på brugere af kommunikationsmidler med oplysninger om de anvendte kommunikationsapparater er en tværministeriel arbejdsgruppe under Justitsministeriet og (nu) Erhvervs- og Vækstministeriet for tiden ved at overveje, hvordan oplysninger om brugere af taletidskort, internetcaféer, gratis trådløs adgang til internettet (hot spots) og internetadgang på biblioteker mv. kan registreres. Arbejdsgruppen skal bl.a. gennemgå og vurdere de tekniske muligheder for at registrere sådanne oplysninger, inddrage erfaringer fra andre lande, belyse økonomiske og administrative konsekvenser samt inddrage telebranchen i arbejdet.

4. Evalueringen af logningsdirektivet

Som nævnt ovenfor under pkt. 3.2 har Kommissionen i april 2011 offentliggjort en evalueringsrapport om logningsdirektivet. Evalueringen viser overordnet set, at logning er et nyttigt værktøj for retshåndhævelsen i EU. Det fremgår dog samtidig af evalueringen, at logningsdirektivets bidrag til en harmonisering af logning har været begrænset med hensyn til f.eks. formålsbegrænsning og lagringsperioder samt godtgørelse af operatørernes udgifter, som ligger uden for direktivets anvendelsesområde.

Kommissionen har i tilknytning til evalueringen oplyst, at den vil foreslå en revision af de nuværende logningsregler. Kommissionen vil finde frem til en række løsningsmuligheder i samråd med de retshåndhævende myndigheder, dommerstanden, erhvervssektoren, forbrugergrupper, datatilsynsmyndigheder og organisationer mv. Kommissionen vil undersøge offentlighedens opfattelse af logning, og logningens indflydelse på adfærden. Resultaterne heraf vil indgå i en konsekvensanalyse af den valgte løsningsmodel, som vil danne grundlag for Kommissionens forslag.

Det forventes, at Kommissionen i løbet af 2012 vil fremlægge et forslag til revision af logningsdirektivet. Kommissionens forslag til revision af logningsdirektivet vil herefter skulle forhandles i Rådet.

5. Justitsministeriets overvejelser

Som anført ovenfor under pkt. 3.3 gennemfører logningsbekendtgørelsen, der er udstedt i medfør af retsplejelovens § 786, stk. 4, væsentlige dele af logningsdirektivet. Danmarks EU-retlige forpligtelser sætter således grænser for, hvilke ændringer der kan foretages af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen, der er fastsat i medfør heraf. Overvejelser om eventuelle ændringer af retsplejelovens § 786, stk. 4, må således ske i lyset af logningsdirektivet, der bl.a. fastsætter, at visse oplysninger om teletrafik *skal* registreres og opbevares i en vis periode.

Som nævnt ovenfor under pkt. 4 forventes Kommissionen at fremlægge et forslag til revision af logningsdirektivet i løbet af 2012. Herefter vil forslaget skulle forhandles af EU-medlemsstaterne i Rådet.

Justitsministeriet foreslår på den baggrund, at revisionen af retsplejelovens § 786, stk. 4, udsættes til folketingsåret 2013-14, så revisionen af de danske logningsregler afventer den kommende revision af logningsdirektivet.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4.

Som tilkendegivet i forarbejderne til lov nr. 650 af 15. juni 2010, hvor revisionen blev udskudt til folketingsåret 2011-12, vil der i forbindelse med en revision af de danske logningsregler så vidt muligt blive taget stilling til, om der er behov for at ændre opbevaringsperioden for loggede data, og om der er behov for at registrere og opbevare flere typer af data. Desuden vil de synspunkter mv., som interessenterne på området fremkommer med, blive inddraget i overvejelserne, ligesom Justitsministeriet vil inddrage relevante myndigheder og organisationer mv., herunder tele- og internetbranchen, i forbindelse med en kommende revision af de danske logningsregler.

Som nævnt ovenfor under pkt. 3.3.3 er en tværministeriel arbejdsgruppe for tiden ved at overveje, hvordan oplysninger om brugere af taletidskort, internetcaféer, gratis trådløs adgang til internettet (hot spots) og internetadgang på biblioteker mv. kan registreres. Når arbejdsgruppens rapport foreligger, vil der være grundlag for at tage stilling til, i hvilket omfang rapporten kan give anledning til initiativer.

De anbefalinger, som arbejdsgruppen måtte fremkomme med, vil også blive inddraget i forbindelse med en kommende revision af retsplejelovens § 786, stk. 4.

6. De økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for det offentlige.

7. De økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

8. De administrative konsekvenser for borgere

Lovforslaget har ingen administrative konsekvenser for borgerne.

9. De miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

10. Forholdet til EU-retten

Lovforslaget indeholder ikke EU-retlige aspekter.

11. Hørte myndigheder og organisationer mv.

Et udkast til lovforslaget har været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Danske Advokater, Landsforeningen af Forsvarsadvokater, Institut for Menneskerettigheder, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, HORESTA, Brancheforeningen Telekommunikationsindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, ISPA DK (Foreningen af Internetleverandører), Foreningen af Danske Internet Medier, IT-Branchen, ITEK/Dansk Industri, PROSA, SAM-DATA (HK), IFPI Danmark, Business Software Alliance Danmark, IT-Politisk Forening, Multimedieforeningen, Kommunedata KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, Lejernes LO og Andelsboligforeningernes Fællesrepræsentation.

12. Sammenfattende skema

	Positive konsekvenser/ Mindreudgifter	Negative konsekvenser/ Merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen

Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Bestemmelsen fastsætter, at justitsministeren i folketingsåret 2013-14 skal fremsætte forslag om revision af bestemmelsen i retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger.

Til § 2

Det foreslås, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Til § 3

Den foreslåede bestemmelse vedrører lovens territoriale gyldighed. Loven vil ikke gælde for Færøerne og Grønland, der har egne retsplejelove.

Bilag 1

Lovforslaget sammenholdt med gældende ret

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006 og lov nr. 650 af 15. juni 2010, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2011-12 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2011-12« til: »2013-14«.
	§ 2
	Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.
	§ 3
	Loven gælder ikke for Færøerne og Grønland.

2012/1 LSF 142 (Gældende)

Forslag til Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af revisionsbestemmelse)

Ministerium: Justitsministeriet

Journalnummer: Justitsmin., j.nr. 2012-731-0021

Fremsat den 6. februar 2013 af justitsministeren (Morten Bødskov)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010 og lov nr. 573 af 18. juni 2012, foretages følgende ændring:

1. I *§ 8* ændres »2012-13« til: »2014-15«.

§ 2

Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Formålet med lovforslaget er at ændre revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om tele- og internetkommunikation (teletrafik) til brug for efterforskning og retsforfølgning af strafbare forhold, således at justitsministeren fremsætter forslag om revision af bestemmelsen i folketingsåret 2014-15 frem for 2012-13.

Retsplejelovens § 786, stk. 4, blev indført for at sikre, at oplysninger om teletrafik er tilgængelige, når politiet til brug for en konkret efterforskning eller retsforfølgning af alvorlig kriminalitet har indhentet en retskendelse med henblik på et indgreb i meddelelseshemmeligheden.

Med hjemmel i bestemmelsen er der fastsat nærmere regler om teleudbydernes registrering og opbevaring af de nævnte oplysninger i bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen). Bekendtgørelsen bygger i vidt omfang på Europa-Parlamentets og Rådets direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Europa-Kommissionen forventes at fremsætte forslag til revision af logningsdirektivet i løbet af 2013, evt. 2014. Herefter skal forslaget forhandles i EU-regi. Regeringen finder, at revisionen af de danske logningsregler bør afvente revisionen af direktivet.

2. Baggrund for revisionsbestemmelsen

2.1. Efter § 8 i lov nr. 378 af 6. juni 2002 (anti-terrorpakke I) skulle justitsministeren i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var, at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning

var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 886.

2.2. Ved § 7 i lov nr. 542 af 8. juni 2006 (anti-terrorpakke II) blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var, at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, idet bestemmelsen først blev sat i kraft den 15. september 2007. Med virkning fra samme dato blev der med logningsbekendtgørelsen fastsat nærmere regler om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

2.3. Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med reglerne om logning med henblik på at vurdere behovet for eventuelle ændringer. Der henvises nærmere til pkt. 4 i de almindelige bemærkninger til det pågældende lovforslag (L 180 – folketingssamlingen 2009-10).

2.4. Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget (L 53 – folketingssamlingen 2011-12) i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13.

Ved Folketingets Retsudvalgs betænkning af 31. maj 2012 over lovforslaget anmodede et flertal i udvalget Justitsministeriet om bl.a. at undersøge, hvorvidt logningsdirektivet er overimplementeret i Danmark, og at fremkomme med nærmere oplysninger om politiets og efterretningstjenesternes anvendelse af registrerede oplysninger om teletrafik. Der henvises til pkt. 3.3.2 og pkt. 3.4 nedenfor.

3. Gældende ret

3.1. Retsplejelovens § 786, stk. 4

3.1.1. Retsplejelovens § 786, stk. 4, blev indført ved lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007, jf. bekendtgørelse nr. 986 af 28. september 2006.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Bestemmelsen bemyndiger endvidere justitsministeren til efter forhandling med (nu) erhvervs- og vækstministeren at fastsætte nærmere regler om denne registrering og opbevaring.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgning af kriminalitet udgør et indgreb i meddelelseshemmeligheden, og adgangen til at få udleveret oplysninger, som en udbyder har registreret og opbevaret efter bestemmelsen, reguleres derfor af reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71 samt eventuelt også reglerne i kapitel 74 om edition. Det betyder blandt andet, at udlevering af oplysningerne i hvert enkelt tilfælde kræver en retskendelse.

3.1.2. Efter retsplejelovens § 786, stk. 4, skal udbydere alene registrere og opbevare oplysninger om,

hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var, f.eks. i form af optagelse af en telefonsamtale.

I bemærkningerne til lovforslaget om anti-terrorpakke I (L 35, jf. Folketingstidende 2001-02 (2. samling), tillæg A, side 879) fremgår det således, at de oplysninger, som logningspligten kan omfatte, for så vidt angår *teletrafik* navnlig vil være de oplysninger, som politiet har brug for i form af teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4. Det kan f.eks. være det kaldende og det kaldte telefonnummer (A- og B-nummer), opkaldstidspunkter og varigheden af samtaler samt – for mobiltelefoners vedkommende – oplysninger om anvendte sendemaster/celler.

For så vidt angår *internettrafik* fremgår det, at der vil kunne fastsættes regler om logning af den dynamiske (skiftende) tildeling af IP-adresser, tidspunkt for opkobling og nedkobling samt opkoblingens varighed.

Samtidig fremgår det, at der *ikke* vil kunne fastsættes regler om, at internetudbydere løbende skal foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger, idet hensigten med bestemmelsen alene er at kunne føre elektroniske spor, der findes på internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

For så vidt angår *e-mail* er det med lovforslaget forudsat, at der ikke skal ske en generel logning af indholdsdata, men alene oplysninger svarende til teleoplysninger, det vil sige oplysninger om f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen imellem disse.

3.2. Logningsdirektivet

Det fremgår af præamblen til logningsdirektivet, at baggrunden for direktivet bl.a. er, at medlemsstaterne har praktiske erfaringer for, at trafikdata og lokaliseringsdata har stor betydning i efterforskning, afsløring og retsforfølgning af strafbare handlinger, og at det derfor er nødvendigt på europæisk plan at sikre, at data, som genereres eller behandles af udbydere af elektronisk kommunikation, lagres i en vis periode.

Direktivet opregner i artikel 5 de kategorier af data om telefoni, internettrafik og e-mail, som skal registreres og opbevares. Efter artikel 6 skal data lagres i mindst 6 måneder og højst 2 år regnet fra datoen for gennemførelsen af den omhandlede kommunikation. Efter artikel 10 skal medlemsstaterne hvert år give Kommissionen statistikker om lagring af data, der er behandlet i forbindelse med levering af offentlige elektroniske kommunikationstjenester.

Det fremgår af direktivets artikel 14, at Kommissionen senest den 15. september 2010 skal forelægge Europa-Parlamentet og Rådet en evaluering af direktivets anvendelse og dets virkning på de økonomiske aktører og forbrugerne. Evalueringen skal ske under hensynstagen til den udvikling, der er sket inden for elektronisk kommunikationsteknologi, og de statistiske oplysninger, som Kommissionen har modtaget i medfør af artikel 10. Formålet med evalueringen er at fastslå, om det er nødvendigt at ændre direktivet, særligt for så vidt angår listen over data i artikel 5 og de lagringsperioder, der er fastsat i artikel 6.

Kommissionen har den 18. april 2011 offentliggjort en evalueringsrapport om logningsdirektivet, jf. nærmere herom nedenfor pkt. 4.

Fristen for medlemsstaterne til at gennemføre direktivet i national ret var den 15. september 2007, hvilket for Danmarks vedkommende bl.a. skete ved logningsbekendtgørelsen.

3.3. Logningsbekendtgørelsen og vejledningen hertil

3.3.1. Justitsministeriet udstedte den 28. september 2006 logningsbekendtgørelsen med hjemmel i rets-

plejelovens § 786, stk. 4. Bekendtgørelsen blev ledsaget af vejledning nr. 74 af 28. september 2006, som mere detaljeret redegør for den registrerings- og opbevaringspligt, som følger af logningsbekendtgørelsen.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net.

Bekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter bekendtgørelsens §§ 4-6 skal udbyderne registrere en række nærmere angivne oplysninger om fastnettelefoni, mobiltelefoni, internettrafik, e-mail og internettelefoni. Det gælder bl.a. oplysninger om det opkaldte og det opkaldende nummer i forbindelse med telefonsamtaler, IP-adresser i forbindelse med brug af internettet samt modtagende og afsendende e-mail-adresser i forbindelse med brug af udbyderens egne e-mail-tjenester.

Udbyderne skal derimod ikke registrere og opbevare indholdet af kommunikation, hverken i forbindelse med telefonsamtaler, brug af internettet eller brug af udbyderens e-mail-tjenester.

De registrerede oplysninger opbevares i 1 år, jf. bekendtgørelsens § 9.

3.3.2. Logningsbekendtgørelsen er i vid udstrækning udtryk for en gennemførelse af logningsdirektivet. Bekendtgørelsen går dog på en række punkter videre, end direktivet kræver. For så vidt angår internetkommunikation drejer det sig om forpligtelsen til at foretage såkaldt sessionslogning og logning af trafikdata fra trådløse WiFi Hot Spots. For så vidt angår telefoni drejer det sig om forpligtelsen til at logge oplysninger om ikke kun den første, men også den sidste mast, som en mobiltelefon er forbundet med som led i kommunikationen. Det er endvidere udtryk for et valg, når der i logningsbekendtgørelsen er fastsat en opbevaringsperiode på 1 år, idet direktivet bestemmer, at medlemsstaterne skal opbevare registrerede oplysninger i mindst 6 måneder og højst 2 år.

Disse forhold er nærmere beskrevet i Justitsministeriet redegørelse af 21. december 2012 til Folketingets Retsudvalg i henhold til udvalgets betænkning af 31. maj 2012, jf. pkt. 2.4.

3.3.3. Med henblik på at forbedre politiets mulighed for at sammenholde oplysninger om identiteten på brugere af kommunikationsmidler med oplysninger om de anvendte kommunikationsapparater har en tværministeriel arbejdsgruppe under Justitsministeriet og (nu) Erhvervs- og Vækstministeriet fået til opgave at overveje, hvordan oplysninger om brugere af taletidskort, internetcaféer, gratis trådløs adgang til internettet (hot spots) og internetadgang på biblioteker mv. kan registreres. Arbejdet er endnu ikke færdiggjort.

3.4. Den efterforskningsmæssige relevans af de registrerede oplysninger

I forbindelse med Folketingets behandling af forslaget til lov nr. 573 af 18. juni 2012 (L 53 – folketingsåret 2011-12) oplyste Justitsministeriet bl.a., at det er vurderingen hos Rigsadvokaten, Rigspolitiet og Politiets Efterretningstjeneste, at de oplysninger om teletrafik, der registreres og opbevares i medfør af logningsbekendtgørelsen, generelt er af væsentlig betydning og i nogle tilfælde afgørende betydning for efterforskning og retsforfølgning af alvorlige forbrydelser. Sådanne oplysninger har således i en lang række tilfælde haft væsentlig eller afgørende betydning for efterforskningen og retsforfølgningen i bl.a. sager om drab, terrorisme, bandekriminalitet, narkokriminalitet, hjemmerøverier og seksuelle overgreb mod

børn mv. Der henvises til Justitsministeriets svar på spørgsmål nr. 6, 24 og 43 fra Folketingets Retsudvalg vedrørende det nævnte lovforslag.

Den i pkt. 3.3.2 nævnte redegørelse til Folketingets Retsudvalg indeholder uddybende oplysninger om erfaringerne med anvendelsen af de registrerede oplysninger om teletrafik. Oplysningerne underbygger den væsentlige betydning af de oplysninger, der registreres om både telekommunikation og internetkommunikation, selv om der har været og fortsat er tekniske udfordringer med hensyn til logning og brug af oplysninger om internetkommunikation.

4. Evaluering og revision af logningsdirektivet

Som nævnt ovenfor under pkt. 3.2 har Kommissionen i april 2011 offentliggjort en evalueringsrapport om logningsdirektivet. Evalueringen viser overordnet set, at logning er et nyttigt værktøj for retshåndhævelsen i EU. Det fremgår dog samtidig af evalueringen, at logningsdirektivets bidrag til en harmonisering af logning har været begrænset med hensyn til f.eks. formålsbegrænsning og lagringsperioder samt godtgørelse af operatørernes udgifter, som ligger uden for direktivets anvendelsesområde.

Kommissionen har i tilknytning til evalueringen oplyst, at den vil foreslå en revision af de nuværende logningsregler. Kommissionen vil finde frem til en række løsningsmuligheder i samråd med de retshåndhævende myndigheder, dommerstanden, erhvervssektoren, forbrugergrupper, datatilsynsmyndigheder og organisationer mv. Kommissionen vil undersøge offentlighedens opfattelse af logning, og logningens indflydelse på adfærden. Resultaterne heraf vil indgå i en konsekvensanalyse af den valgte løsningsmodel, som vil danne grundlag for Kommissionens forslag.

Ifølge de senest foreliggende oplysninger forventes det, at Kommissionen vil fremsætte det tidligere bebudede forslag til revision af logningsdirektivet i løbet af 2013, evt. 2014. Kommissionens forslag til revision af logningsdirektivet vil herefter skulle forhandles i EU-regi.

Forsinkelsen af revisionen i forhold til den oprindelige tidshorisont, jf. pkt. 2.4 ovenfor, skyldes efter det oplyste blandt andet, at der i forbindelse med forhandlingerne om Kommissionens forslag til en generel forordning om databeskyttelse KOM (2012) 0011) er identificeret nogle problemstillinger, som efter Kommissionens opfattelse må afklares, inden logningsdirektivet kan revideres.

5. Justitsministeriets overvejelser

5.1. Efter Justitsministeriets opfattelse er registreringen og opbevarelsen af oplysninger om teletrafik i medfør af logningsbekendtgørelsen et centralt redskab i forbindelse med efterforskning og retsforfølgning af alvorlig kriminalitet.

Som anført under pkt. 3.4 har sådanne oplysninger i en lang række tilfælde haft væsentlig eller afgørende betydning for efterforskningen og retsforfølgningen i bl.a. sager om drab, terrorisme, bandekriminalitet, narkokriminalitet, hjemmerøverier og seksuelle overgreb mod børn mv.

Regeringen lægger i forlængelse heraf vægt på, at en revision af logningsreglerne ikke svækker mulighederne for at efterforske og retsforfølge terrorisme og andre former for alvorlig kriminalitet

5.2. Logningsbekendtgørelsen, der er udstedt i medfør af retsplejelovens § 786, stk. 4, bygger som anført under pkt. 3.3 i vidt omfang på logningsdirektivet. Danmarks EU-retlige forpligtelser sætter således grænser for, hvilke ændringer der kan foretages af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Endvidere vil fremtidige ændringer af logningsdirektivet med stor sandsynlighed nødvendiggøre tilpasning af de danske logningsregler.

En revision af de danske logningsregler er et meget omfattende arbejde, som indebærer inddragelse af

relevante myndigheder og organisationer mv., herunder tele- og internetbranchen. Hvis arbejdet gennemføres inden revisionen af logningsdirektivet, er der en nærliggende risiko for, at væsentlige forudsætninger for arbejdet brister, idet et revideret logningsdirektiv må forventes at ændre de EU-retlige krav til de danske regler.

Hertil kommer, at hvis der gennemføres en ændring af de gældende danske logningsregler, inden det reviderede logningsdirektiv foreligger, vil dette formentlig indebære, at reglerne skal ændres flere gange inden for kort tid, hvilket kan være til gene for bl.a. de virksomheder, andelsforeninger, ejerforeninger mv., der skal efterleve reglerne.

Justitsministeriet foreslår på den anførte baggrund, at revisionen af retsplejelovens § 786, stk. 4, udsættes til folketingsåret 2014-15, så revisionen af de danske logningsregler afventer den kommende revision af logningsdirektivet.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4.

5.3. Som tilkendegivet i forarbejderne til lov nr. 650 af 15. juni 2010, hvor revisionen blev udskudt til folketingsåret 2011-12, vil der i forbindelse med en revision af de danske logningsregler så vidt muligt blive taget stilling til, om der er behov for at ændre opbevaringsperioden for loggede data, og om der er behov for at registrere og opbevare flere typer af data. Desuden vil de synspunkter mv., som interessenterne på området fremkommer med, blive inddraget i overvejelserne, ligesom Justitsministeriet vil inddrage relevante myndigheder og organisationer mv., herunder tele- og internetbranchen, i forbindelse med en kommende revision af de danske logningsregler.

6. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for det offentlige.

7. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

8. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

9. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

10. Forholdet til EU-retten

Lovforslaget indeholder ikke EU-retlige aspekter.

11. Hørte myndigheder og organisationer mv.

Et udkast til lovforslaget har været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Danske Advokater, Landsforeningen af Forsvarsadvokater, Institut for Menneskerettigheder, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, HORESTA, Brancheforeningen Telekommunikationsindustrien, Brancheorganisationen Forbruger Elek-

tronik, Dansk IT, ISPA DK (Foreningen af Internetleverandører), Foreningen af Danske Internet Medier, IT-Branchen, ITEK/Dansk Industri, PROSA, SAM-DATA (HK), IFPI Danmark, Business Software Alliance Danmark, IT-Politisk Forening, Multimedieforeningen, Kommunedata KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, Lejernes LO og Andelsboligforeningernes Fællesrepræsentation.

12. Sammenfattende skema

	Positive konsekvenser/ Mindreudgifter	Negative konsekvenser/ Merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Bestemmelsen fastsætter, at justitsministeren i folketingsåret 2014-15 skal fremsætte forslag om revision af bestemmelsen i retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger.

Til § 2

Det foreslås, at loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006 og lov nr. 650 af 15. juni 2010, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2012-13 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2012-13« til: »2014-15«.
	§ 2
	Loven træder i kraft dagen efter bekendtgørelsen i Lovtidende.

BILAG 4

JUSTITSMINISTERIET
Lovafdelingen

Dato: 2. juni 2014
Kontor: EU-retskontoret
Sagsbeh: Nicholas Rahui Webster Rømer
Sagsnr.: 2014-6140-0620
Dok.: 1188632

Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler

1. Indledning

EU-Domstolen har ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 erklæret direktiv 2006/24/EF af 15. marts 2006 (herefter logningsdirektivet) ugyldigt under henvisning til, at EU-lovgiver har overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til artikel 7, 8 og 52, stk. 1, i Den Europæiske Unions Charter om grundlæggende rettigheder (herefter Charteret).

Nedenfor under pkt. 2 redegøres for EU-Domstolens bemærkninger i dommen af 8. april 2014. Dernæst redegøres under pkt. 3 for gældende dansk ret for så vidt angår logning, øvrige regler, der angår registrering og opbevaring af personers tele- og internetkommunikation, og udvalgte bestemmelser i persondataloven. Pkt. 4 indeholder Justitsministeriets vurdering af dommens betydning for de danske logningsregler, herunder muligheden for at opretholde gældende lovgivning. Den samlede konklusion fremgår under pkt. 5.

2. EU-Domstolens bemærkninger i de forenede sager C-293/12 og C-594/12

EU-Domstolen fastslår indledningsvis, at den pligt, der i henhold til (det nu ugyldige) logningsdirektiv gælder med hensyn til at lagre de i direktivets artikel 5 nævnte data samt de kompetente nationale myndigheders adgang til dataene, udgør et indgreb i de rettigheder, der er sikret ved Charterets artikel 7 om retten til respekt for privat- og familieliv, jf. præmis 34-35. Domstolen fastslår endvidere, at direktivet ligeledes indebærer et indgreb i den grundlæggende ret til beskyttelse af personoplysninger, som er

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

sikret ved Charterets artikel 8, eftersom det foreskriver en behandling af personoplysninger, jf. præmis 36. Domstolen bemærker på den baggrund, at det indgreb i de grundlæggende rettigheder, som direktivet herved indebærer, er meget vidtrækkende og må anses for at være af særligt alvorlig karakter. Den omstændighed, at lagringen af data og den efterfølgende anvendelse af dem finder sted, uden at abonnenten eller den registrerede bruger oplyses herom, er egnet til at skabe en følelse hos de berørte personer af, at deres privatliv er genstand for konstant overvågning, jf. præmis 37.

EU-Domstolen undersøger herefter, om indgrebet kan begrundes.

EU-Domstolen fastslår i den forbindelse, at den lagring af data, som kræves i henhold til direktivet, ikke er af en karakter, der kan krænke det væsentligste indhold af den grundlæggende ret til respekt for privatliv og beskyttelse af personoplysninger. Direktivet giver således ikke mulighed for at gøre sig bekendt med indholdet af den elektroniske kommunikation som sådan og bestemmer, at udbydere af tjenester eller telenet skal overholde visse principper om beskyttelse og sikkerhed vedrørende data, jf. præmis 38-40.

Endvidere fastslår EU-Domstolen, at lagring af data med henblik på en eventuel udlevering af disse til de kompetente nationale myndigheder i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet i medlemsstaterne, forfølger et formål af almen interesse, nemlig bekæmpelse af grov kriminalitet samt i sidste ende at bidrage til den offentlige sikkerhed, jf. præmis 41-44.

EU-Domstolen undersøger dernæst, om EU-lovgiver ved at vedtage direktivet overskred de grænser, der følger af proportionalitetsprincippet, dvs. om direktivet er udfærdiget på en sådan måde, at det både er egnet til at nå det tilsigtede lovlige mål (bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed) og ikke går videre, end hvad der er nødvendigt og passende for at nå dette mål, jf. præmis 46. Domstolen bemærker i den forbindelse, at EU-lovgivers skønsbeføjelse – henset dels til den betydelige rolle, som beskyttelsen af personoplysninger spiller i forhold til den grundlæggende ret til respekt for privatliv, dels til rækkevidden og alvoren af det indgreb i denne ret, som direktivet indebærer – er begrænset, således at der skal foretages en streng efterprøvelse, jf. præmis 47-48.

Det er EU-Domstolens opfattelse, at den lagring af data, der kræves i henhold til direktivet, kan anses for *egnet* til at gennemføre det mål, som forfølges med det nævnte direktiv, jf. præmis 49.

For så vidt angår vurderingen af, om direktivet går videre, end hvad der er nødvendigt og passende for at nå det tilsigtede mål (dvs. om direktivet er proportionalt), udtaler EU-Domstolen, at selv om bekæmpelse af grov kriminalitet, navnlig organiseret kriminalitet og terrorisme, er af afgørende betydning for at beskytte den offentlige sikkerhed, kan et sådant mål af almen interesse, hvor grundlæggende det end er, ikke i sig selv begrunde, at en foranstaltning som den lagring, der finder sted efter direktivet, anses som nødvendig. Beskyttelsen af personoplysninger har en særlig betydning for retten til respekt for privatlivet, der efter EU-Domstolens faste praksis kræver, at undtagelser fra eller begrænsninger i beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige, jf. præmis 51-53.

EU-Domstolen anfører på den baggrund i præmis 54, at EU-lovgivningen skal fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning og opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger.

I forlængelse heraf understreger EU-Domstolen, at behovet for at råde over sådanne garantier er så meget desto større, når persondata er undergivet automatisk databehandling, og hvor der er en betydelig risiko for ulovlig adgang til disse data, jf. præmis 55.

Det er EU-Domstolens opfattelse, at direktivet ikke fastsætter klare og præcise regler, der regulerer rækkevidden af indgrebet i de grundlæggende rettigheder beskyttet i Charterets artikel 7 og 8, hvorfor direktivet indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige. Domstolens begrundelse herfor er treleddet:

For det første omfatter direktivet generelt alle personer, alle elektroniske kommunikationsmidler og samtlige trafikdata, uden at der i direktivet fore-

tages nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om bekæmpelse af grov kriminalitet, jf. præmis 57.

Dels omfatter direktivet således generelt alle personer, der gør brug af elektroniske kommunikationstjenester, uden at de personer, hvis data lagres, dog – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning, og indeholder endvidere ikke nogen undtagelsesbestemmelse og finder således anvendelse selv på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt. Dels kræver direktivet ikke nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel mod den offentlige sikkerhed, og det er navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller den anden måde vil kunne være indblandet i grov kriminalitet, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til forebyggelse, afsløring og retsforfølgning af grov kriminalitet, jf. præmis 58-59.

For det andet fastsætter direktivet ikke et objektivt kriterium, der gør det muligt at afgrænse de kompetente nationale myndigheders adgang til dataene og den efterfølgende anvendelse af disse med henblik på forebyggelse, afsløring eller strafferetlig retsforfølgning vedrørende kriminalitet, der – henset til rækkevidden og alvoren af indgrebet i rettighederne, der er beskyttet i Charterets artikel 7 og 8 – kan anses for tilstrækkeligt grov til at begrunde et sådant indgreb. I direktivets artikel 1, stk. 1, er der i stedet alene henvist til "grov kriminalitet" som defineret i national ret, jf. præmis 60.

Endvidere indeholder direktivet ingen materielle og processuelle betingelser for de kompetente nationale myndigheders adgang til dataene og efterfølgende anvendelse heraf. Direktivet foreskriver således ikke udtrykkeligt, at denne adgang og efterfølgende anvendelse skal være strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger eller strafferetlig retsforfølgning heraf, jf. præmis 61.

Navnlig fastsætter direktivet ikke noget objektivt kriterium, der gør det muligt at begrænse antallet af personer, der er bemyndigede til at få adgang til og efterfølgende anvende lagrede data til det strengt nødvendige henset til formålet. Særligt er myndighedernes adgang til lagrede data ikke undergivet en forudgående kontrol, der udøves enten af en retsinstans eller af en uafhængig administrativ enhed, jf. præmis 62.

For det tredje foreskriver direktivet, at dataene skal lagres i minimum 6 måneder og maksimum 2 år, uden at der på nogen måde foretages en sondring mellem de forskellige kategorier af data efter deres relevans for det mål, som forfølges, eller afhængigt af, hvilke personer der er berørt. Det er således ikke præciseret, at fastsættelsen af lagringsperioden skal være baseret på objektive kriterier for at sikre en begrænsning til det strengt nødvendige, jf. præmis 63-64.

EU-Domstolen anfører på den baggrund, at direktivet ikke fastsætter klare og præcise regler, der regulerer rækkevidden af indgrebet i de grundlæggende rettigheder, som er fastslået i Chartrets artikel 7 og 8. Derfor fastslås det, at direktivet indebærer et indgreb i disse grundlæggende rettigheder, som er meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb er præcist afgrænset af bestemmelser, der gør det muligt at sikre, at det faktisk er begrænset til det strengt nødvendige, jf. præmis 65.

I de efterfølgende præmisser fastslår EU-Domstolen derudover, at direktivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre en effektiv beskyttelse af data – sådan som det er påkrævet efter artikel 8 i Charteret – mod risikoen for misbrug og mod enhver ulovlig adgang til og benyttelse af disse data. Der er således ikke fastsat regler, som er specifikke og tilpasset den meget store mængde data, til disse datas følsomme karakter samt til risikoen for ulovlig adgang til dataene, og som navnlig skulle udgøre en klar og streng regulering af beskyttelsen og sikkerheden af de omhandlede data med henblik på at sikre deres integritet og fortrolighed. Domstolen anfører endvidere, at direktivet sammenholdt med de relevante bestemmelser i direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (herefter e-data-beskyttelsesdirektivet) og direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter databeskyttelsesdirektivet) ikke sikrer, at udbyderne anvender et særlig højt beskyttelses- og sikkerhedsniveau ved hjælp af tekniske og organisatoriske foranstaltninger, men bl.a. tillader disse at tage økonomiske hensyn i betragtning ved fastlæggelsen af det sikkerhedsniveau, de anvender. Navnlig sikrer direktivet ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden, jf. præmis 66-67.

Endelig bemærker EU-Domstolen, at direktivet ikke fastsætter krav om, at dataene skal lagres inden for EU's område. Domstolen konstaterer, at det derfor ikke kan antages, at det fuldt ud er sikret, at overholdelse af kravene om beskyttelse og sikkerhed kontrolleres af en uafhængig myndighed, således som det udtrykkeligt påkræves efter Charterets artikel 8, stk. 3, jf. præmis 68.

EU-Domstolen erklærer henset til samtlige ovenstående betragtninger logningsdirektivet ugyldigt med henvisning til, at EU-lovgiver med vedtagelsen af direktivet anses for ikke at have handlet i overensstemmelse med proportionalitetsprincippet i lyset af Charterets artikel 7, 8 og 52, stk. 1, jf. præmis 69.

3. Dansk ret

3.1. Nedenfor redegøres først for de danske regler om logning, jf. pkt. 3.2. Dernæst redegøres for reglerne i telelovgivningen, der regulerer teleudbyderes adgang til i visse nærmere bestemte situationer at registrere og opbevare personers tele- og internetkommunikation, jf. pkt. 3.3. Endelig redegøres for udvalgte bestemmelser i persondataloven, jf. pkt. 3.4.

3.2.1. Ved lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I), blev der indsat en bestemmelse i retsplejelovens § 786, stk. 4, om registrering og opbevaring af oplysninger om teletrafik samt om telenet- og teletjenesteudbyderes praktiske bistand til politiet.

Det fremgår af forarbejderne til denne lov (pkt. 3.1.1.1 i de almindelige bemærkninger til lovforslag nr. L 35 fremsat den 13. december 2001), at bestemmelsen er indsat på baggrund af et forslag fra Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (Brydensholt-udvalget) i betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning.

3.2.2. Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysnin-

ger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Efter bestemmelsen fastsætter justitsministeren efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslaget), at retsplejelovens § 786, stk. 4, indebærer pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det er endvidere i forarbejderne (pkt. 1.2 i de almindelige bemærkninger til lovforslaget) forudsat, at udbydere alene skal registrere og opbevare oplysninger om, hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var.

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Efter logningsbekendtgørelsens § 4 skal teleudbydere registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, herunder oplysninger om det opkaldte og det opkaldende nummer og tidspunktet for kommunikationens start og afslutning.

Efter logningsbekendtgørelsens § 5 skal teleudbydere registrere en række nærmere angivne oplysninger om internettrafik. Det gælder bl.a. oplysninger om en brugers adgang til internettet og tidspunktet for kommunikationens start og afslutning. Der skal endvidere registreres oplysninger om selve internetsessionen, dvs. kilden og endepunktet for en internetkommunikation (sessionslogning).

Efter logningsbekendtgørelsens § 6 skal teleudbydere registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og in-

ternettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mail-adresser.

Det bemærkes i den forbindelse, at logningsbekendtgørelsen på enkelte punkter går videre end de forpligtigelser, der følger af logningsdirektivet, som er et minimumsdirektiv. Ifølge bekendtgørelsens § 4, stk. 1, nr. 6, skal der således registreres og opbevares oplysninger om den første og sidste mast, som en mobiltelefon er forbundet til som led i en kommunikation, mens direktivet kun stiller krav om, at der registreres og opbevares oplysninger om den første mast, jf. direktivets artikel 5, stk. 1, litra f, nr. 1.

For så vidt angår internetkommunikation går logningsbekendtgørelsen videre end direktivet, idet oplysninger om internetsessionen (også kaldet sessionslogning), dvs. kilden og endepunktet for en internetkommunikation, skal registreres og opbevares jf. § 5, stk. 1 og stk. 4. Der skal tillige logges oplysninger om trådløs adgang til internettet, herunder oplysninger om det lokale netværks geografiske placering samt identiteten på det benyttede kommunikationsudstyr.

3.2.3. Efter retsplejelovens § 786, stk. 4, og logningsbekendtgørelsens § 9 skal de registrerede oplysninger opbevares i 1 år.

For så vidt angår opbevaring af teletrafikdata fremgår det bl.a. af forarbejderne til lov nr. 378 af 6. juni 2002 (pkt. 3.1.3.1 i de almindelige bemærkninger til lovforslaget), at

> "Justitsministeriet foreslår, at opbevaringsperiodens varighed fastsættes til 1 år. Dette vil være i overensstemmelse med Europa-Parlamentet og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (97/66/EF), jf. pkt. 2.1.2. ovenfor. I det omfang, der ikke er tale om oplysninger, der i henhold til direktivet kan opbevares med henblik på kundedebitering, kan opbevaringstiden ikke være længere end hensynet til "forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager" tilsiger, jf. direktivets artikel 14, stk. 1. Efter Justitsministeriets opfattelses går en opbevaringsperiode på 1 år ikke videre, end dette hensyn tilsiger."

For så vidt angår opbevaring af internettrafikdata fremgår det endvidere af de nævnte forarbejder (pkt. 3.1.3.2 i de almindelige bemærkninger til lovforslaget), at

> "[d]er er, som [Brydensholt-]udvalget ligeledes anfører, tale om en vanskelig afvejning mellem på den ene side hensynet til kriminalitetsbekæmpelse og på den anden side hensynet til både privatlivets

> fred og de omkostninger, der påføres udbyderne. Særligt vedrørende hensynet til privatlivets fred tilsiger dette hensyn, at der logges mindst muligt, og at loggen opbevares i så kort tid som muligt, idet risikoen for, at oplysningerne falder i de forkerte hænder, er større, jo længere opbevaringsperioden er.
>
> Imidlertid tager selv terrorhandlinger af væsentlig mindre omfang end de tragiske angreb på New York og Washington den 11. september 2001 normalt lang tid at planlægge. Justitsministeriet finder det i lyset heraf tvivlsomt, om en opbevaringsfrist på kun 6 måneder dækker det behov for adgang til oplysninger, som politiet måtte have i en konkret sag. Efter Justitsministeriets opfattelse bør der derfor lægges afgørende vægt på de efterforskningsmæssige hensyn, der som Brydensholt-udvalget påpeger taler for en frist på ikke under 1 år. Justitsministeriet stiller på den baggrund forslag om en lovfæstet opbevaringsperiode på 1 år."

3.2.4. Det følger af § 1 i logningsbekendtgørelsen, at de registrerede oplysninger skal opbevares med henblik på at kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

De nærmere betingelser for, hvornår udbydere af telenet og teletjenester skal udlevere oplysningerne, fremgår af retsplejelovens regler om indgreb i meddelelseshemmeligheden og edition.

3.2.4.1. De oplysninger om teletrafik, som teleudbydere ifølge logningsbekendtgørelsen skal registrere, udgør i vidt omfang historiske teleoplysninger i retsplejelovens forstand. Det betyder efter retspraksis, at indhentelse af oplysningerne kan finde sted efter reglerne om edition, hvis betingelserne for indgreb i meddelelseshemmeligheden samtidig er opfyldt.

Visse oplysninger, som er registreret hos en teleudbyder i henhold til logningsbekendtgørelsen, vil dog kunne indhentes alene efter reglerne om edition. Det drejer sig navnlig om oplysninger om de master, som en mobiltelefon er forbundet til som led i en kommunikation, samt oplysning om, hvem der på et givet tidspunkt har været bruger af en specifik internetprotokol-adresse.

Retsplejelovens regler om indgreb i meddelelseshemmeligheden og edition gennemgås nærmere nedenfor.

3.2.4.2. Det er alene politiet, der efter retsplejelovens § 780 kan foretage indgreb i meddelelseshemmeligheden, herunder få udleveret registrerede historiske teleoplysninger.

De nærmere betingelser for at foretage indgreb i meddelelseshemmeligheden fremgår navnlig af retsplejelovens §§ 781-783.

Retsplejelovens § 781 opstiller særlige krav til mistankegrundlaget (mistankekravet), behovet for at foretage indgrebet (indikationskravet) samt til grovheden af den kriminalitet, som efterforskningen angår (kriminalitetskravet). Således kræves det, at der foreligger bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt, ligesom indgrebet må antages at være af afgørende betydning for efterforskningen. Det er endvidere et krav, at efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af f.eks. straffelovens kapitel 12 (forbrydelser mod statens selvstændighed og sikkerhed) og 13 (forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.), eller en række særligt oplistede bestemmelser i straffeloven og særlovgivningen, herunder bl.a. udlændingeloven.

Fælles for disse særligt oplistede bestemmelser, jf. retsplejelovens § 781, stk. 1, nr. 3, sidste led, stk. 2 og stk. 3, er, at de alle har en lavere strafferamme end 6 års fængsel, jf. det generelle strafferammekrav i retsplejelovens § 781, stk. 1, nr. 3.

Bestemmelserne om indgreb i meddelelseshemmeligheden har i det væsentligste fået deres nuværende udformning ved lov nr. 227 af 6. juni 1985, der er udarbejdet på grundlag af Strafferetsplejeudvalgets betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Straffelovens § 124, stk. 2 (ændret fra stk. 1 til stk. 2 ved lov nr. 382 af 6. juni 2002), og §§ 125, 127, stk. 1, 266 og 281 blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved denne lov. Det fremgår i den forbindelse af pkt. 2.4 i de almindelige bemærkninger til lovforslaget, at de nævnte bestemmelser blev taget med under henvisning til betænkning nr. 1023/1984.

Det fremgår af betænkningen s. 51, at der i udvalget var enighed om, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden. Samtidig påpegede udvalget, at der i det moderne samfund findes nye kriminalitetsformer, der er kendetegnet ved, at sædvanlige efterforskningsmetoder ikke er tilstrækkelige.

Det fremgår nærmere af betænkning nr. 1023/1984, s. 91f, at udvalget har fundet det nødvendigt at føje enkelte bestemmelser til hovedreglen om et kriminalitetskrav på 6 års fængsel i strafferammen. Indføjelse af straffelovens §§ 124, 125 og 127, stk. 1, begrundes med, at de har karakter af komplot, og at telefonaflytning kan være en hensigtsmæssig foranstaltning til at hindre eller opklare fangeflugt. For så vidt angår straffelovens § 281 fremgår det, at telefonaflytning og teleoplysninger her er helt relevante efterforskningsmidler. Vedrørende straffelovens § 266 lægger udvalget vægt på, at telefonkommunikation netop er et særligt egnet middel til at fremsætte trusler, hvorfor telefonaflytning kan være nødvendig for at afsløre den truendes identitet.

Straffelovens § 235 om børnepornografi blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 441 af 31. maj 2000. Det fremgår bl.a. af pkt. 8.3.2 i de almindelige bemærkninger til lovforslaget, at det fortsat er Justitsministeriets principielle synspunkt, at der generelt bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, men at der imidlertid kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige. Justitsministeriet finder derfor, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der – på enkelte områder – er særlige behov for at udvide adgangen til at foretage indgreb i meddelelseshemmeligheden. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv. Det fremgår endvidere, at Justitsministeriet på det foreliggende grundlag kun har overvejet, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, da denne kriminalitet i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er tilstrækkelige, hvorfor der i sager af denne karakter skal være mulighed for at foretage indgreb i meddelelseshemmeligheden, uanset at det almindelige krav om mindst 6 års fængsel i strafferammen ikke er opfyldt.

Straffelovens § 233, stk. 1, (tidligere § 228) om rufferi blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 436 af 10. juni 2003. Der henvises i pkt. 6.2 i de almindelige bemærkninger til lovforslaget på ny til, at der generelt bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, og at der i forbindelse med overvejelser om, at udvide adgangen hertil foretages en overordnet afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den

anden side hensynet til borgernes privatliv, men at der imidlertid kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige. Det fremgår i den forbindelse bl.a., at udviklingen i det danske prostitutionsmiljø, herunder den mere organiserede måde prostitution drives på i dag, har medført, at politiet har fået stadig vanskeligere ved at efterforske og opklare bagmandsvirksomhed i forbindelse med prostitution, og at frygten for repressalier afholder de prostituerede, der udnyttes ved bagmændenes virksomhed, fra at medvirke til sagens opklaring.

Muligheden for at foretage indgreb i meddelelseshemmeligheden ved mistanke om overtrædelse af udlændingelovens § 59, stk. 7, nr. 1-5 (dengang § 59, stk. 3, og senere § 59, stk. 5), om forsætlig bistand til udlændinge med ulovlig indrejse, ophold, arbejde samt vidererejse blev indsat i retsplejelovens § 781, stk. 1, nr. 3, ved lov nr. 411 af 6. oktober 1997.

Det fremgår af pkt. 3.3 i de almindelige bemærkninger til lovforslaget fra 1997, at indgreb i meddelelseshemmeligheden i mange tilfælde vil være et relevant efterforskningsmiddel i forhold til kriminalitet, som er kendetegnet ved, at den begås af flere personer i forening, og at der på den baggrund bør være adgang til indgreb i meddelelseshemmeligheden for kriminalitetsformer, der ofte begås af en flerhed af personer, i det omfang, der er tale om kriminalitet af en sådan alvorlig karakter, at sådanne indgreb er velbegrundede.

Det fremgår endvidere af Retsudvalgets betænkning over lovforslaget, at baggrunden for ændringsforslaget, hvorefter en overtrædelse af udlændingelovens § 59, stk. 7, nr. 1-5, blev indsat i retsplejelovens § 781, stk. 1, nr. 3, var, at udviklingen i den internationale menneskesmugling i stadig stigende omfang bar præg af professionel planlægning, at en meget stor andel af asylansøgerne var kommet til Danmark illegalt, bistået af personer, der mod betaling havde hjulpet de pågældende hertil, at menneskesmugling udgjorde en grov kriminalitetsform, og at det således var af afgørende betydning at styrke politiets muligheder for at optrevle den professionelle menneskesmugling ved at give politiet adgang til at foretage indgreb i meddelelseshemmeligheden som led i efterforskningen af sager om menneskesmugling. Det fremgår endvidere, at de almindelige betingelser for at foretage indgreb i meddelelseshemmeligheden, herunder mistankekravet (§ 781, stk. 1, nr. 1) og indikationskravet (retsplejelovens § 781, stk. 1, nr. 2) også gælder i disse sager. Herudover gælder kravet om proportionalitet i retsplejelovens § 782.

Efter retsplejelovens § 782 må indgrebet ikke være uforholdsmæssigt i forhold til indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer.

Endvidere foreskriver retsplejelovens § 783, at indgreb i meddelelseshemmeligheden alene kan ske efter indhentelse af en retskendelse, medmindre indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes. I så fald skal indgrebet forelægges for retten senest 24 timer fra indgrebets iværksættelse.

Det følger af retsplejelovens § 784, stk. 1, at der – inden retten træffer afgørelse efter § 783 – skal beskikkes en advokat for den, som indgrebet vedrører, og at advokaten skal have lejlighed til at udtale sig.

Endelig følger det af retsplejelovens § 788, at der efter afslutningen af et indgreb i meddelelseshemmeligheden skal gives underretning om indgrebet til bl.a. indehaveren af den pågældende telefon ved telefonaflytning og teleoplysning, medmindre underretning eksempelvis vil være til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 788, stk. 4.

3.2.4.3. For så vidt angår reglerne om edition fremgår det af retsplejelovens § 804, at retten som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, kan meddele en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande, hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. I modsætning til reglerne om indgreb i meddelelseshemmeligheden indeholder reglerne om edition – bortset fra kravet om, at der skal være tale om lovovertrædelse, der er undergivet offentlig påtale – ikke noget krav om, at lovovertrædelserne skal være af en særlig art eller grovhed.

Det fremgår af retsplejelovens § 806, stk. 2, at afgørelse om pålæg om edition træffes af retten ved kendelse. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet dog i medfør af § 806, stk. 4, træffe beslutning om edition. Fremsætter den, som indgrebet retter sig mod, anmodning herom, skal politiet snarest muligt og senest in-

den 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes.

3.2.4.4. For så vidt angår politiets, herunder PET's, erfaringer med anvendelsen af logningsreglerne henvises der til pkt. 5 og 6 i Justitsministeriets redegørelse af 21. december 2012 til Folketingets Retsudvalg om diverse spørgsmål vedrørende logningsreglerne og Justitsministeriets svar af 28. maj 2014 på spørgsmål nr. 942 (Alm. del) fra Folketingets Retsudvalg.

3.2.5. For så vidt angår anden hjemmel end retsplejeloven til udlevering af oplysninger, der registreres og opbevares i henhold til logningsbekendtgørelsen, kan det om Justitsministeriets område oplyses, at Datatilsynet efter persondatalovens § 62, stk. 1, kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under persondatalovens bestemmelser.

Baggrunden for bestemmelsen, der udspringer af persondatadirektivets artikel 28, stk. 3, er, at Datatilsynet som tilsynsmyndighed skal have mulighed for at kræve oplysninger udleveret af både den offentlige forvaltning og private dataansvarlige.

Bestemmelsen omfatter – jf. udtrykket "enhver oplysning" – i princippet også oplysninger registreret efter logningsbekendtgørelsen, men det må antages, at det kun i helt særlige tilfælde vil være relevant for Datatilsynet at indhente sådanne oplysninger.

Efter § 73 i lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014 (herefter teleloven), som hører under Erhvervs- og Vækstministeriet, kan Erhvervsstyrelsen kræve alle oplysninger og alt materiale, som Erhvervsstyrelsen skønner relevant i forbindelse med tilsyn med overholdelse af lovens regler eller regler fastsat i medfør heraf og i forbindelse med administration, undersøgelser og konkrete afgørelser, der gennemføres og træffes efter lovens bestemmelser herom, af blandt andre udbydere af elektroniske kommunikationsnet eller -tjenester og udbydere af teleterminaludstyr, der anvendes til mobilkommunikationstjenester.

Erhvervs- og Vækstministeriet har oplyst, at bestemmelsen efter sin ordlyd principielt kunne omfatte de i logningsbekendtgørelsen anførte oplysninger, men at indhentelse mv. af sådanne oplysninger ville forudsætte, at dette kunne betragtes som relevant i forhold til de pågældende bestemmelsers

formål, hvilket er usandsynligt.

Ifølge skattekontrollovens § 8 D, som hører under Skatteministeriet, skal blandt andre bestyrelser eller lignende øverste ledelser for private juridiske personer efter anmodning meddele told- og skatteforvaltningen oplysninger, der af myndighederne skønnes at være af væsentlig betydning for skatteligningen.

Bestemmelsen blev i sin nuværende form indsat i skattekontrolloven ved lov nr. 1113 af 21. december 1994. Det fremgår af lovforslagets specielle bemærkninger om bestemmelsen, at skattemyndighedernes adgang efter skattekontrollovens § 8 D, stk. 1, til at rekvirere oplysninger til brug for skattemyndighedernes virksomhed fra juridiske personer mv. begrænses til kun at omfatte oplysninger, der skønnes at ville være af væsentlig betydning for skattemyndighedernes virksomhed. I væsentlighedskriteriet ligger bl.a., at skattemyndighederne skal være tilbageholdende med at kræve nødvendige oplysninger direkte fra juridiske personer mv., hvis oplysningerne lige så vel kan kræves af den skattepligtige selv eller gennem denne.

Skatteministeriet har oplyst, at SKAT med hjemmel i den nævnte bestemmelse i forbindelse med ligning af en skattepligtig kan anmode teleselskaberne om at oplyse den skattepligtiges brug af telefon, typisk ved fremsendelse af specificeret faktura. Skatteministeriet har endvidere oplyst, at der i praksis er tale om oplysninger, der registreres i henhold til bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet og -tjenester (herefter udbudsbekendtgørelsen, jf. nærmere nedenfor). Skatteministeriet har i samarbejde med Erhvervsstyrelsen rettet henvendelse til Europa-Kommissionen for at få afklaret, om der eventuelt er regelkonflikt mellem skattekontrolloven og e-data-beskyttelsesdirektivet (2002/58/EF). Skatteministeriet har oplyst, at de oplysninger, der i praksis indhentes, er oplysninger, der registreres i henhold til udbudsbekendtgørelsen, og at det er usandsynligt, at SKAT skulle få behov for at indhente oplysninger registreret i henhold til logningsbekendtgørelsen. Efter det oplyste har Skatteministeriet ikke taget stilling til, om sådanne oplysninger i givet fald ville kunne indhentes med hjemmel i skattekontrollovens § 8 D.

3.3. Lov om elektroniske kommunikationsnet og -tjenester (teleloven) indeholder regler, hvis formål er at fremme et velfungerende og innovationspræget marked for elektroniske kommunikationsnet og -tjenester til gavn for slutbrugerne. Loven indeholder regler, der bl.a. gennemfører e-data-beskyttelsesdirektivet.

I medfør af bl.a. telelovens § 8, stk. 1, 2 og 4, jf. § 20, stk. 1, har erhvervs- og vækstministeren udstedt udbudsbekendtgørelsen. Ifølge bekendtgørelsens § 19 skal teleudbydere, hvis deres opkrævning er afhængig af forbruget, tilbyde kunden specificeret regning. Til brug for dette registrerer og opbevarer teleudbyderen oplysninger, sådan at kunden kan identificere forbruget af tjenesten. De oplysninger, teleudbyderen skal registrere, er blandt andet tidspunkt, varighed og opkaldt nummer.

Formålet med bestemmelsen er at give kunderne mulighed for at kontrollere, at teleudbyderens opkrævning for forbrug af teletjenesten er korrekt.

Efter § 23 i udbudsbekendtgørelsen skal udbydere af offentlige elektroniske kommunikationsnet eller -tjenester sikre, at trafikdata vedrørende abonnenter eller brugere slettes eller anonymiseres, når de ikke længere er nødvendige for fremføringen af kommunikationen. Det fremgår dog samtidig af bestemmelsen, at det er tilladt for en udbyder at opbevare trafikdata til visse nærmere angivne formål, herunder bl.a. til debitering af abonnenter samt til opfyldelsen af de forpligtelser, der påhviler dem i medfør af logningsbekendtgørelsen.

Erhvervsstyrelsen under Erhvervs- og Vækstministeriet har oplyst, at sletningsreglen i udbudsbekendtgørelsens § 23 bl.a. gælder for oplysninger, der er logget efter logningsbekendtgørelsen. Oplysninger, som teleudbyderne registrerer og opbevarer *alene* med det formål at opfylde logningsforpligtelsen i henhold til logningsbekendtgørelsen, vil således ikke efter de gældende regler kunne opbevares i mere end 1 år, jf. den 1-årige opbevaringspligt i logningsbekendtgørelsens § 9.

Erhvervsstyrelsen har over for Justitsministeriet på spørgsmålet om, hvilke sikkerhedskrav til teleudbyderne der gælder på telelovgivningens område, herunder hvilke garantier der i denne lovgivning er fastsat for at sikre en effektiv beskyttelse af data mod risiko for misbrug samt ulovlig adgang til og benyttelse af data, endvidere oplyst følgende:

> "Erhvervsstyrelsen kan som uafhængig telemyndighed oplyse, at opbevaring eller lagring af data, som er logget efter Justitsministeriets logningsbekendtgørelse er underlagt reglerne i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester. Bekendtgørelsen er udstedt med hjemmel i § 8, stk. 1 og 8, stk. 4 i lov 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester.
>
> Reglerne om persondatasikkerhed følger af bekendtgørelsens § 7. Efter denne bestemmelse skal net- og tjenesteudbyderne jf. § 5 gennemføre en risikovurdering og udarbejde en sikkerhedspolitik

for persondatasikkerheden i forbindelse med net- og tjenesteudbuddet og i relevant omfang sikringsplaner omfattende foranstaltninger til beskyttelse heraf. Sådanne foranstaltninger skal leve op til kravene i kap. 4 i bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet- og tjenester – herunder kravene til behandling (navnlig sletning og anonymisering) af trafik- og lokaliseringsdata.

Herudover skal foranstaltningerne som minimum:

1. Sikre at kun autoriserede personer får adgang til persondata til lovlige formål
2. Beskytte lagrede persondata og persondata under transmission mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse.

Erhvervsstyrelsen kan desuden oplyse, at der på myndighedens område ikke findes specifikke regler, der regulerer overførsel af data til lande uden for EU."

Erhvervsstyrelsen fører som telemyndighed tilsyn med, at teleudbyderne overholder reglerne i udbudsbekendtgørelsen og bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester (herefter sikkerhedsbekendtgørelsen), jf. den generelle tilsynspligt i telelovens § 20.

3.4. Persondataloven indeholder regler om persondatabeskyttelse. Loven gennemfører databeskyttelsesdirektivet.

Persondataloven gælder bl.a. for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, jf. lovens § 1, stk. 1.

Teleudbyderes behandling af personoplysninger er ud over reglerne i telelovgivningen reguleret af de generelle bestemmelser i persondataloven, i det omfang disse ikke er fortrængt af særregler i f.eks. telelovgivningen, jf. herved persondatalovens § 2, stk. 1.

Det fremgår af persondatalovens § 55, at Datatilsynet fører tilsyn med enhver behandling, der omfattes af loven. Tilsynet med de bestemmelser i persondataloven, som finder anvendelse på teleudbydernes behandling af personoplysninger, fordi de ikke er fortrængt af særregler i telelovgivningen, ligger derfor hos Datatilsynet. Datatilsynet udøver sine funktioner i fuld uafhængighed, jf. lovens § 56.

Af persondatalovens §§ 41 og 42 fremgår bl.a., at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Det fremgår endvidere, at en dataansvarlig, når denne overlader en behandling af oplysninger til en databehandler, skal sikre sig, at databehandleren kan træffe de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker. Det er i forarbejderne til persondataloven forudsat, at foranstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. herved også databeskyttelsesdirektivets artikel 17, stk. 1, 2. afsnit.

I persondataloven er der desuden fastsat nærmere regler om overførsel af oplysninger til tredjelande.

Det fremgår af persondatalovens § 27, stk. 1, at oplysninger kun må overføres til et tredjeland, hvis dette land sikrer et tilstrækkeligt sikkerhedsniveau. Ved tredjeland forstås en stat, som ikke indgår i EU, og som ikke har gennemført aftaler, der er indgået med EU, og som indeholder regler svarende til databeskyttelsesdirektivet, jf. persondatalovens § 3, nr. 9.

Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, skal efter persondatalovens § 27, stk. 2, ske på grundlag af samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, herunder regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet.

Kommissionen kan med bindende virkning for medlemsstaterne træffe beslutning om, at et bestemt tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, jf. artikel 25, stk. 6, i databeskyttelsesdirektivet.

I de tilfælde, hvor et tredjeland ikke kan siges at sikre et tilstrækkeligt beskyttelsesniveau, kan der ske overførsel af oplysninger til det pågældende tredjeland, hvis betingelserne i § 27, stk. 3, er opfyldt, herunder hvis den registrerede har givet udtrykkeligt samtykke hertil, jf. stk. 3, nr. 1, eller hvis overførslen er nødvendig eller følger af lov eller bestemmelser fastsat i henhold til lov for at beskytte en vigtig samfundsmæssig interesse eller

for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. stk. 3, nr. 4. Det bemærkes i den forbindelse, at det følger af persondatalovens § 50, stk. 2, at ved overførsel af oplysninger, som nævnt i bestemmelsens stk. 1 – det vil bl.a. sige ved overførsel af følsomme personoplysninger – til tredjelande i medfør af bl.a. § 27, stk. 3, nr. 2-4, skal der indhentes en tilladelse fra Datatilsynet.

Uden for de i stk. 3 nævnte tilfælde kan Datatilsynet give tilladelse til, at der overføres oplysninger til tredjelande, som ikke opfylder stk. 1, hvis den dataansvarlige yder tilstrækkelige garantier for beskyttelse af de registreredes rettigheder, jf. persondatalovens § 27, stk. 4.

Efter persondatalovens § 27, stk. 5, kan overførsel til tredjelande ske uden tilladelse fra Datatilsynet, på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser godkendt af Kommissionen.

Det bemærkes, at bestemmelsen i persondatalovens § 27 om overførsel af personoplysninger til tredjelande både gælder ved videregivelse af personoplysninger til en anden dataansvarlig, ved overladelse af personoplysninger til en databehandler samt ved intern brug, f.eks. inden for en koncern.

4. Dommens betydning for de danske logningsregler

4.1. På baggrund af EU-Domstolens dom af 8. april 2014 er der rejst spørgsmål om, hvorvidt de danske logningsregler kan opretholdes, altså om de gældende danske logningsregler er i overensstemmelse med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og om retten til beskyttelse af personoplysninger (artikel 8).

4.2. Justitsministeriet skal indledningsvis bemærke, at det er ministeriets vurdering, at Charteret finder anvendelse i forhold til de danske logningsregler.

Efter Charterets artikel 51 finder det anvendelse i forhold til medlemsstaterne, "når de gennemfører EU-retten". Det fremgår af de såkaldte forklaringer til Charterets artikel 51, der i overensstemmelse med Traktaten om Den Europæiske Unions artikel 6, stk. 1, og Charterets artikel 52, stk. 7, skal tages i betragtning i forbindelse med fortolkningen af dette, at Charteret også finder anvendelse, når medlemsstaterne handler inden for EU-retten. Samtidig følger det af e-data-beskyttelsesdirektivets artikel 15, stk. 1, 2. pkt., at medlemsstaterne af hensyn til bl.a. forebyggelse, efterforsk-

ning, afsløring og retsforfølgning i straffesager kan vedtage retsforskrifter om lagring af data i en begrænset periode[1]. En medlemsstat, der, som sket ved de danske logningsregler, fastsætter regler om logning af teledata, handler således efter Justitsministeriets opfattelse inden for rammerne af EU-retten.

På den baggrund er det Justitsministeriets opfattelse, at de danske logningsregler – selv om Danmark, nu hvor logningsdirektivet er erklæret ugyldigt, strengt taget ikke gennemfører dette – som følge af e-databeskyttelsesdirektivets artikel 15 falder inden for EU-rettens anvendelsesområde, jf. Charterets artikel 51, stk. 1, således som denne bestemmelse er fortolket i EU-Domstolens dom i sag C-617/10, Hans Åkerberg Fransson[2].

4.3. Det skal derfor vurderes, om den gældende danske lovgivning på området er i overensstemmelse med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og ret til beskyttelse af personoplysninger (artikel 8).

De rettigheder, der sikres ved Charterets artikel 7 om respekt for privatliv og familieliv, svarer indholdsmæssigt til de rettigheder, der er sikret ved Den Europæiske Menneskerettighedskonventions (herefter EMRK) artikel 8. Ligeledes er Charterets artikel 8 om beskyttelse af personoplysninger baseret på bl.a. EMRK artikel 8.

EMRK artikel 8 har følgende ordlyd:

> "Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
> Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundhe-

[1] Det bemærkes, at det fremgår af direktivets artikel 1, stk. 3, at direktivet under ingen omstændigheder gælder for bl.a. "statens aktiviteter på det strafferetlige område." Efter Justitsministeriets opfattelse er denne undtagelse vedrørende det strafferetlige område begrænset til tilfælde, hvor staten opbevarer og behandler data som led i strafferetlige aktiviteter. I modsætning hertil retter de danske logningsregler sig mod teleudbydere.

[2] I denne sag havde de svenske myndigheder fastsat regler om sanktioner i tilknytning til et direktiv, uden at direktivet forpligtede hertil. EU-Domstolen fandt, at strafforfølgningen af Åkerberg Fransson efter de pågældende bestemmelser udgjorde en gennemførelse af EU-retten i den forstand, hvori udtrykket er anvendt i Charterets artikel 51, stk. 1, selv om den svenske lovgivning ikke var vedtaget for at gennemføre direktivet i national ret, da anvendelsen af de svenske regler havde til formål at sanktionere en tilsidesættelse af direktivets bestemmelser og dermed havde til formål at gennemføre medlemsstaternes traktatmæssige forpligtelse til effektivt at sanktionere adfærd, der skader Unionens finansielle interesser.

> den eller sædeligheden eller for at beskytte andres rettigheder og friheder."

Det følger af Charterets artikel 52, stk. 3, at i det omfang Charteret indeholder rettigheder svarende til dem, der er sikret ved EMRK, har de samme betydning og omfang som i konventionen. I det omfang rettighederne i Charteret således svarer til rettighederne i EMRK, skal rettighederne i Charteret derfor fortolkes i overensstemmelse med Den Europæiske Menneskerettighedsdomstols (herefter Menneskerettighedsdomstolen) retspraksis vedrørende de relevante bestemmelser i EMRK.

4.4. I det følgende foretages en analyse af betydningen af EU-Domstolens dom af 8. april 2014 for dansk ret med udgangspunkt i dommen og artikel 7 og 8 i Charteret og med inddragelse af Menneskerettighedsdomstolens praksis vedrørende EMRK, hvor det er relevant.

4.4.1. Indledningsvis bemærkes, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen tager udgangspunkt i den forpligtelse til at foretage registrering og opbevaring af oplysninger, der fulgte af logningsdirektivet. Der er grundlæggende tale om registrering og opbevaring af den samme type af oplysninger, dvs. oplysninger, der skaber mulighed for i et vist omfang at få indblik i kommunikationen foretaget af de personer, hvis oplysninger registreres og opbevares, uden at der dog skabes mulighed for at få indblik i indholdet af denne kommunikation.

Formålet med registreringen og opbevaringen af oplysninger efter logningsbekendtgørelsen er desuden det samme som formålet med registrering og opbevaring ifølge logningsdirektivet, dvs. at skabe mulighed for at anvende oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold.

Med udgangspunkt i EU-Domstolens afgørelse vedrørende logningsdirektivet er det derfor Justitsministeriets vurdering, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen udgør et indgreb i retten til privatliv, jf. Charterets artikel 7, og retten til beskyttelse af personoplysninger, jf. Charterets artikel 8.

Det er desuden Justitsministeriets vurdering, at registreringen og opbevaringen af oplysninger i henhold til logningsbekendtgørelsen med henblik på, at oplysningerne kan indgå som led i efterforskning og retsforfølgning

af strafbare forhold, forfølger et sagligt formål, og at registreringen og opbevaringen af oplysninger er egnet til at opnå dette formål.

Særligt for så vidt angår oplysninger registreret som led i sessionslogning, jf. logningsbekendtgørelsens § 5, stk. 1, har erfaringerne dog vist, at oplysningerne kun i meget begrænset omfang er brugbare i praksis i forbindelse med efterforskning og retsforfølgning af strafbare forhold. Det skyldes bl.a., at reglerne er udformet på en måde, der gør det muligt for internetudbyderne at nøjes med at logge hver 500. datapakke, der indgår i en slutbrugers kommunikation på internettet. Endvidere kan internetudbyderne foretage registreringen af internetkommunikationen på kanten til andre net i deres netværk. Der henvises nærmere herom til pkt. 5.5.1.1 i Justitsministeriets redegørelse af 21. december 2012 til Folketingets Retsudvalg om diverse spørgsmål vedrørende logningsreglerne. Det er efter Justitsministeriets opfattelse tvivlsomt, om reglerne om sessionslogning på nuværende tidspunkt og i deres nuværende udformning kan anses for "egnede" til at opnå deres formål (skabe mulighed for anvendelse af oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold). Justitsministeriet vil derfor tage skridt til at ophæve reglerne herom i bekendtgørelsens § 5, stk. 1. Der kan i forlængelse heraf henvises til, at justitsministeren i folketingsåret 2014-15 vil fremsætte et lovforslag om revision af logningsreglerne.

På den anførte baggrund forholder det nedenfor angivne sig ikke til reglerne om sessionslogning efter bekendtgørelsens § 5, stk. 1.

4.4.2. Som anført i pkt. 2 ovenfor er det i forhold til logningsdirektivet EU-Domstolens opfattelse, at indgrebet i de grundlæggende rettigheder beskyttet i Charterets artikel 7 og 8 ikke er tilstrækkeligt afgrænset med henblik på at sikre, at det pågældende indgreb rent faktisk er begrænset til det strengt nødvendige.

Med udgangspunkt i EU-Domstolens treleddede begrundelse for, at Domstolen ikke fandt indgrebet tilstrækkeligt afgrænset, jf. gennemgangen af dommen i pkt. 2 ovenfor, analyseres i det følgende betydningen af dommen i forhold til de gældende danske regler om registreringen af oplysninger (I), adgangen til de registrerede oplysninger (II) og varigheden af opbevaringen af de registrerede oplysninger (III).

I. For så vidt angår *registreringen og opbevaringen* af oplysninger bemærkes, at den registrering og opbevaring, der skal foretages i henhold til log-

ningsbekendtgørelsen, som udgangspunkt svarer til den registrering og opbevaring, der skulle foretages med udgangspunkt i logningsdirektivet. Hertil kommer, at der som anført i pkt. 3 ovenfor på enkelte punkter (mobiltelefoni og sessionslogning og trådløs adgang til internettet) foretages registrering og opbevaring af oplysninger, der går videre end de forpligtelser, der fulgte af logningsdirektivet.

For så vidt angår vurderingen i forhold til Charterets artikel 7 og 8 bemærkes, at registreringen og opbevaringen af oplysninger foretaget i henhold til logningsbekendtgørelsen – på samme generelle vis som registreringen og opbevaringen foretaget i henhold til logningsdirektivet – omfatter alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe kriminalitet.

II. I relation til spørgsmålet om *adgangen* til de oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen, bemærkes, at logningsdirektivet i vidt omfang overlader det til medlemsstaterne at udfylde de materielle og proceduremæssige betingelser for denne adgang, ligesom direktivet også i vidt omfang overlader det til medlemsstaterne at fastsætte de nærmere krav til opbevaringen af oplysningerne.

Som anført i EU-Domstolens dom, præmis 54, må det kræves, at lovgivningen fastsætter klare og præcise regler, således at de personer, hvis oplysninger registreres og opbevares, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger.

Menneskerettighedsdomstolen har i sin afgørelse af 29. juni 2006 i sagen *Weber og Saravia mod Tyskland (54934/00)*, særligt præmis 93-95, taget stilling til forholdet mellem EMRK artikel 8 og hemmelig overvågning af kommunikation med henblik på kriminalitetsbekæmpelse. I den forbindelse bemærkede Menneskerettighedsdomstolen, at det ikke kan kræves af national lovgivning, at den enkelte skal være i stand til at forudse, hvornår vedkommendes kommunikation bliver overvåget. Derimod må det kræves, at national lovgivning er tilstrækkeligt klar for så vidt angår betingelserne for, at hemmelig overvågning af kommunikation kan iværksættes med henblik på at sikre den enkelte mod vilkårlige indgreb i retten til privatliv. Menneskerettighedsdomstolen opsummerede herefter sin retspraksis således:

> "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

Det bemærkes, at der i forbindelse med registrering og opbevaring af oplysninger i henhold til logningsbekendtgørelsen ikke er tale om egentlig hemmelig overvågning (logningen medfører således ikke i sig selv, at politi mv. automatisk får adgang til de opbevarede data), ligesom der heller ikke er tale om overvågning af indholdet af kommunikationen mv. (logningen indebærer således ikke nogen adgang til indholdet af de opbevarede data). Med forbehold herfor må Menneskerettighedsdomstolens afgørelse dog efter Justitsministeriets opfattelse antages at kunne tjene som grundlag for vurderingen af de krav, der må stilles til national lovgivning for så vidt angår adgangen til og opbevaringen af oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen.

Som beskrevet i pkt. 3.2.4 ovenfor er adgangen til de oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen med henblik på at kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold, reguleret i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og kapitel 74 om edition.

For så vidt angår de materielle betingelser for adgangen til registrerede og opbevarede oplysninger i form af indgreb i meddelelseshemmeligheden, skal der særligt henvises til retsplejelovens § 781, der opstiller krav til mistankegrundlaget (mistankekravet), behovet for at foretage indgrebet (indikationskravet) samt til grovheden af den kriminalitet, som mistanken angår (kriminalitetskravet).

For så vidt angår kriminalitetskravet bemærkes, at der som betingelse for indgreb i meddelelseshemmeligheden generelt kræves, at der er tale om kriminalitet af en vis grovhed (strafferamme på mindst 6 års fængsel eller forsætlig overtrædelse af straffelovens kapitel 12 om forbrydelser mod statens selvstændighed og sikkerhed eller straffelovens kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv.).

Overtrædelse af en række andre specifikke bestemmelser i straffeloven og særlovgivningen, herunder udlændingeloven kan dog også begrunde indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 781, stk. 1, nr. 3, stk. 2 og stk. 3.

Som det fremgår af pkt. 3.2.4 ovenfor, er det ved indsættelsen af de særlige bestemmelser i retsplejelovens § 781, stk. 1, nr. 3, generelt forudsat, at der bør sættes snævre grænser for politiets adgang til at foretage indgreb i meddelelseshemmeligheden, at der i forbindelse med overvejelser om at udvide adgangen hertil foretages en overordnet afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv, og at der imidlertid kan vise sig at være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke er tilstrækkelige.

I forbindelse med indsættelse af hver enkelt af de særligt oplistede bestemmelser i retsplejelovens § 781, stk. 1, nr. 3, er der således foretaget en konkret vurdering af behovet for at udvide adgangen til at foretage indgreb i meddelelseshemmeligheden. Behovet begrundes med, at udviklingen af nye kriminalitetsformer i det moderne samfund gør det nødvendigt at tage andre end de sædvanlige efterforskningsmetoder i brug, og at der løbende bør tages stilling til dette behov. Det gælder f.eks., hvor kommunikationsdata er det afgørende bevismiddel eller det helt relevante efterforskningsmiddel, hvor overtrædelsen begås af en flerhed af personer, har karakter af et komplot eller som led i organiseret international kriminalitet, eller hvor overtrædelsen sker ad ren elektronisk vej.

Det bemærkes i forlængelse heraf, at mistankekravet i retsplejelovens § 781, stk. 1, nr. 1, og indikationskravet i stk. 1, nr. 2, samt proportionalitetskravet i § 782 ligeledes finder anvendelse for så vidt angår de særligt oplistede bestemmelser. Der henvises i øvrigt til den nærmere beskrivelse af de materielle betingelser i pkt. 3.2.4 ovenfor.

Ved indhentelse af historiske teleoplysninger skal de materielle betingelser for både editionspålæg, jf. retsplejelovens § 804, og indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 781, være opfyldt.

De proceduremæssige betingelser for adgang til sådanne oplysninger fremgår af retsplejelovens § 783 (krav om retskendelse), § 784 (advokatbeskikkelse for den, som indgrebet vedrører) og § 788 (efterfølgende underretning af den, som indgrebet vedrører).

Også ved indhentelse af andre oplysninger (alene) efter reglerne om edition, jf. retsplejelovens § 804, jf. pkt. 3.2.4.1 ovenfor, gælder der proceduremæssige betingelser, jf. retsplejelovens § 806, herunder krav om retskendelse.

Dansk ret indeholder således klare betingelser for adgangen til oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen[3].

Ud over adgang i form af indgreb i meddelelseshemmeligheden og pålæg om edition efter bestemmelserne i retsplejeloven findes der som nævnt ovenfor i pkt. 3.2.5 på visse områder hjemmel til, at myndigheder kan kræve at få indblik i oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. Således vil både Datatilsynet og Erhvervsstyrelsen kunne kræve at få adgang til oplysninger registreret og opbevaret i henhold til logningsbekendtgørelsen, hvis det måtte være relevant for de pågældende myndigheders tilsynsvirksomhed. Dette vil kun i helt særlige tilfælde være relevant for Datatilsynet, og efter det af Erhvervs- og Vækstministeriet oplyste usandsynligt i forhold til Erhvervsstyrelsen. Endvidere har Skatteministeriet oplyst, at de oplysninger, der i praksis indhentes, er oplysninger, der registreres i henhold til udbudsbekendtgørelsen, og at det er usandsynligt, at SKAT skulle få behov for at indhente oplysninger registreret i henhold til logningsbekendtgørelsen. Efter det oplyste har Skatteministeriet ikke taget stilling til, om sådanne oplysninger i givet fald ville kunne indhentes med hjemmel i skattekontrollovens § 8 D.

For så vidt angår opbevaringen af oplysninger, der er registreret i henhold til logningsbekendtgørelsen, bemærkes, at persondataloven som anført i pkt. 3.4 ovenfor gælder for oplysninger, som registreres og opbevares efter logningsbekendtgørelsen, og at Datatilsynet fører tilsyn med enhver behandling, der omfattes af loven.

Hertil kommer, at der i udbudsbekendtgørelsen er fastsat særlige bestemmelser for teleudbydere, herunder bekendtgørelsens § 23 om sletning eller anonymisering af trafikdata, der også finder anvendelse på trafikdata, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. Det indebærer som nævnt i pkt. 3.3 ovenfor, at oplysninger, som teleudbyderne registrerer og opbevarer alene med det formål at opfylde forpligtelsen i

[3] Justitsministeriet vil i forbindelse med den kommende revision af logningsreglerne nærmere overveje forholdet mellem Danmarks internationale forpligtelser med hensyn til retten til respekt for privatlivet og de krav, der efter retsplejelovens editionsregler gælder i forhold til politiets adgang til visse loggede oplysninger.

henhold til logningsbekendtgørelsen, ikke vil kunne opbevares i mere end 1 år.

Der er således i dansk ret etableret en række garantier vedrørende adgangen til og opbevaringen af oplysninger, der er registreret og opbevaret i henhold til logningsbekendtgørelsen. For så vidt angår adgangen til oplysningerne adskiller de danske regler sig væsentligt fra logningsdirektivet, der i vidt omfang overlod reguleringen af disse spørgsmål til medlemsstaterne.

III. Om *opbevaringsperioden* for oplysninger, der registreres og opbevares i henhold til logningsbekendtgørelsen, bemærkes, at det efter retsplejelovens § 786, stk. 4, påhviler teleudbydere at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. I overensstemmelse hermed fremgår det af logningsbekendtgørelsens § 9, at de registrerede oplysninger skal opbevares i 1 år.

Der henvises til pkt. 3.2.3 ovenfor for en beskrivelse af motiverne bag fastlæggelsen af opbevaringsperioden til 1 år. Som det fremgår heraf, er det udtrykkeligt anført i forarbejderne til lov nr. 378 af 6. juni 2002 (pkt. 3.1.3.1 i de almindelige bemærkninger til lovforslaget), at fastsættelsen af en opbevaringsperiode på 1 år ikke går videre, end hensynet til forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager tilsiger.

Også på dette punkt adskiller dansk ret sig fra logningsdirektivet, idet det i direktivet var overladt til medlemsstaterne selv at fastlægge en opbevaringsperiode på mellem 6 måneder og 2 år. EU-Domstolen fremhævede i den forbindelse bl.a., at det ikke var præciseret i direktivet, at fastsættelsen af lagringsperioden skal være baseret på objektive kriterier for at sikre en begrænsning til det strengt nødvendige, jf. præmis 64.

Det bemærkes desuden, at der som også anført ovenfor gælder en forpligtelse for teleudbyderne i medfør af udbudsbekendtgørelsens § 23 til at slette eller anonymisere oplysninger, der udelukkende er registreret og opbevaret i henhold til logningsbekendtgørelsen, ved udløbet af den 1-årige opbevaringsperiode.

For så vidt angår, hvor længe de registrerede oplysninger skal opbevares, har Danmark således på dette punkt fastsat en klar afgrænsning i lovgivningen baseret på hensynet til efterforskning og kriminalitetsbekæmpelse.

4.5. Det bemærkes endelig, at EU-Domstolen anfører i præmis 66-68, at logningsdirektivet ikke fastsætter tilstrækkelige garantier i forhold til effektiv beskyttelse af lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse data, således som foreskrevet i Charterets artikel 8. Navnlig sikrer direktivet efter Domstolens opfattelse ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden. Direktivet fastsætter endvidere ikke krav om, at lagrede data skal opbevares på EU's område, hvilket kan underminere den uafhængige myndighedskontrol, der skal foretages efter Charterets artikel 8, stk. 3.

4.5.1. Som det fremgår ovenfor under pkt. 3.3, er der på teleområdet i sikkerhedsbekendtgørelsen fastsat sikkerhedskrav til teleudbyderne.

Formålet med sikkerhedsbekendtgørelsen er at sikre en effektiv beskyttelse af data mod risiko for misbrug samt ulovlig adgang til og benyttelse af data. Dette omfatter også data, der er blevet logget efter logningsbekendtgørelsen.

Efter reglerne i sikkerhedsbekendtgørelsen er der bl.a. krav om, at tjenesteudbyderne skal udarbejde en sikkerhedspolitik, der som minimum sikrer, at det kun er en begrænset kreds af personer, som får adgang til persondata til lovlige formål, og at der bl.a. ikke kan ske en ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse af persondata. Endvidere er der – som nærmere redegjort for under pkt. 3.3 – efter udbudsbekendtgørelsens § 23 krav om, at teleudbydere ikke kan opbevare logningsdata ud over logningsperioden på 1 år, idet teleudbyderne efter den nævnte bestemmelse er forpligtet til at slette eller anonymisere dataene.

Hertil kommer, at udbyderne skal overholde persondatalovens regler om fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

Disse sikkerhedskrav og -foranstaltninger er som nævnt ovenfor en gennemførelse af henholdsvis e-data-beskyttelsesdirektivet og databeskyttelsesdirektivet. Dommens præmis 67 må efter Justitsministeriets opfattelse forstås sådan, at der navnlig sigtes til krav om irreversibel destruktion af data. Dette er som nævnt ovenfor opfyldt ved udbudsbekendtgørelsens § 23, hvorefter teleudbyderne ikke kan opbevare oplysninger, der (alene) er logget efter logningsreglerne, ud over logningsperioden på 1 år, hvorefter dataene skal slettes eller anonymiseres.

4.5.2. Særligt i forhold til EU-Domstolens bemærkning om, at logningsdirektivet ikke sikrer, at lagrede data skal opbevares på EU's område, bemærkes, at der i persondatalovens § 27 er fastsat nærmere regler for overførsel af oplysninger til lande uden for EU. Denne bestemmelse gælder også for oplysninger, der er blevet logget efter logningsbekendtgørelsen.

Persondatalovens regler indebærer således, at oplysninger kun må overføres til et tredjeland, hvis dette land sikrer et tilstrækkeligt sikkerhedsniveau, hvis betingelserne i lovens § 27, stk. 3, er opfyldt, hvis Datatilsynet i medfør af § 27, stk. 4, har givet tilladelse til overførslen, eller hvis overførslen sker på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser godkendt af Kommissionen.

Som nævnt ovenfor gælder bestemmelsen i persondatalovens § 27 om overførsel til tredjelande også ved overladelse af personoplysninger til en databehandler samt ved intern brug, f.eks. inden for en koncern.

5. Konklusion

Som det nærmere fremgår under pkt. 2 ovenfor, foretog EU-Domstolen en *samlet* vurdering af, om det indgreb i EU-borgernes rettigheder efter Charterets artikel 7 og 8, som logningsdirektivet indebar, var begrænset til det strengt nødvendige. Domstolen fandt – med henvisning til samtlige i dommen angivne betragtninger – at EU-lovgiver ved ikke at have fastsat klare og præcise regler for medlemsstaterne havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til Charterets artikel 7, 8 og 52, stk. 1, jf. dommens præmis 65 og 69.

Henset til, at dommen er baseret på en samlet vurdering, kan det give anledning til tvivl, hvilken vægt de enkelte led i begrundelsen skal tillægges, og dermed også hvilken betydning dommen i givet fald kan tillægges i forhold til de danske logningsregler.

I og med, at der er tale om en samlet vurdering, kan det forhold, at registreringen og opbevaringen af oplysninger foretaget i henhold til de danske logningsregler – på samme generelle vis som registreringen og opbevaringen foretaget i henhold til logningsdirektivet – omfatter alle personer og alle elektroniske kommunikationsmidler og samtlige trafikdata uden nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om at bekæmpe grov kriminalitet, efter Justitsministeriets opfattelse ik-

ke i sig selv føre til, at de danske regler må anses for at være i strid med Charteret.

Som det fremgår ovenfor, fastsætter den danske lovgivning klare og præcise regler, der indeholder en række væsentlige garantier med henblik på effektivt at beskytte logningsdata mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse data.

Modsat logningsdirektivet indeholder dansk lovgivning en række materielle og proceduremæssige betingelser for adgangen til de registrerede oplysninger. Særligt skal det fremhæves, at adgangen til oplysningerne – som beskrevet ovenfor – sker under iagttagelse af retsplejelovens regler om indgreb i meddelelseshemmeligheden og/eller edition, hvilket medfører, at en række materielle og proceduremæssige krav skal være opfyldt, for at politiet kan få adgang til oplysningerne. Derudover fastsætter de danske logningsregler – modsat direktivet – pligten for teleudbyderne til at opbevare oplysningerne til 1 år. Endelig følger det af udbudsbekendtgørelsen, at oplysninger, der udelukkende er registreret og opbevaret under henvisning til logningsbekendtgørelsen, herefter irreversibelt skal slettes eller anonymiseres.

Samlet set finder Justitsministeriet af de ovenfor anførte grunde, at der ikke er grundlag for at antage, at de gældende danske regler om registrering og opbevaring af oplysninger i henhold til retsplejeloven og logningsbekendtgørelsen og om adgangen til disse oplysninger skulle være i strid med Charterets bestemmelser om retten til respekt for privatliv og familieliv (artikel 7) og ret til beskyttelse af personoplysninger (artikel 8)[4].

[4] Det bemærkes, at som anført ovenfor under pkt. 4.4.1 vil Justitsministeriet tage skridt til at ophæve reglerne om sessionslogning.

Lovforslag nr. **L 193** Folketinget 2014-15

Fremsat den 29. april 2015 af justitsministeren (Mette Frederiksen)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012 og lov nr. 635 af 12. juni 2013, foretages følgende ændring:

1. I *§ 8* ændres »2014-15« til: »2015-16«.

§ 2

Loven træder i kraft den 1. juli 2015.

Justitsmin., j.nr. 2014-5002-0024

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Det påhviler i medfør af en revisionsbestemmelse justitsministeren i folketingsåret 2014-15 at fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Formålet med lovforslaget er at ændre revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4, således at justitsministeren fremsætter forslag om revision af bestemmelsen i folketingsåret 2015-16 frem for 2014-15.

Retsplejelovens § 786, stk. 4, som sammen med den mere detaljerede logningsbekendtgørelse udgør de gældende logningsregler, har til formål at sikre, at tele- og internetoplysninger er tilgængelige hos teleudbyderne, når politiet har brug for at indhente sådanne oplysninger efter retsplejelovens regler om edition og indgreb i meddelelseshemmeligheden.

De danske logningsregler bygger i vidt omfang på direktiv 2006/24/EF af 15. marts 2006 (herefter logningsdirektivet), som blev erklæret ugyldigt ved EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd.

Det er på nuværende tidspunkt ikke endeligt afklaret, om – og i givet fald hvornår – Kommissionen vil fremsætte forslag om nye EU-regler på området.

Justitsministeriet finder på den baggrund, at revisionen af de danske logningsregler bør udsættes med henblik på at afvente en afklaring af dette spørgsmål.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (Anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i et år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Efter bestemmelsen fastsætter justitsministeren efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 af 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det er endvidere i pkt. 1.2 i de almindelige bemærkninger til lovforslaget forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke af selve indholdet af kommunikationen.

Retsplejelovens § 786, stk. 4, har til formål at sikre, at tele- og internetoplysninger er tilgængelige hos teleudbyderne, når politiet har brug for at indhente sådanne oplysninger.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at der indhentes en retskendelse.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslag nr. L 35 af 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 886), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til lovforslag nr. L 217 af 31. marts 2006, jf. Folketingstidende 2005-06, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. logningsdirektivet, som var blevet vedtaget den 15. marts 2006.

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overve-

jelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger til lovforslag nr. L 180 af 24. marts 2010, jf. Folketingstidende 2009-10, Tillæg A, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger til lovforslag nr. L 53 af 14. december 2011, jf. Folketingstidende 2011-12, Tillæg A, side 4, og Retsudvalgets betænkning af 31. maj 2012, Folketingstidende 2011-12, Tillæg B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger til lovforslag nr. L 142 af 6. februar 2013, jf. Folketingstidende 2012-13, Tillæg A, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om sessionslogning efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L142) fra Folketingets Retsudvalg.

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om sessionslogning blev ophævet, jf. nærmere herom pkt. 3.2.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet. Oplysningerne giver dermed mulighed for at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere en række nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. oplysninger om den tildelte brugeridentitet (hvem en IP-adresse tilhører) og tidspunktet for kommunikationens start og afslutning.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde efter logningsreglerne registrere indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester. Det er således ikke muligt for politiet på baggrund af de data, teleudbyderne skal logge efter logningsbekendtgørelsen, at få adgang til oplysninger om indholdet af den tele- eller internetkommunikation, som har været ført. Det bemærkes i den forbindelse, at politiets mulighed for at foretage aflytninger og dermed få adgang til indholdet af kommunikationen alene har et fremadrettet sigte og i øvrigt forudsætter, at retsplejelovens regler om indgreb i meddelelseshemmeligheden er opfyldt.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten i logningsbekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

Logningsbekendtgørelsens bestemmelser er i vidt omfang udtryk for en gennemførelse af det nu ophævede logningsdirektiv.

3. EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. (om logningsdirektivet)

Logningsdirektivet blev ved EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd., erklæret ugyldigt under henvisning til, at EU-lovgiver havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver, henset til artikel 7, 8 og 52, stk. 1, i Den Europæiske Unions Charter om grundlæggende rettigheder (herefter Charteret).

3.1. EU-Domstolens bemærkninger

EU-Domstolen fastslog, at logningsdirektivet indebar et indgreb i de grundlæggende rettigheder, som er fastslået i Charterets artikel 7 (ret til respekt for privatliv og familieliv) og 8 (ret til beskyttelse af personoplysninger). EU-Domstolen lagde i den forbindelse bl.a. vægt på, at direktivet ikke fastsatte klare og præcise regler, der regulerede rækkevidden af indgrebet. Dermed indebar direktivet et indgreb i disse grundlæggende rettigheder, som var meget vidtrækkende og af særligt alvorlig karakter i EU's retsorden, uden at dette indgreb var præcist afgrænset af bestemmelser, der gjorde det muligt at sikre, at det faktisk var begrænset til det strengt nødvendige.

EU-Domstolen fastslog endvidere, at logningsdirektivet ikke fastsatte tilstrækkelige garantier, der gjorde det muligt at sikre en effektiv beskyttelse af data – sådan som det kræves efter artikel 8 i Charteret – mod risikoen for misbrug og mod enhver ulovlig adgang til og benyttelse af disse data.

Endelig bemærkede EU-Domstolen, at logningsdirektivet ikke fastsatte krav om, at dataene skulle lagres inden for EU's område, og at det derfor ikke kunne antages, at det fuldt ud var sikret, at overholdelse af kravene om beskyttelse og sikkerhed kontrolleres af en uafhængig myndighed, som det kræves efter Charterets artikel 8, stk. 3.

For en nærmere redegørelse for EU-Domstolens bemærkninger i dommen af 8. april 2014 henvises til pkt. 2 i Justitsministeriets notat af 2. juni 2014, der blev oversendt til Folketingets Retsudvalg i forbindelse med besvarelsen af udvalgets spørgsmål nr. 919 (Alm. del).

3.2. Dommens betydning for de danske logningsregler

På baggrund af EU-Domstolens dom af 8. april 2014 foretog Justitsministeriet en vurdering af dommens betydning for de danske logningsregler. Der henvises herved til pkt. 4 og 5 i ministeriets notat af 2. juni 2014 om dommen.

For så vidt angår de på det tidspunkt gældende regler om sessionslogning (logning af oplysninger om internetbaseret kommunikation) var det efter Justitsministeriets opfattelse tvivlsomt, om reglerne på daværende tidspunkt og i deres daværende udformning kunne anses for "egnede" til at opnå deres formål (skabe mulighed for anvendelse af oplysningerne som led i efterforskning og retsforfølgning af strafbare forhold). Det skyldtes bl.a., at reglerne var udformet på en måde, der gjorde det muligt for udbyderne at nøjes med at logge hver 500. datapakke, der indgår i en slutbrugers kommunikation på internettet. Endvidere foretog en del udbydere registrering af internetkommunikationen på kanten til andre net i deres netværk i stedet for at logge hver enkelt brugers kommunikation. Det betød, at de oplysninger, der herved blev logget, var meget sporadiske og ikke kunne bruges til at stykke et egentligt billede sammen af den førte kommunikation om for eksempel et gerningstidspunkt. Derfor var reglerne ikke brugbare i praksis.

Justitsministeriet ophævede på den baggrund ved bekendtgørelse nr. 660 af 19. juni 2014 reglerne om sessionslogning i logningsbekendtgørelsen.

For så vidt angår de øvrige regler om registrering og opbevaring af oplysninger i henhold til retsplejeloven og logningsbekendtgørelsen og om adgangen til disse oplysninger fandt Justitsministeriet samlet set, at der ikke var grundlag for at antage, at de gældende danske regler skulle være i strid med Charterets bestemmelser om ret til respekt for privatliv og familieliv (artikel 7) og ret til beskyttelse af personoplysninger (artikel 8).

Justitsministeriet lagde herved bl.a. vægt på, at den danske lovgivning fastsætter klare og præcise regler, der indeholder en række væsentlige garantier med henblik på effektivt at beskytte logningsdata mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse data.

Modsat det nu ugyldige logningsdirektiv indeholder dansk lovgivning således en række materielle og proceduremæssige betingelser for adgangen til de registrerede oplysninger. Særligt skal det fremhæves, at adgangen til oplysningerne sker under iagttagelse af retsplejelovens regler om indgreb i meddelelseshemmeligheden og/eller edition, hvilket medfører, at en række materielle og proceduremæssige krav skal være opfyldt, for at politiet kan få adgang til oplysningerne. Derudover fastsætter de danske logningsregler – modsat direktivet – pligten for teleudbyderne til at opbevare oplysningerne til 1 år. Endelig følger det af udbudsbekendtgørelsen (bekendtgørelse nr. 715 af 23. juni 2011), at oplysninger, der udelukkende er registreret og opbevaret under henvisning til logningsbekendtgørelsen, herefter irreversibelt skal slettes eller anonymiseres.

4. Justitsministeriets overvejelser

EU-Domstolen har ved dom af 8. april 2014 erklæret logningsdirektivet, som de danske logningsregler i vidt omfang bygger på, for ugyldigt. Det er på nuværende tidspunkt ikke endeligt afklaret, om – og i givet fald hvornår – Kommissionen vil fremsætte forslag om nye EU-regler på området.

Justitsministeriet finder, at der er behov for en nærmere afklaring af dette spørgsmål.

Justitsministeriet har i den forbindelse noteret sig, at en række interessenter på området, herunder repræsentanter fra tele- og internetbranchen og interesseorganisationer, har anbefalet Justitsministeriet at udsætte revisionen af de danske logningsregler med henblik på at afvente en afklaring på EU-niveau.

Det foreslås på den baggrund, at revisionen af retsplejelovens § 786, stk. 4, udsættes til folketingsåret 2015-16 med henblik på at afvente en afklaring af, om – og i givet fald hvornår – Europa-Kommissionen vil fremsætte forslag om nye EU-regler på området.

Der foreslås således ikke på nuværende tidspunkt ændringer af retsplejelovens § 786, stk. 4.

Som senest tilkendegivet i forarbejderne til lov nr. 635 af 12. juni 2013, hvor revisionen blev udskudt til folketingsåret 2014-15, vil der i forbindelse med en revision af de danske logningsregler så vidt muligt blive taget stilling til, om der er behov for at registrere og opbevare flere typer af data. Desuden vil Justitsministeriet inddrage relevante myndigheder og organisationer mv., herunder tele- og internetbranchen, i forbindelse med en kommende revision af de danske logningsregler, ligesom de synspunkter mv., som interessenterne på området fremkommer med, vil blive inddraget i overvejelserne.

5. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for det offentlige.

6. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

7. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

8. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

9. Forholdet til EU-retten

Lovforslaget indeholder ikke EU-retlige aspekter.

10. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 16. marts 2015 til den 13. april 2015 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Journalistforbundet, Justitia, Rådet for Digital Sikkerhed, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, ITEK/Dansk Industri, PROSA, SAM-DATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/ Stofa, Lejernes LO og Andelsboligforeningernes Fællesrepræsentation.

11. Sammenfattende skema

	Positive konsekvenser/ Mindreudgifter	Negative konsekvenser/ Merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget indeholder ikke EU-retlige aspekter	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 635 af 12. juni 2013, skal justitsministeren i folketingsåret 2014-15 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2015-16.

Der henvises i øvrigt til lovforslagets almindelige bemærkninger.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2015.

Bilag 1

Lovforslaget sammenholdt med gældende ret

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012 og lov nr. 635 af 12. juni 2013, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2014-15 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2014-15« til: »2015-16«.
	§ 2
	Loven træder i kraft den 1. juli 2015.

Seneste Indlæg (Nyt)

teleindu.dk/ny-logning-pa-vej/

Vi har i dag fået præsenteret Justitsministeriets forslag til nye logningsregler.

Præsentationen kan ses her Nye logningsregler

Vi ved ikke meget mere end det der fremgår af præsentationen. Man påtænker at fremsætte et lovforslag om nye regler allerede i marts 2016.

Det er på flere måder nogle bekymrende meldinger vi fik fra Justitsministeriet i dag. Der er mange uklarheder – af både juridisk, teknisk og økonomisk karakter.

Der er tale om ikke bare en genindførelse af sessionslogningen – men en genindførelse af logningen i en stærkt udvidet form.

Helt grundlæggende er det betænkeligt at fremsætte et forslag om så massiv overvågning af danskerne i lyset af dommen fra EU-domstolen fra 2014, hvor direktivet blev underkendt. Endvidere har man på ingen måde lavet de tekniske analyser om muligheder og begrænsninger – og om det igen bliver en masseindsamling af oplysninger, som ikke har nogen værdi. Man vil altså have mere af det, man tidligere konstaterede var værdiløst. Endelig er vi som telebranche stærkt bekymrede for de økonomiske omkostninger, der følger med de nye regler. Der vil være tale om udgifter til udstyr til flere hundrede millioner kr. og store løbende omkostninger til drift og administration. Det vil helt utvivlsom føre til færre penge til investeringer i bredbånd og bedre mobildækning i Danmark.

Det vil være helt uansvarligt at fremsætte et lovforslag til marts 2016 på et så uklart grundlag. Eneste rigtige beslutning vil være at udsætte revisionen af reglerne.

Vi skal ikke igen gå dansk enegang i EU og gennemføre en indgribende og juridisk stærkt tvivlsom logning, hvor det er vanskeligt at se, hvordan det vil have større værdi end tidligere.

Og vi er i branchen meget spændte på, hvordan regeringen vil kombinere dette med deres løfte om byrdestop for erhvervslivet – og ambitionerne om at sikre bedre bredbånd og mobildækning i hele landet.

Jakob Willer
20102365

FOLKETINGSTIDENDE A

Lovforslag nr. **L 183** Folketinget 2015-16

Fremsat den 27. april 2016 af justitsministeren (Søren Pind)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012 og lov nr. 635 af 12. juni 2013, foretages følgende ændring:

1. I *§ 8* ændres »2014-15« til: »2016-17«.

§ 2

Loven træder i kraft den 1. juli 2016.

Justitsmin., j.nr. 2016-5002-0027

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Det påhviler justitsministeren at fremsætte lovforslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I).

Det påhviler justitsministeren at foretage revisionen i folketingsåret 2014-15, jf. § 1 i lov nr. 635 af 12. juni 2013 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af revisionsbestemmelse).

Retsplejelovens § 786, stk. 4, udgør sammen med den mere detaljerede bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) de gældende logningsregler. Reglerne har til formål at sikre, at en række oplysninger om tele- og internetkommunikation er tilgængelige hos udbyderne, når politiet har brug for at indhente sådanne oplysninger til brug for efterforskning og retsforfølgning af strafbare forhold.

Til brug for revisionen af logningsreglerne har Rigspolitiet fremsat en række anbefalinger, som bygger på politiets hidtidige erfaringer med anvendelsen af reglerne. Et eksternt konsulenthus har med afsæt i Rigspolitiets anbefalinger beregnet de erhvervsøkonomiske konsekvenser, som peger på omstillingsomkostninger for udbyderne i omegnen af en milliard kr. Det overstiger efter Justitsministeriets opfattelse grænsen for det acceptable.

Justitsministeriet har samtidig med beregningen af de erhvervsøkonomiske konsekvenser afholdt møder med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen. På møderne er der blevet etableret en nyttig og konstruktiv dialog om udformningen af fremtidens logningsregler.

Efter Justitsministeriets opfattelse er der ingen tvivl om, at behovet for nye logningsregler er reelt og presserende. Omvendt ønsker ministeriet ikke, at udbyderne pålægges økonomiske byrder for nye logningsregler i en størrelsesorden, som ikke er acceptabel.

Justitsministeriet finder på den baggrund, at revisionen af logningsreglerne bør udsættes med henblik på at fortsætte den gode dialog med udbyderne, således at de nye regler både i tilstrækkelig grad tilgodeser politiets behov, og samtidig ikke pålægger udbyderne unødige økonomiske byrder.

Justitsministeriet vil i tillæg til den igangværende dialog gennemføre en høring af relevante myndigheder, organisationer mv. om deres vurdering og erfaringer med de gældende logningsregler.

2. Logning af oplysninger om tele- og internetkommunikation

2.1. Gældende ret

2.1.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervs- og vækstministeren og energi-, klima- og forsyningsministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 af 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det er endvidere i pkt. 1.2 i de almindelige bemærkninger til lovforslaget forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke af selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.1.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens

kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder blandt andet, at udlevering af oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at der indhentes en retskendelse.

2.1.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslag nr. L 35 af 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til lovforslag nr. L 217 af 31. marts 2006, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger til lovforslag nr. L 180 af 24. marts 2010, jf. Folketingstidende 2009-10, Tillæg A, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger til lovforslag nr. L 53 af 14. december 2011, jf. Folketingstidende 2011-12, Tillæg A, side 4, og Retsudvalgets betænkning af 31. maj 2012, Tillæg B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger til lovforslag nr. L 142 af 6. februar 2013, jf. Folketingstidende 2012-2013, Tillæg A, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger til lovforslag nr. L 193 af 29. april 2015, jf. Folketingstidende 2014-15 (1. samling), Tillæg A, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

2.1.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om internettrafik (sessionlogning) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS-, og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere og opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester. Det er således ikke muligt for politiet på baggrund af de data, teleudbydernes skal logge efter logningsbekendtgørelsen, at få adgang til oplysninger om indholdet af den tele- eller internetkommunikation, som har været ført. Det bemærkes, at der i retsplejeloven findes særskilte regler om politiets adgang til at foretage aflytninger og dermed fremadrettet få adgang til indholdet af tele- og internetkommunikation.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8, kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten i bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.2. Justitsministeriets overvejelser

Det er efter Justitsministeriets opfattelse afgørende, at logningsreglerne sikrer politiet et effektivt redskab til kriminalitetsbekæmpelse. Samtidig er det afgørende, at logningsreglerne respekterer borgernes grundlæggende ret til beskyttelse af privatlivet, og at erhvervslivet ikke pålægges unødige byrder.

Til brug for Justitsministeriets revision af logningsreglerne har Rigspolitiet fremsat en række anbefalinger, som bygger på politiets hidtidige erfaringer med anvendelsen af reglerne.

Rigspolitiet har i den forbindelse oplyst, at det grundlæggende er helt afgørende for politiets efterforskning at have mulighed for at få oplysning om, hvem der har kommunikeret med hvem, i hvilket tidsrum, og hvor de pågældende var på det pågældende tidspunkt, hvad enten der er kommunikeret via tele- eller internettrafik.

Bl.a. henset til, at telekommunikation i stigende grad går fra traditionel telefoni (som er omfattet af den nuværende logningsforpligtelse) til internetbaseret telefoni (som ikke er omfattet), har Rigspolitiet anbefalet, at logningspligten udvides, således at pligten til at logge data om internettrafik kommer til at svare til den gældende pligt til at logge data om traditionel telefonitrafik. Anbefalingerne skal bl.a. imødegå, at politiets efterforskningsmuligheder udhules som følge af den teknologiske udvikling.

Kriminelle og radikaliserede kredse anvender således – i lighed med andre mennesker – i stadig stigende omfang kommunikation via internettet i form af apps, IP-telefoni og chat-funktioner via diverse internetservices mv. i stedet for almindelig telefoni, idet denne teknologi ofte er billigere og mere tilgængelig.

Det er derfor af afgørende betydning for politiets mulighed for at efterforske og retsforfølge alvorlig kriminalitet, at politiet også har adgang til oplysninger om den kommunikation, der foregår på de digitale platforme.

Behovet for loggede oplysninger om internetkommunikation skal endvidere ses i lyset af, at kriminelle i stigende omfang anvender internetbaserede kommunikationsformer med indbyggede krypteringsværktøjer, hvilket gør det sværere for politiet gennem aflytning at gøre sig bekendt med indholdet af en mistænkts kommunikation. Loggede oplysninger om internetkommunikation, som ikke vedrører indholdet af kommunikationen, og som derfor ikke er krypterede, kan i den sammenhæng tjene som et vigtigt alternativt efterforskningsmæssigt redskab for politiet.

Rigspolitiet har endvidere oplyst, at kriminalitetsbilledet i disse år ændrer sig i takt med den teknologiske udvikling, således at den traditionelle kriminalitet falder, mens kriminaliteten på internettet stiger. Stigningen sker både inden for netbedrageri og misbrug af betalingskort og for de mere avancerede og komplicerede kriminalitetstyper som hacking. I sådanne sager er politiets efterforskningsmuligheder helt afhængige af, at der kan findes spor af den datakommunikation, som har været et led i udførelsen af forbrydelsen.

Rigspolitiet anbefaler på den baggrund at udvide teleudbydernes pligt til at logge internetoplysninger, navnlig ved at genindføre regler om logning af oplysninger om internettrafik i en forbedret form, som vil gøre de loggede oplysninger mere anvendelige i politiets efterforskning.

For så vidt angår mobil internettrafik anbefaler Rigspolitiet endvidere, at der logges oplysninger om de celler, den mobile kommunikationsenhed er forbundet til ved kommunikationens start og afslutning, og eventuelle celleskift i løbet af kommunikationen samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen.

Herudover anbefaler Rigspolitiet, at den gældende logningsforpligtelse i det væsentlige fastholdes.

Justitsministeriet har med afsæt i Rigspolitiets anbefalinger fået et eksternt konsulenthus til at beregne anbefalingernes erhvervsmæssige konsekvenser for tele- og internetudbyderne. Konsulenthusets beregninger peger på omstillingsomkostninger for udbyderne i omegnen af en milliard kr. Det overstiger efter Justitsministeriets opfattelse grænsen for det acceptable.

Justitsministeriet har samtidig med beregningen af de erhvervsøkonomiske konsekvenser afholdt møder med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen. På møderne er der blevet etableret en nyttig og konstruktiv dialog om udformningen af fremtidens logningsregler.

Efter Justitsministeriets opfattelse er der ingen tvivl om, at behovet for nye logningsregler er reelt og presserende. Omvendt ønsker ministeriet ikke, at udbyderne pålægges økonomiske byrder for nye logningsregler i en størrelsesorden, som ikke er acceptabel.

Justitsministeriet finder på den baggrund, at revisionen af logningsreglerne bør udsættes med henblik på at fortsætte den gode dialog med udbyderne, således at de nye regler både i tilstrækkelig grad tilgodeser politiets behov, og samtidig ikke pålægger udbyderne unødige økonomiske byrder.

2.3. Den foreslåede ordning

Efter den foreslåede ordning vil justitsministeren i folketingsåret 2016-17 fremsætte forslag om revision af logningsreglerne.

3. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for det offentlige.

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

5. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

6. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

7. Forholdet til EU-retten

Lovforslaget indeholder ikke EU-retlige aspekter.

8. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 21. april 2016 til den 19. maj 2016 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Journalistforbundet, Justitia, Rådet for Digital Sikkerhed, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, ITEK/ Dansk Industri, PROSA, SAM-DATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.

9. Sammenfattende skema

	Positive konsekvenser/mindre-udgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet mv.	Ingen	Ingen
Administrative konsekvenser for erhvervslivet mv.	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Forslaget indeholder ikke EU-retlige aspekter	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 635 af 12. juni 2013, skal justitsministeren i folketingsåret 2014-15 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2016-17.

Der kan i den forbindelse henvises til pkt. 2.2 i de almindelige bemærkninger.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2016.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012 og lov nr. 635 af 12. juni 2013, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2014-15 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2014-15« til: »2016-17«.
	§ 2
	Loven træder i kraft den 1. juli 2016.

BILAG 7

Retsudvalget 2016-17
REU Alm.del endeligt svar på spørgsmål 415
Offentligt

JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Dato: 24. februar 2017
Kontor: Sikkerhedskontoret
Sagsbeh: Niels Dam Dengsøe Petersen
Sagsnr.: 2017-0035-0395
Dok.: 2180093

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmål AA og AB (Alm. del) fra Folketingets Retsudvalg den 2. marts 2017

Samrådsspørgsmål AA:

"Hvad agter den danske regering at foretage sig som reaktion på dommen i Tele2-Watson sagen ved EU-domstolen?"

Samrådsspørgsmål AB:

"Vil ministeren suspendere den logning, der finder sted med hjemmel i den danske logningsbekendtgørelse, indtil lovgivningen er ændret, så lovgivningen ikke er i strid med grundlæggende menneskerettigheder"

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmålene er stillet efter ønske fra Rune Lund (EL).

Svar:

[Indledning]
Tak for ordet.

Temaet for samrådet her i dag er logning. Jeg er blevet stillet 2 samrådsspørgsmål, som begge udspringer af den dom, som EU-Domstolen afsagde kort før jul om de svenske og britiske logningsregler i den såkaldte Tele2-sag.

[Hvad er logning?]
Selvom der de senere år er talt meget om logning – eller måske netop derfor – vil jeg gerne starte med at lige at rekapitulere, hvad logning er, og hvad logning ikke er.

Logning drejer sig om at stille nogle krav til teleudbyderne om opbevaring af oplysninger om deres kunders tele- og internettrafik. Det er navnlig oplysninger om, hvem der kommunikerede med hvem, samt hvor og hvornår kommunikationen fandt sted.

Logning angår derimod ikke indholdet i en kommunikation, f.eks. hvad der bliver sagt i en telefonsamtale, eller hvad der bliver skrevet i en SMS-besked.

Det er vigtigt at holde sig for øje, at hverken politiet eller PET har direkte adgang til loggede oplysninger. Oplysningerne befinder sig hos de danske teleselskaber.

Hvis politiet eller PET skal have adgang til konkrete oplysninger, skal de anmode om det efter retsplejelovens regler. Det betyder bl.a., at der skal indhentes en retskendelse, og at de kun kan få adgang til de specifikke oplysninger, som kendelsen omfatter.

Det er således ikke muligt for politiet og PET løbende at sidde og følge med i, hvem vi taler med, eller hvor vi befinder os.

[EU-Domstolens dom af 21. december 2016]

Med den indledning vil jeg nu vende mig mod det første samrådsspørgsmål: Hvad vil regeringen foretage sig i lyset af Tele2-dommen, der blev afsagt lige før jul?

Jeg skal starte med at understrege, at vi ikke er færdige med at analysere konsekvenserne af dommen i Tele2-sagen for de danske logningsregler.

Der er dog to centrale konklusioner i EU-domstolens dom, som ligger fast allerede på nuværende tidspunkt.

For det første: Ifølge dommen er EU-retten til hinder for en såkaldt "generel og udifferentieret" logning af alle oplysninger. Det vil med andre ord sige, at regler om logning ikke må omfatte alle teleselskabernes kunder til enhver tid.

For det andet: Ifølge dommen er EU-retten ikke til hinder for såkaldt "målrettet" logning af oplysninger med henblik på bekæmpelse af grov kriminalitet eller en fare mod den offentlige sikkerhed.

[Dommens betydning for dansk ret]

De danske regler om logning indebærer i dag, at teleudbyderne skal logge oplysninger om alle deres kunder.

Med visse variationer er det, når vi taler teleoplysninger, også tilfældet i de øvrige EU-lande, der har regler om logning.

Dommen i Tele2-sagen rejser derfor en væsentlig problemstilling i forhold til den måde logningsreglerne i EU-landene er skruet sammen på i dag.

Den problemstilling skal der selvfølgelig findes en løsning på, ikke bare i Danmark, men også i de øvrige berørte lande.

Det skal efter regeringens opfattelse være en løsning, der "målretter" logningen, og som samtidigt sikrer, at politiet i videst muligt omfang har adgang til de loggede oplysninger, som de har brug for i konkrete efterforskninger.

EU-domstolen har ikke taget præcis stilling til, hvordan "målrettede" regler om logning kan se ud.

Derfor er både vi her i Danmark, vores kollegaer i de øvrige EU-lande samt EU-kommissionen i gang med at overveje, hvordan logningsreglerne bør indrettes fremadrettet.

EU-kommissionen har bl.a. for nyligt tilkendegivet, at man vil udarbejde retningslinjer for, hvordan regler om logning fremadrettet kan konstrueres.

Justitsministeriet og Rigspolitiet har desuden – sideløbende med EU-processen – indledt drøftelser med teleselskaberne om de tekniske muligheder for at målrette logningsreglerne. Den viden skal vi selvfølgelig også

have, før vi kan tage stilling til, hvordan vi skal tilpasse logningsreglerne.

Derfor er det bedste svar jeg på nuværende tidspunkt kan give på, hvad regeringen vil foretage sig i lyset af dommen, ret overordnet:

Vi kommer til at lave nogle tilpasninger af logningsreglerne, således at de ikke længere omfatter alle teleselskabernes kunder, men det er for tidligt at sige, hvordan sådanne "målrettede" logningsregler nærmere kommer til at se ud.

Jeg vil dog allerede nu gerne understrege, at det er regeringen magtpåliggende, at politiet og PET har de efterforskningsredskaber, der skal til for at beskytte os.

Logning har i et årti været et centralt efterforskningsredskab i kampen mod alvorlig kriminalitet og terror. Og regeringen vil derfor sikre, at politiet og PET fortsat har adgang til loggede oplysninger i videst muligt omfang.

Jeg skal i den forbindelse også understrege, at regeringsgrundlagets forudsætning om, at kommende regler

om logning også skal omfatte oplysninger om internettrafik, ikke er ændret.

Dommen i Tele2-sagen er således ikke til hinder for, at der indføres regler om logning af internettrafik, så længe disse regler også er målrettede.

[Suspension af reglerne]

Det bringer mig videre til det andet samrådsspørgsmål: Vil regeringen suspendere reglerne om logning her og nu?

Til det spørgsmål kan jeg heldigvis give et klart svar:

Nej.

Vi kommer ikke til at suspendere eller ophæve de gældende logningsregler, uden at vi har et nyt system på plads. Det er loggede oplysninger simpelthen for vigtige til.

Indhentelse af loggede oplysninger er således en fast og velafprøvet del af politiets daglige arbejde med at bekæmpe alvorlig kriminalitet og beskytte os.

Bare for at tage et konkret eksempel, var det noget af det første, som politiet gjorde i forbindelse med angrebet på Krudttønden den 14. februar 2015.

Og vi kan altså ikke få et nyt logningssystem på plads fra dag til dag.

Det skyldes som nævnt bl.a., at vi i samråd med de andre EU-lande og EU-kommissionen stadig er ved at afklare, hvordan nye logningsregler juridisk kan skrues sammen.

Og så skyldes det, at vi skal sikre, at et nyt målrettet logningssystem også rent teknisk kan hænge sammen ude hos teleselskaberne. Det kræver selvfølgelig nogle undersøgelser.

Og så må vi i øvrigt forvente, at telebranchen skal have noget tid til systemtilpasning og opsætning af nyt udstyr.

Det er derfor vores opfattelse, at både vi – og de andre medlemsstater – nødvendigvis må have en vis tid til at tilpasse logningsreglerne i lyset af dommen.

Jeg kan i den forbindelse i øvrigt nævne, at det – så vidt vi ved – kun er i Sverige, der jo som bekendt forelagde sagen for EU-Domstolen, at logningspligten er blevet suspenderet i forhold til teleselskabet Tele2 som følge af dommen.

De andre EU-lande har således – efter det vi har fået oplyst – ikke suspenderet deres logningsregler, mens der arbejdes på en afklaring af mulighederne for at tilpasse systemerne.

Jeg vil for god ordens skyld også nævne, at hverken Danmark eller de andre EU-lande er blevet mødt med et krav fra EU-kommissionen om at suspendere de nationale regler.

Tværtimod har Kommissionen tilkendegivet at ville arbejde konstruktivt for at finde løsninger i samråd med medlemsstaterne. Kommission er således som sagt bl.a. ved at udarbejde et sæt af retningslinjer for, hvordan regler om logning fremadrettet kan skrues sammen.

[Om den fremadrettede proces]

Hvis jeg så skal opsummere og sige lidt om den fremadrettede proces:

Det, vi ser ind i, er, at vi hurtigst muligt skal have afklaret mulighederne for at tilpasse de danske logningsregler i lyset af dommen i Tele2-sagen.

Derefter skal Folketinget tage stilling til et forslag om revision af logningsreglerne, der tager højde for dommen.

Regeringen agter i den forbindelse som nævnt samtidigt at foreslå, at logningsreglerne udvides til at omfatte oplysninger om internettrafik. For den teknologiske udvikling går fortsat kun i en retning: fra traditionel telefoni til internetbaseret kommunikation – og det udhuler de gældende logningsregler.

Det lovforslag forventer vi at kunne være klar til at fremsætte i næste samling.

[Afrunding]

Til sidst vil jeg igen gerne understrege, at logning i et årti har været et centralt efterforskningsredskab for politiet og PET i kampen mod alvorlig kriminalitet og terror.

Det er afgørende for regeringen i den kommende proces at sikre, at det også vil være tilfældet i fremtiden.

Tak for ordet.

BILAG 10

JUSTITSMINISTERIET

Teleindustrien
Att. Direktør Jakob Willer
Axeltorv 6, 3. sal
1609 København V

Dato: 16 MRS. 2017
Kontor: Sikkerhedskontoret
Sagsbeh: Niels Dam Dengsøe Petersen
Sagsnr.: 2017-1924-0633
Dok.: 2240331

Kære Jakob Willer

Lad mig indledningsvis kvittere for din og telebranchens konstruktive tilgang til drøftelserne om nye logningsregler, som har været et væsentligt emne for såvel jer som for Justitsministeriet det seneste år.

Som du ved, har logning i et årti været et centralt efterforskningsredskab for politiet og PET i kampen mod alvorlig kriminalitet og terror, og det har derfor været vigtigt for regeringen at sikre tidssvarende regler på området.

Som du også ved, afsagde EU-Domstolen den 21. december 2016 dom i de forenede sager C-203/15 (*Tele2*) og C-698/15 (*Watson*) (Tele2-sagen) om de britiske og svenske logningsreglers forenelighed med EU-retten.

Dommen i Tele2-sagen nødvendiggør nogle tilpasninger af de gældende danske logningsregler. Jeg ved, at det i den forbindelse har været vigtigt for teleselskaberne at få klarhed over, hvilke regler der skal efterleves i den kommende tid, og hvilken proces vi forventer i forhold til tilpasning af reglerne.

Jeg kan i den anledning oplyse, at det er vigtigt for regeringen, at et lovforslag fremsættes for Folketinget, som tilpasser de gældende danske logningsregler i overensstemmelse med dommen i Tele2-sagen, uden unødigt ophold.

Det er imidlertid ligeledes vigtigt for regeringen, at udformningen af de nye regler sker på et fuldt oplyst grundlag, og at udlægningen af dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Kommissionen. Derfor er Justitsministeriet også i tæt dialog med de øvrige berørte EU-lande og EU-Kommissionen.

Justitsministeriet og Rigspolitiet vil i øvrigt fortsætte den konstruktive dialog med teleselskaberne med henblik på at sikre, at selskabernes indsigt og synspunkter inddrages i arbejdet.

Som jeg også har oplyst offentligt, betyder dette, at vi først forventer at kunne fremsætte et lovforslag om revision af logningsreglerne i den kommende folketingssamling, og at de gældende danske logningsregler opretholdes, indtil tilpasningerne er gennemført.

Det bemærkes i den forbindelse for en god ordens skyld, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. Efter EU-Domstolens praksis skal man blot hurtigst muligt iværksætte foranstaltninger til opfyldelse af en dom.

I forlængelse heraf bemærkes det endvidere, at Højesteret i en dom af 19. januar 2017 i en sag om opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom har fastslået, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser. Udredningsarbejdet om retten til erstatningsferie ved sygdom havde – på samme måde som i denne sag – til formål at tilvejebringe et fyldestgørende beslutningsgrundlag og indebar bl.a. dialog med andre EU-lande om deres opfølgning på dommen.

Lad mig afslutningsvis understrege, at det som justitsminister er mig magtpåliggende at sikre, at politiet og PET har de efterforskningsredskaber, der skal til for at beskytte os alle. Politiets og PETs fortsatte adgang til – efter en retskendelse – at indhente loggede oplysninger fra teleselskaberne er i den forbindelse et centralt element. Samtidigt skal det naturligvis sikres, at reglerne om logning holdes inden for EU-rettens grænser.

Med venlig hilsen

Søren Pape Poulsen

FOLKETINGSTIDENDE A

Lovforslag nr. **L 191** Folketinget 2016-17

Fremsat den 26. april 2017 af justitsministeren Søren Pape Poulsen

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013 og lov nr. 640 af 8. juni 2016, foretages følgende ændring:

1. I *§ 8* ændres »2016-17« til: »2017-18«.

§ 2

Loven træder i kraft den 1. juli 2017.

Justitsmin., j.nr. 2017-5002-0032

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Det påhviler justitsministeren i folketingsåret 2016-17 at fremsætte lovforslag om revision af retsplejelovens § 786, stk. 4, der fastsætter en pligt for teleudbyderne til at registrere og opbevare (logge) oplysninger om tele- og internettrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven mv., som senest ændret ved lov nr. 640 af 8. juni 2016.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler. Logningsreglerne indebærer overordnet set, at en række oplysninger om tele- og internetkommunikation skal registreres og opbevares hos teleudbyderne, således at politiet og Politiets Efterretningstjeneste (PET) til brug for efterforskning og retsforfølgning af strafbare forhold kan indhente nærmere specificerede oplysninger, som de har brug for i konkrete sager. Det er en betingelse for politiets og PETs indhentelse af oplysninger, at myndighederne i hvert enkelt tilfælde indhenter en retskendelse i overensstemmelse med retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden og edition.

EU-Domstolen afsagde den 21. december 2016 dom i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (Tele2-sagen) om de britiske og svenske logningsreglers forenelighed med EU-retten. Justitsministeriet er – ligesom de øvrige EU-lande og EU-Kommissionen – endnu ikke færdig med at udrede Tele2-sagens nærmere konsekvenser for de danske logningsregler, men dommen forventes at indebære, at der vil skulle foretages nogle tilpasninger af logningsreglerne.

Det foreslås på den baggrund, at revisionen af logningsreglerne udskydes til folketingsåret 2017-18 med henblik på, at der i forbindelse med revisionen kan tages højde for dommen i Tele2-sagen.

En udskydelse af ændringen af logningsreglerne til folketingsåret 2017-18 vurderes således at være nødvendig for at kunne tilpasse de danske logningsregler mest hensigtsmæssigt i lyset af dommen i Tele2-sagen. Der er bl.a. behov for en grundig dialog med en række andre berørte EU-lande, der står i samme situation som Danmark, samt EU-Kommissionen om, hvilke muligheder der er for at indrette nationale logningsregler i lyset af dommen i Tele2-sagen. Det er desuden af afgørende betydning, at der er den fornødne tid til at sikre det bedste operationelle resultat for politiet og PET i forbindelse med ændringer af logningsreglerne, der udgør et centralt efterforskningsredskab for myndighederne. Endelig vil en udskydelse af revisionen af logningsreglerne give mulighed for en grundig drøftelse med bl.a. telebranchen om de tekniske muligheder – og de forventede omkostninger – ved at tilpasse logningsreglerne i lyset af Tele2-dommen.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og energi-, klima- og forsyningsministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat den 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke af selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde kræver, at der indhentes en retskendelse.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslag nr. L 35 som fremsat den 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til lovforslag nr. L 217 som fremsat den 31. marts 2006, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2009-10, A, lovforslag nr. L 180 som fremsat den 24. marts 2010, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2011-12, A, lovforslag nr. L 53 som fremsat den 14. december 2011, side 4, og Retsudvalgets betænkning af 31. maj 2012, B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2012-2013, A, lovforslag nr. L 142 som fremsat den 6. februar 2013, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L 142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2014-15 (1. samling), A, lovforslag nr. L 193 som fremsat den 29. april 2015, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17. Baggrunden herfor var, at et eksternt konsulentfirma havde foretaget beregninger vedrørende en række anbefalinger, som Rigspolitiet var fremkommet med til brug for revisionen, som pegede på, at omstillingsomkostninger for udbyderne ved at følge anbefalingerne var i omegnen af en milliard kr. Det oversteg efter Justitsministeriets opfattelse grænsen for det acceptable. Samtidig havde Justitsministeriet indledt en dialog med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen, og ministeriet fandt det hensigtsmæssigt at fortsætte denne dialog, før revisionen blev foretaget. Der henvises til lovens forarbejder (pkt. 2.2 i de almindelige bemærkninger, jf. Folketingstidende 2015-16, A, lovforslag nr. L 183 som fremsat den 27. april 2016, side 4).

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbru-

gere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i lov om elektroniske kommunikationsnet og -tjenesters (teleloven) § 2, nr. 1. Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.4. EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (om de britiske og svenske logningsregler)

I EU-Domstolens dom af 21. december 2016 i Tele2-sagen udtalte Domstolen bl.a., at artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet), sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i EU's charter om grundlæggende rettigheder (Chartret), skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation (præmis 112).

EU-Domstolen udtalte i den forbindelse, at en sådan national lovgivning, der navnlig ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, derfor overskrider det strengt nødvendige og ikke kan anses for at være begrundet i et demokratisk samfund, således som det er påkrævet i henhold til artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7 (ret til respekt for privatliv og familieliv), 8 (ret til beskyttelse af personoplysninger) og 11 (ret til ytrings- og informationsfrihed) (præmis 106 og 107).

Endvidere udtalte EU-Domstolen, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (præmis 108).

EU-Domstolen udtalte, at en sådan national lovgivning for det første skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at be-

skytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige (præmis 109).

Endvidere udtalte EU-Domstolen, at en national lovgivning, der med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet gør det muligt i forebyggende øjemed at lagre trafikdata og lokaliseringsdata, skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds (præmis 110).

For så vidt angår afgrænsningen af en sådan foranstaltning, udtalte EU-Domstolen, at den nationale lovgivning skal være baseret på objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan endvidere sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået (præmis 111).

3. Justitsministeriets overvejelser og den foreslåede ordning

De danske logningsregler indebærer, at teleudbyderne skal foretage logning af en række oplysninger om alle deres kunder, på alle tidspunkter og i hele landet, jf. nærmere herom pkt. 2.3.

Det må derfor forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.4 ovenfor, vil skulle foretages nogle tilpasninger af de danske logningsregler, således at reglerne målrettes. EU-Domstolen har ikke taget stilling til, hvordan målrettede logningsregler nærmere kan udfærdiges.

Justitsministeriet er på den baggrund for tiden ved at udrede, hvordan de danske logningsregler kan tilpasses i lyset af dommen i Tele2-sagen. Et centralt element i den udredning er en dialog med en række andre EU-lande, der står i samme situation som Danmark for så vidt angår spørgsmålet om tilpasning af deres nationale logningsregler.

EU-Kommissionen har desuden tilkendegivet, at Kommissionen – i tæt samarbejde med medlemsstaterne – vil udarbejde retningslinjer for, hvordan medlemsstaterne kan fastsætte nationale logningsregler i overensstemmelse med dommen i Tele2-sagen. EU-Kommissionen har ikke på nuværende tidspunkt tilkendegivet, hvornår disse retningslinjer forventes at foreligge.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2017-18 bl.a. med henblik på at kunne gennemføre en grundig dialog med de andre berørte EU-lande og EU-Kommissionen om, hvordan logningsregler fremadrettet kan indrettes. En udskydelse af revisionen vil desuden give bedre tid at sikre det bedste operationelle resultat for politiet og PET i forbindelse med ændringer af logningsreglerne, der udgør et centralt efterforskningsredskab for myndighederne. Endelig vil en udskydelse af revisionen af logningsreglerne give mulighed for en grundig drøftelse med bl.a. telebranchen om de tekniske muligheder – og de forventede omkostninger – ved at tilpasse logningsreglerne i lyset af dommen i Tele2-sagen.

Det foreslås på den baggrund, at revisionsbestemmelsen i § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven og visse andre love, som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013 og lov nr. 640 af 8. juni 2016, ændres således, at revisionen af logningsreglerne skal foretages i folketingsåret 2017-18.

Der henvises til lovforslagets § 1, nr. 1.

Det bemærkes, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ophæves, før revisionen af logningsreglerne er gennemført.

Det skal i den forbindelse bemærkes, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. Efter EU-Domstolens praksis skal medlemsstaterne blot hurtigst muligt iværksætte foranstaltninger til opfyldelse af en dom.

I forlængelse heraf bemærkes det, at Højesteret i en dom af 19. januar 2017 i en sag om opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom har fastslået, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser, herunder på at tilvejebringe et fyldestgørende beslutningsgrundlag, som bl.a. indebar dialog med andre EU-lande om deres opfølgning på dommen.

Regeringen vil hurtigst muligt fremsætte et lovforslag for Folketinget om tilpasning af de gældende danske logningsregler.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for stat, kommuner og regioner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget har ikke i sig selv EU-retlige konsekvenser. Det bemærkes dog, at det forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen vil skulle foretages nogle tilpasninger af de danske logningsregler, jf. nærmere herom pkt. 2.4 og 3.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 20. marts 2017 til den 18. april 2017 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Journalistforbundet, Justitia, Rådet for Digital Sikkerhed, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, ITEK/ Dansk Industri, PROSA, SAM-DATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Der henvises til pkt. 2.4, 3 og 8.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt X)	JA	NEJ X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 640 af 8. juni 2016, skal justitsministeren i folketingsåret 2016-17 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2017-18.

Der henvises til pkt. 3 i de almindelige bemærkninger i lovforslaget.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2017.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013 og lov nr. 640 af 8. juni 2016, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2016-17 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2016-17« til: »2017-18«.
	§ 2
	Loven træder i kraft den 1. juli 2017.

BILAG 5

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 11. januar 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Jacob Christian Gaard-høje
Sagsnr.: 2017-10-0122
Dok.: 623618

Revision af reglerne om logning

1. Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18 for, at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).

Af pkt. 3 i de almindelige bemærkninger til lovforslag nr. L 191, der lå til grund for lovændringen, fremgår det bl.a. *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, *at* et centralt element i den udredning var en dialog med de andre EU-lande, *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen, og *at* de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.

2. I forbindelse med fremsættelsen af lovforslag nr. L 191 tilkendegav jeg, at logningsreglerne ville blive revideret i indeværende samling. Denne tilkendegivelse var baseret på, at EU-Kommissionen på daværende tidspunkt forventede at udarbejde de ovenfor nævnte retningslinjer i efteråret 2017. Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.

Det er efter min opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

På denne baggrund påtænker jeg i løbet af de kommende måneder at fremsætte et lovforslag for Folketinget om at udskyde revisionen af logningsreglerne til folketingssamlingen 2018/19.

3. Jeg skal for god ordens skyld oplyse, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen fortsat opretholdes indtil revisionen af logningsreglerne er gennemført.

Det kan i den forbindelse bemærkes, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen i en præjudiciel sag vedrørende en anden medlemsstats lovgivning. Efter EU-Domstolens praksis skal medlemsstaterne så hurtigt som muligt iværksætte foranstaltninger til opfyldelse af en dom.

I den foreliggende situation har sagen vist sig at være for kompliceret til, at arbejdet i EU om konsekvenserne af Tele2-sagen har kunnet afsluttes, og at EU-Kommissionen har kunnet udstede de forudsatte retningslinjer om logning. Der foreligger derfor efter Justitsministeriets opfattelse ikke et tilstrækkeligt oplyst grundlag for gennemførelsen af en revision af logningsreglerne i Danmark på nuværende tidspunkt.

Det bemærkes, at EU-Kommissionen er orienteret om, at Danmark såvel som de øvrige berørte medlemslande opretholder deres gældende logningsregler indtil videre, hvilket ikke har givet EU-Kommissionen anledning til bemærkninger.

4. Lad mig afslutningsvis understrege, at det for mig som justitsminister er afgørende, at politiet og PET til enhver tid har de efterforskningsredskaber, der skal til for at beskytte os alle. Politiets og PETs adgang til – efter en retskendelse – at indhente loggede oplysninger fra teleselskaberne er i den forbindelse et centralt element.

Søren Pape Poulsen

/

Jacob Christian Gaardhøje

BILAG 8

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

By email:
First Vice-President Timmermans

Cc:
Vice-President Ansip
Commissioner Avramopoulos
Commissioner Jourova

Copenhagen, 12 January 2018

Dear Vice-President Timmermans,

We write to you and your Commissioner colleagues as representatives of the Danish telecom industry.

As you know, the European Court of Justice on December 21, 2016 issued its judgement that Members States may not impose a general obligation to retain data on providers of electronic communications services. The judgements, C-203/15 and C-698/15, involved legislation in Ireland and Sweden, both of which were comparable to Danish legislation still in force.

In our delivery of telecommunications services, we are obliged under Danish law (specifically, The Data Retention Order) to retain certain telecommunication data for public law enforcement authorities' use.

The Danish Minister of Justice has publicly acknowledged that Danish law is non-compliant with the ECJ verdict, and needs to be adjusted accordingly. In a March 2017 letter, the Danish government has notified the telecom sector that current national data retention rules are expected to be upheld, while the government works to establish legal compliance with the ECJ verdict.

Until this adjustment has taken place, the Danish telecom sector is subject to untenable legal ambiguity. In the initial phase of the process, the Danish government has estimated a reasonable timeline for national legal revision to be approximately one year. However, the government has not met this timeline. No legislative adjustments has been proposed, and no immediate solution is in sight. In explaining the delay, the Danish government has pointed out that implementation of the ECJ ruling must happen in collaboration with other Member

States and the European Commission, and that this process has yet to arrive at a conclusion.

We agree with the importance of data retention rules being consistently implemented across the European Union, both for the sake of citizens and commerce, and therefore urge you, as the Commissioners responsible for a resolution, to treat this as a matter of absolute urgency. We are exposed to legal jeopardy from lawsuits, and unable to respond properly to citizens who demand reasonable clarification of our adherence to the verdicts of the Unions highest court.

We look forward to your response, and remain at your disposal, should you need any additional input towards an expedited resolution of this issue.

Yours sincerely,

Jakob Willer
Director
Telecom Industry Association Denmark
jw@teleindu.dk

Bilag AO
Kammeradvokaten

JUSTITSMINISTERIET

Dato: 15. januar 2018
Kontor: EU-retskontoret
Sagsbeh: Fie Westergren Hendel
Sagsnr.: 2018-614-0189
Dok.: 623223

Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af mundtligt indlæg i EU-Domstolens sag C-207/16, Ministerio Fiscal

1. Indledning

Audiencia provincial de Tarragona, der er en spansk domstol, har i en straffesag om voldeligt røveri forelagt EU-Domstolen præjudicielle spørgsmål om rækkevidden af beskyttelsen i artikel 7 og 8 i EU's Charter om Grundlæggende Rettigheder ("Chartret") om ret til respekt for privat og familieliv og beskyttelse af personoplysninger i relation til udlevering af oplysninger om mobilabonnenter til brug for efterforskning af kriminalitet. Spørgsmålene angår, hvorvidt EU-retten opstiller nærmere betingelser for grovheden af den kriminalitet, der efterforskes eller retsforfølges, for at personoplysningerne kan udleveres til de retshåndhævende myndigheder.

EU-Domstolen har i forbindelse med indkaldelsen til den mundtlige forhandling anmodet deltagerne om at tage stilling til følgende:

1) Hvis indgrebet i de grundlæggende rettigheder ikke kan anses som graverende henset til typen og omfanget af de omhandlede personlysninger, kan hensynet til bekæmpelsen af "simpel" kriminalitet da begrunde, at der med hjemmel i artikel 15, stk. 1, i direktiv 2002/58[1], i lyset af artikel 7, 8 og 52, stk. 1, i Chartret, gives adgang til personoplysningerne.?.

2) Hvis indgrebet i de grundlæggende rettigheder kan betragtes som graverende, hvilke kriterier fastsætter EU-retten da for medlemsstaternes skøn

[1] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juni 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

over, hvad der anses for grov kriminalitet i henhold til artikel 15, stk. 1, i direktiv 2002/58, set i lyset af artikel 7, 8 og 52, stk. 1, i Chartret?

2. Sagens faktiske omstændigheder

Det spanske politi anmodede i forbindelse med efterforskningen af et voldeligt røveri mod en navngiven person en spansk forundersøgelsesdommer om tilladelse til at indhente oplysninger fra forskellige teleoperatører. Teleoperatørerne skulle udlevere personoplysninger om indehaverene og brugerne af de SIM-kort, der havde været aktiveret via den fra offeret stjålne telefon inden for en af politiet nærmere afgrænset periode.

Politiets anmodning blev afvist af den spanske forundersøgelsesdommer. Forundersøgelsesdommeren lagde vægt på, dels at oplysningerne ikke kunne anses for særligt egnede til opklaring af røveriet, dels at forbrydelsen ikke fandtes at være tilstrækkelig grov i henhold til spansk lovgivning.

Den spanske anklagemyndighed appellerede afgørelsen om afvisning til den forelæggende ret. Den spanske lovgivning var i mellemtiden blevet ændret således, at de oplysninger, politiet ønskede udleveret, kunne udleveres i forbindelse med efterforskning eller retsforfølgning af kriminalitet med en straframme på mindst 3 år. Den forelæggende ret har i forbindelse med behandlingen af sagen forelagt præjudicielle spørgsmål for EU-Domstolen.

Spørgsmålene angår, om EU-retten opstiller betingelser for grovheden af den kriminalitet, der efterforskes, for at personoplysninger om mobilabonnenter kan udleveres til de retshåndhævende myndigheder. Den forelæggende ret ønsker svar på, om det er tilstrækkeligt alene at tillægge strafferammen for den begåede kriminalitet betydning ved afgørelsen af, om der er tale om grov kriminalitet, herunder om en straframme på tre års fængsel er tilstrækkelig til, at oplysningerne kan udleveres i overensstemmelse med EU-retten.

Det bemærkes, at EU-Domstolen til brug for besvarelsen af de præjudicielle spørgsmål har anmodet den spanske regering om skriftligt at redegøre nøjagtigt for hvilke personoplysninger, hovedsagen angår. Domstolen ønsker navnlig bekræftet, om der alene er tale om navn og adresse på indehaverne af de SIM-kort, som er blevet aktiveret via den i hovedsagen stjålne mobiltelefon, eller om der er tale om samtlige oplysninger, som er opbevaret af teleudbydere i forhold til disse SIM-kort, f.eks. data knyttet til udført kommunikation og lokationsdata.

3. Den danske interesse i sagerne

Regeringen vil afgive indlæg i denne sag, idet myndighedernes adgang til loggede oplysninger også i Danmark har sammenhæng med grovheden af den kriminalitet, der efterforskes eller retsforfølges i den enkelte sag. Myndighedernes adgang til loggede oplysninger, der udgør indgreb i meddelelseshemmeligheden, afhænger endvidere som udgangspunkt i Danmark – ligesom det generelt er tilfældet i Spanien – af straframmen for kriminaliteten.

Domstolens besvarelse af de af Audiencia provincial de Tarragona forelagte præjudicielle spørgsmål kan derfor have betydning for vurderingen af den danske lovgivning i forhold til bl.a. Chartrets artikel 7 og 8.

Regeringen vil argumentere for, at de oplysninger, som hovedsagen – efter det af den forelæggende ret oplyste – vedrører, bør kunne udleveres til de retshåndhævende myndigheder til brug for bekæmpelse af enhver form for kriminalitet og ikke blot grov kriminalitet.

Regeringen vil endvidere anføre, at EU-retten ikke stiller – og ikke kan stille – krav om, hvad der udgør tilstrækkelig grov kriminalitet til, at der i en situation, der vedrører loggede trafik- og lokationsoplysninger, kan ske udlevering til de retshåndhævende myndigheder som led i efterforskning og retsforfølgning, idet dette efter regeringens opfattelse er op til de enkelte medlemsstater at fastlægge i national ret.

BILAG 6

JUSTITSMINISTERIET

Dato: 9. februar 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Rune Werner Christensen
Sagsnr.: 2018-731-0024
Dok.: 646431

Forslag
til
Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige
(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016 og lov nr. 673 af 8. juni 2017, foretages følgende ændring:

1. I *§ 8* ændres »2017-18« til: »2018-19«.

§ 2

Loven træder i kraft den 1. juli 2018.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Det påhviler justitsministeren i folketingsåret 2017-18 at fremsætte lovforslag om revision af retsplejelovens § 786, stk. 4, der fastsætter en pligt for teleudbyderne til at registrere og opbevare (logge) oplysninger om tele- og internettrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven mv., som senest ændret ved lov nr. 673 af 8. juni 2017.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler. Logningsreglerne indebærer overordnet set, at en række oplysninger om tele- og internetkommunikation skal registreres og opbevares hos teleudbyderne, således at politiet og Politiets Efterretningstjeneste (PET) til brug for efterforskning og retsforfølgning af strafbare forhold kan indhente nærmere specificerede oplysninger, som de har brug for i konkrete sager. Det er en betingelse for politiets og PETs indhentelse af oplysninger, at myndighederne i hvert enkelt tilfælde indhenter en retskendelse i overensstemmelse med retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden og edition.

Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18 for, at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).

Af pkt. 3 i de almindelige bemærkninger til lovforslag nr. L 191, der lå til grund for lov nr. 673 af 8. juni 2017, fremgår det bl.a. *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, *at* et centralt element i den udredning var en dialog med de andre EU-lande, *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale

logningsregler i lyset af dommen i Tele2-sagen, og *at* de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.

Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.

Det er efter Justitsministeriets opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

Det foreslås på den baggrund, at revisionen af logningsreglerne udskydes til folketingsåret 2018/19.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og energi-, klima- og forsyningsministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat den 13. december 2001,

jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke af selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde kræver, at der indhentes en retskendelse.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslag nr. L 35 som fremsat den 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til lovforslag nr. L 217 som fremsat den 31. marts 2006, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts

2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2009-10, A, lovforslag nr. L 180 som fremsat den 24. marts 2010, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2011-12, A, lovforslag nr. L 53 som fremsat den 14. december 2011, side 4, og Retsudvalgets betænkning af 31. maj 2012, B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2012-2013, A, lovforslag nr. L 142 som fremsat den 6. februar 2013, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L 142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2014-15 (1. samling), A, lovforslag nr. L 193 som fremsat den 29. april 2015, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17. Baggrunden herfor var, at et eksternt konsulentfirma havde foretaget beregninger vedrørende en række anbefalinger, som Rigspolitiet var fremkommet med til brug for revisionen, som pegede på, at omstillingsomkostninger for udbyderne ved at følge anbefalingerne var i omegnen af en milliard kr. Det oversteg efter Justitsministeriets opfattelse grænsen for det acceptable. Samtidig havde Justitsministeriet indledt en dialog med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen, og ministeriet fandt det hensigtsmæssigt at fortsætte denne dialog, før revisionen blev foretaget. Der henvises til lovens forarbejder (pkt. 2.2 i de almindelige bemærkninger, jf. Folketingstidende 2015-16, A, lovforslag nr. L 183 som fremsat den 27. april 2016, side 4).

Ved lov nr. 673 af 8. juni 2017 blev revisionen udskudt til folketingsåret 2017-18. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2016-17, A, lovforslag nr. L 191 som fremsat den 26. april 2017, side 6-7) navnlig, *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.4 nedenfor, *at* et centralt element i den udredning var en dialog med de andre EU-lande, og *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen.

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller –tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i lov om elektroniske kommunikationsnet og -tjenesters (teleloven) § 2, nr. 1. Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.4. EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (om de britiske og svenske logningsregler)

I EU-Domstolens dom af 21. december 2016 i Tele2-sagen udtalte Domstolen bl.a., at artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet), sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i EU's charter om grundlæggende rettigheder (Chartret), skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende

samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation (præmis 112).

EU-Domstolen udtalte i den forbindelse, at en sådan national lovgivning, der navnlig ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, derfor overskrider det strengt nødvendige og ikke kan anses for at være begrundet i et demokratisk samfund, således som det er påkrævet i henhold til artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7 (ret til respekt for privatliv og familieliv), 8 (ret til beskyttelse af personoplysninger) og 11 (ret til ytrings- og informationsfrihed) (præmis 106 og 107).

Endvidere udtalte EU-Domstolen, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (præmis 108).

EU-Domstolen udtalte, at en sådan national lovgivning for det første skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige (præmis 109).

Endvidere udtalte EU-Domstolen, at en national lovgivning, der med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet gør det muligt i forebyggende øjemed at lagre trafikdata og lokaliseringsdata, skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds (præmis 110).

For så vidt angår afgrænsningen af en sådan foranstaltning, udtalte EU-Domstolen, at den nationale lovgivning skal være baseret på objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan endvidere sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået (præmis 111).

3. Justitsministeriets overvejelser og den foreslåede ordning

Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18 for, at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).

Af pkt. 3 i de almindelige bemærkninger til lovforslag nr. L 191, der lå til grund for lov nr. 673 af 8. juni 2017, fremgår det bl.a. *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, *at* et centralt element i den udredning var en dialog med de andre EU-lande, *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen, og *at* de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.

Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.

Det er efter Justitsministeriets opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2018-19.

Det foreslås på den baggrund, at revisionsbestemmelsen i § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven og visse andre love, som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016 og lov nr. 673 af 8. juni 2017, ændres således, at revisionen af logningsreglerne skal foretages i folketingsåret 2018-19.

Der henvises til lovforslagets § 1, nr. 1.

Det bemærkes, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ophæves, før revisionen af logningsreglerne er gennemført.

Det skal i den forbindelse bemærkes, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. Efter EU-Domstolens praksis skal medlemsstaterne blot hurtigst muligt iværksætte foranstaltninger til opfyldelse af en dom.

I den foreliggende situation har sagen vist sig at være for kompliceret til, at arbejdet i EU om konsekvenserne af Tele2-sagen har kunnet afsluttes, og at EU-Kommissionen har kunnet udstede de forudsatte retningslinjer om logning. Der foreligger derfor efter Justitsministeriets opfattelse ikke et tilstrækkeligt oplyst grundlag for gennemførelsen af en revision af logningsreglerne i Danmark på nuværende tidspunkt.

Højesteret har i en dom af 19. januar 2017 i en sag om opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom fundet, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser og tilvejebringe et fyldestgørende beslutningsgrundlag, herunder ved at undersøge opfølgningen i andre lande på dommen. Først efter at der var udarbejdet et fyldestgørende beslutningsgrundlag, der pegede på, at der skulle foretages en ifølge Højesteret afgrænset og relativ enkel ændring af ferieloven, var de danske myndigheder forpligtet til at fremsætte et lovforslag om at ændre ferieloven hurtigst muligt.

Det bemærkes, at EU-Kommissionen er orienteret om, at Danmark såvel som de øvrige berørte medlemslande opretholder deres gældende lognings-regler indtil videre, hvilket ikke har givet EU-Kommissionen anledning til bemærkninger.

Regeringen vil hurtigst muligt fremsætte et lovforslag for Folketinget om tilpasning af de gældende danske logningsregler.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for stat, kommuner og regioner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget har ikke i sig selv EU-retlige konsekvenser. Det bemærkes dog, at det forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen vil skulle foretages nogle tilpasninger af de danske logningsregler, jf. nærmere herom pkt. 2.4 og 3.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 9. februar 2018 til 9. marts 2018 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigfor-

eningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten , Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Dansk Journalistforbund, Justitia, Rådet for Digital Sikkerhed, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, DI Digital, PROSA, SAM-DATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.

10. Sammenfattende skema

	Positive konsekvenser/mindre-udgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet mv.	Ingen	Ingen
Administrative konsekvenser for erhvervslivet mv.	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Der henvises til pkt. 2.4, 3 og 8.	
Overimplementering af EU-retlige minimumsforpligtelser (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 673 af 8. juni 2017, skal justitsministeren i folketingsåret 2017-18 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2018-19.

Der henvises til pkt. 3 i de almindelige bemærkninger i lovforslaget.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2018.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016 og lov nr. 673 af 8. juni 2017, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2017-18 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2017-18« til: »2018-19«.
	§ 2
	Loven træder i kraft den 1. juli 2018.

BILAG 9

EUROPEAN COMMISSION
Office of the First Vice-President Mr Frans Timmermans

Member of Cabinet

Brussels, 08. 03. 2018
CA.02 MaS/mp – SV 1064110

Dear Mr Willer,

I refer to your letter of 12 January 2018 in which you share the concerns of the Danish telecom industry about your continued obligation to retain communications data under Denmark's current data retention law in light of the ruling issued by the Court of Justice of the European Union in the "Tele2/Watson" case[1].

The Commission is fully aware of the significance of the Tele2 ruling and its consequences on national data retention legislation, including the need to ensure the protection of privacy and the confidentiality of communications. At the same time, the importance of data retention as an essential component enabling law enforcement authorities to effectively fight crime, including cybercrime, must also be recognised.

This is why, since the Tele2 ruling was delivered, the Commission has been involved in discussions, first of all, primarily with the Member States and the relevant EU agencies, to examine possible ways forward which would satisfactorily meet the Court's Tele2 criteria and law enforcement's operational requirements. The issues raised in these discussions are wide-ranging which is why the assessment on the way forward is still ongoing.

Let me assure you that the Commission is treating this issue with the close attention it deserves. Our commitment is to continue engaging with all relevant stakeholders and doing all we can to find viable, workable and legally sound solutions on this complex subject.

Yours sincerely,

MaartenS MIT

Mr Jakob Willer
Director
Telecom Industry Association Denmark
E-mail: jw@teleindu.dk

[1] Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and others, ECLI:EU:C:2016:970, 21 December 2016.

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium .
Office: BERL 1 2/243. Phone: direct line (32-2) 2951121.
E-mail: maarte n.smit@ec.europa.eu

FOLKETINGSTIDENDE A

Lovforslag nr. **L 218** Folketinget 2017-18

Fremsat den 11. april 2018 af justitsministeren (Søren Pape Poulsen)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006 og senest ved lov nr. 673 af 8. juni 2017, foretages følgende ændring:

1. I *§ 8* ændres »2017-18« til: »2018-19«.

§ 2

Loven træder i kraft den 1. juli 2018.

Justitsmin., j.nr. 2018-731-0024

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Det påhviler justitsministeren i folketingsåret 2017-18 at fremsætte lovforslag om revision af retsplejelovens § 786, stk. 4, der fastsætter en pligt for teleudbyderne til at registrere og opbevare (logge) oplysninger om tele- og internettrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven mv., som senest ændret ved lov nr. 673 af 8. juni 2017.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler. Logningsreglerne indebærer overordnet set, at en række oplysninger om tele- og internetkommunikation skal registreres og opbevares hos teleudbyderne, således at politiet og Politiets Efterretningstjeneste (PET) til brug for efterforskning og retsforfølgning af strafbare forhold kan indhente nærmere specificerede oplysninger, som de har brug for i konkrete sager. Det er en betingelse for politiets og PETs indhentelse af oplysninger, at myndighederne i hvert enkelt tilfælde indhenter en retskendelse i overensstemmelse med retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden og edition.

Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18, for at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).

Baggrunden for udskydelsen var bl.a., *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, *at* et centralt element i den udredning var en dialog med de andre EU-lande, *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen, og *at* de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.

Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.

Det er efter Justitsministeriets opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

Det foreslås på den baggrund, at revisionen af logningsreglerne udskydes til folketingsåret 2018/19.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og energi-, forsynings- og klimaministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat den 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at udbyderne alene skal logge

oplysninger om trafikdata og ikke om selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde kræver, at der indhentes en retskendelse.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til lovforslag nr. L 35 som fremsat den 13. december 2001, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til lovforslag nr. L 217 som fremsat den 31. marts 2006, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2009-10, A, lovforslag nr. L 180 som fremsat den 24. marts 2010, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2011-12, A, lovforslag nr. L 53 som fremsat den 14. december 2011, side 4, og Retsudvalgets betænkning af 31. maj 2012, B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2012-2013, A, lovforslag nr. L 142 som fremsat den 6. februar 2013, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L 142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2014-15 (1. samling), A, lovforslag nr. L 193 som fremsat den 29. april 2015, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17. Baggrunden herfor var, at et eksternt konsulentfirma havde foretaget beregninger vedrørende en række anbefalinger, som Rigspolitiet var fremkommet med til brug for revisionen, som pegede på, at omstillingsomkostninger for udbyderne ved at følge anbefalingerne var i omegnen af en milliard kr. Det oversteg efter Justitsministe-

riets opfattelse grænsen for det acceptable. Samtidig havde Justitsministeriet indledt en dialog med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen, og ministeriet fandt det hensigtsmæssigt at fortsætte denne dialog, før revisionen blev foretaget. Der henvises til lovens forarbejder (pkt. 2.2 i de almindelige bemærkninger, jf. Folketingstidende 2015-16, A, lovforslag nr. L 183 som fremsat den 27. april 2016, side 4).

Ved lov nr. 673 af 8. juni 2017 blev revisionen udskudt til folketingsåret 2017-18. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2016-17, A, lovforslag nr. L 191 som fremsat den 26. april 2017, side 6-7) navnlig, *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.4 nedenfor, *at* et centralt element i den udredning var en dialog med de andre EU-lande, og *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen.

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i lov om elektroniske kommunikationsnet og -tjenesters (teleloven) § 2, nr. 1. Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.4. EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (om de britiske og svenske logningsregler)

I EU-Domstolens dom af 21. december 2016 i Tele2-sagen udtalte Domstolen bl.a., at artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet), sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i EU's charter om grundlæggende rettigheder (Chartret), skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation (præmis 112).

EU-Domstolen udtalte i den forbindelse, at en sådan national lovgivning, der navnlig ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, derfor overskrider det strengt nødvendige og ikke kan anses for at være begrundet i et demokratisk samfund, således som det er påkrævet i henhold til artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7 (ret til respekt for privatliv og familieliv), 8 (ret til beskyttelse af personoplysninger) og 11 (ret til ytrings- og informationsfrihed) (præmis 106 og 107).

Endvidere udtalte EU-Domstolen, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (præmis 108).

EU-Domstolen udtalte, at en sådan national lovgivning for det første skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige (præmis 109).

Endvidere udtalte EU-Domstolen, at en national lovgivning, der med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet gør det muligt i forebyggende øjemed at lagre trafikdata og lokaliseringsdata, skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds (præmis 110).

For så vidt angår afgrænsningen af en sådan foranstaltning, udtalte EU-Domstolen, at den nationale lovgivning skal være baseret på objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan endvidere sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået (præmis 111).

3. Justitsministeriets overvejelser og den foreslåede ordning

Ved lov nr. 673 af 8. juni 2017 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2017/18 for, at der kunne tages højde for EU-Domstolens dom af 21. december 2016 om de britiske og svenske logningsreglers forenelighed med EU-retten (Tele2-sagen).

Af pkt. 3 i de almindelige bemærkninger til loven, jf. Folketingstidende 2016-17, A, lovforslag nr. L 191 som fremsat den 26. april 2017, side 6-7, fremgår det bl.a. *at* Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af Tele2-sagen, *at* et centralt element i den udredning var en dialog med de andre EU-lande, *at* EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen, og *at* de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ville blive ophævet, før revisionen af logningsreglerne er gennemført.

Kommissionen har imidlertid endnu ikke færdiggjort arbejdet med de nævnte retningslinjer. Ifølge den seneste tilkendegivelse fra Kommissionen vil retningslinjerne foreligge i løbet af 2018.

Det er efter Justitsministeriets opfattelse afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekven-

ser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og PET samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2018-19.

Det foreslås på den baggrund, at revisionsbestemmelsen i § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven og visse andre love, som ændret ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016 og lov nr. 673 af 8. juni 2017, ændres således, at revisionen af logningsreglerne skal foretages i folketingsåret 2018-19.

Der henvises til lovforslagets § 1, nr. 1.

Det bemærkes, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen ikke ophæves, før revisionen af logningsreglerne er gennemført.

Det skal i den forbindelse bemærkes, at der ikke er nogen bestemt EU-retlig frist for, hvor hurtigt medlemsstaterne skal tage højde for en dom fra EU-Domstolen. Efter EU-Domstolens praksis skal medlemsstaterne blot hurtigst muligt iværksætte foranstaltninger til opfyldelse af en dom.

I den foreliggende situation har sagen vist sig at være for kompliceret til, at arbejdet i EU om konsekvenserne af Tele2-sagen har kunnet afsluttes, og at EU-Kommissionen har kunnet udstede de forudsatte retningslinjer om logning. Der foreligger derfor efter Justitsministeriets opfattelse ikke et tilstrækkeligt oplyst grundlag for gennemførelsen af en revision af logningsreglerne i Danmark på nuværende tidspunkt.

I forlængelse heraf bemærkes, at Højesteret i en dom af 19. januar 2017 i en sag om opfølgning på en dom fra EU-Domstolen om ret til erstatningsferie ved sygdom har fundet, at det var velbegrundet, at de danske myndigheder brugte et års tid på at udrede dommens nærmere konsekvenser og tilvejebringe et fyldestgørende beslutningsgrundlag, herunder ved at undersøge opfølgningen i andre lande på dommen. Først efter at der var udarbejdet et fyldestgørende beslutningsgrundlag, der pegede på, at der skulle foretages en ifølge Højesteret afgrænset og relativ enkel ændring af ferieloven, var de danske myndigheder forpligtet til at fremsætte et lovforslag om at ændre ferieloven hurtigst muligt.

Det bemærkes, at EU-Kommissionen er orienteret om, at Danmark såvel som de øvrige berørte medlemslande opretholder deres gældende logningsregler indtil videre, hvilket ikke har givet EU-Kommissionen anledning til bemærkninger.

Regeringen vil hurtigst muligt fremsætte et lovforslag for Folketinget om tilpasning af de gældende danske logningsregler.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget har ingen økonomiske eller administrative konsekvenser for stat, kommuner og regioner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget har ikke i sig selv EU-retlige konsekvenser. Det bemærkes dog, at det forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen vil skulle foretages nogle tilpasninger af de danske logningsregler, jf. nærmere herom pkt. 2.4 og 3.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 9. februar 2018 til 9. marts 2018 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten ¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet,

Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Dansk Journalistforbund, Justitia, Rådet for Digital Sikkerhed, Retssikkerhedsfonden, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, DI Digital, PROSA, SAM-DATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget har ikke i sig selv EU-retlige konsekvenser. Der henvises til pkt. 8.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering /Går videre end minimumskrav i EU-regulering (sæt X)	JA	NEJ X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 673 af 8. juni 2017, skal justitsministeren i folketingsåret 2017-18 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2018-19.

Der henvises til pkt. 3 i de almindelige bemærkninger i lovforslaget.

Til § 2

Det foreslås, at loven træder i kraft den 1. juli 2018.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006 og senest ved lov nr. 673 af 8. juni 2017, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2017-18 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2017-18« til: »2018-19«.

JUSTITSMINISTERIET

Dato: 29. november 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Michael Hadberg
Sagsnr.: 2018-614-0611
Dok.: 927908

Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i EU-Domstolens sag C-520/18, Ordre des barreaux francophones et germanophone m.fl.

1. Indledning

Cour constitutionnelle (Forfatningsdomstolen) i Belgien har i en sag om annullation af en lov om indsamling og lagring af data i den elektroniske kommunikationssektor forelagt EU-Domstolen tre præjudicielle spørgsmål vedrørende de EU-retlige rammer for nationale bestemmelser, der forpligter teleudbydere mv. at lagre trafik- og lokaliseringsdata. Af de tre forelagte spørgsmål er navnlig to af interesse i dansk kontekst.

Det første spørgsmål af interesse angår, hvorvidt artikel 15, stk. 1, i direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor, sammenholdt med bestemmelserne i Den Europæiske Unions charter om grundlæggende rettigheder (Chartret), er til hinder for en national lovgivning, der fastsætter en generel pligt for operatører og udbydere af elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata, når lovgivningen har til formål bl.a. at sikre den personlige og nationale sikkerhed, som staten har en positiv forpligtelse til at sikre for alle borgere, og reglerne indeholder præcise garantier vedrørende lagring af data og adgangen dertil.

Det andet spørgsmål af interesse angår, hvorvidt den belgiske forfatningsdomstol – hvis domstolen på baggrund af besvarelsen af de to første spørgsmål finder, at den anfægtede lov er i strid med EU-retten – midlertidigt kan opretholde virkningerne af denne lov med henblik på at undgå retsusikkerhed og muliggøre, at data, der allerede er indsamlet og lagret, fortsat kan anvendes.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

2. Sagens faktiske omstændigheder

En række sagsøgere har ved en sag anlagt ved den belgiske forfatningsdomstol gjort gældende, at den belgiske lovgivning, der pålægger udbydere af elektronisk kommunikation en generel pligt til i en vis periode at lagre trafik- og lokationsdata (logning), er uforenelig med EU-retten.

Baggrunden for søgsmålet er EU-Domstolens dom af 21. december 2016 i de forenede sager Tele2/Sverige og Watson, C-203/15 og C-698/15 (Store Afdeling), hvori det bl.a. blev fastslået, at de svenske regler om logning var i strid med direktiv 2002/58 sammenholdt med Chartret, idet de medførte en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

Sagsøgerne i den nationale sag gør med støtte i EU-Domstolens dom i Tele2-sagen i det væsentlige gældende, at den belgiske lovgivning, er i strid med EU-retten, fordi den fastsætter en sådan generel pligt til udifferentieret logning, som EU-Domstolen underkendte i Tele2-sagen.

Den belgiske regering har heroverfor i det væsentlige gjort gældende, at den anfægtede lov har et bredere formål end de regler, der var genstand for EU-Domstolens bedømmelse i Tele2-sagen, hvorfor konklusionerne i denne sag ikke kan overføres til den belgiske lovgivning. Den belgiske lovs formål er således ikke alene bekæmpelsen af grov kriminalitet, men også at garantere det strafferetlige systems integritet og forbedre borgernes tillid til retsvæsenets funktionsdygtighed.

Den belgiske regering har endvidere henvist til, at det ganske simpelt er umuligt på forhånd at foretage en sondring mellem personer, tidsmæssige perioder og geografiske områder i forhold til en pligt til at foretage logning, som EU-Domstolen lagde op til i Tele2-sagen.

Det bemærkes i øvrigt, at der ligeledes er forelagt en fransk sag for Domstolen, der omhandler tilsvarende problemstilling (sag C-511/18 og C-512/18, La Quadrature du Net m.fl.).

3. Den danske interesse i sagen

Det er regeringens opfattelse, at regeringen bør afgive indlæg i denne sag, da EU-Domstolens besvarelse af de forelagte spørgsmål vil kunne have betydning for medlemsstaternes mulighed for at pålægge teleselskaber at

gemme og opbevare oplysninger om tele- og internettrafik (logning) til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

De danske regler om logning skal som konsekvens af EU-Domstolens afgørelse i Tele2-sagen revideres. Tele2-dommen efterlader imidlertid væsentlig fortolkningstvivl i forhold til, hvorledes nationale bestemmelser om logning kan indrettes i overensstemmelse med direktiv 2002/58 og Chartret. Der har således siden foråret 2017 været løbende drøftelser i regi af Rådet om, hvordan medlemsstaterne kan indrette de nationale regler i lyset af dommen.

Domstolens besvarelse af de forelagte spørgsmål kan derfor få stor betydning for, hvordan logningsregler kan indrettes i overensstemmelse med EU-retten på en måde, hvor logning fortsat vil udgøre et centralt og effektivt efterforskningsredskab.

Endvidere er spørgsmålet fra den belgiske forfatningsdomstol, der vedrører muligheden for midlertidig opretholdelse af logningsregler i strid med EU-retten, af væsentlig dansk interesse, idet der er anlagt et civilt søgsmål mod Justitsministeriet, hvor et centralt spørgsmål forventes at blive, om Danmark har brugt for lang tid på at revidere logningsreglerne i lyset af Tele2-dommen.

Regeringens synspunkter i sagen

Det er overordnet regeringens opfattelse, at EU-Domstolen skal opfordres til at genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen. Det bør i den forbindelse fremhæves, at loggede oplysninger udgør et centralt og effektivt redskab for politiet og PET, som i forhold til efterforskning og strafforfølgning af alvorlig kriminalitet og terror er af afgørende betydning. Der bør efter regeringens opfattelse argumenteres bl.a. på den baggrund for, at EU-retten ikke er til hinder for en generel og udifferentieret logningsforpligtelse, hvis formål bl.a. er at sikre den personlige og nationale sikkerhed, som staten har en positiv forpligtelse til at sikre for alle borgere.

I forhold til medlemsstaternes forpligtelse til at efterleve EU-retten, er det regeringens opfattelse, at der bør argumenteres for, at dette i overensstemmelse med EU-Domstolens faste praksis skal ske hurtigst muligt[1]. Hvad der i en konkret sag er hurtigst muligt vil imidlertid bero på en samlet bedøm-

[1] Jf. bl.a. de forenede sager C-231/06 – C-233/06, pr. 41.

melse under inddragelse af flere momenter, herunder navnlig sagens kompleksitet.

Europaudvalget 2018-19
EUU Alm.del - Bilag 171
Offentligt

Bilag AP

Kammeradvokaten

JUSTITSMINISTERIET

Dato: 29. november 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Michael Hadberg
Sagsnr.: 2018-614-0612
Dok.: 888946

Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl.

1. Indledning

Conseil d'État i Frankrig har i to sager om dels gyldigheden af en række dekreter vedtaget med hjemmel i fransk lovgivning, dels ophævelsen af en række bestemmelser i fransk lovgivning, forelagt EU-Domstolen fem præjudicielle spørgsmål – hvoraf to er enslydende – om bl.a. fortolkningen af direktiv 2002/58/EF, som vedrører behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

Af disse spørgsmål er navnlig de to (enslydende) spørgsmål af dansk interesse, idet de vedrører det retlige grundlag for at pålægge teleselskaber at logge oplysninger om kommunikation til brug for bl.a. bekæmpelse af kriminalitet. Der ønskes med spørgsmålene svar på, om en forpligtelse til generel og udifferentieret lagring, som pålægges udbyderne på grundlag af bestemmelserne i artikel 15, stk. 1, i direktiv 2002/58/EF, i en situation, der er præget af alvorlige og vedvarende trusler mod den nationale sikkerhed og navnlig af risikoen for terror, skal anses for et indgreb, der er begrundet i retten til personlig sikkerhed og hensynet til den nationale sikkerhed, som medlemsstaterne er eneansvarlige for i medfør af artikel 4 i Traktaten om Den Europæiske Union.

2. Sagernes faktiske omstændigheder

En række sagsøgere har i den ene sag anlagt fire sager mod forskellige ministre i den franske regering med påstand om, at fire dekreter om efterretningstjenester og efterretningsarbejde skal annulleres. Sagerne er efterfølgende blevet forenet.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Baggrunden for søgsmålet er EU-Domstolens dom af 21. december 2016 i de forenede sager, Tele2/Sverig og Watson, C-203/15 og C-698/15, (Store Afdeling), hvori det bl.a. blev fastslået, at de svenske regler om logning var i strid med direktiv 2002/58 sammenholdt med Den Europæiske Unions Charter om Grundlæggende Rettigheder (Chartret), idet de medførte en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

Sagsøgerne i de nationale sager gør i det væsentlige gældende, at de franske regler, er i strid med både Den Europæiske Menneskerettighedskonvention og Chartret, fordi de fastsætter en sådan generel pligt til udifferentieret logning, som EU-Domstolen underkendte i Tele2-sagen.

Den franske regeringen har heroverfor i begge sager gjort gældende, at sagsøgernes anbringender er ugrundede, og har nedlagt påstand om frifindelse.

Det bemærkes i øvrigt, at der ligeledes er forelagt en belgisk sag for Domstolen, der omhandler tilsvarende problemstilling (sag C-520/18, Ordre des barraeaux francophones et germanophpne e.a.).

3. Den danske interesse i sagen

Det er regeringens opfattelse, at regeringen bør afgive indlæg i denne sag, da EU-Domstolens besvarelse af de forelagte spørgsmål vil kunne have betydning for medlemsstaternes mulighed for at pålægge teleselskaber at gemme og opbevare oplysninger om tele- og internettrafik (logning) til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

De danske regler om logning skal som konsekvens af EU-Domstolens afgørelse i Tele2-sagen revideres. Tele2-dommen efterlader imidlertid væsentlig fortolkningstvivl i forhold til, hvorledes nationale bestemmelser om logning kan indrettes i overensstemmelse med direktiv 2002/58 og Chartret. Der har således siden foråret 2017 været løbende drøftelser i regi af Rådet om, hvordan medlemsstaterne kan indrette de nationale regler i lyset af dommen.

Domstolens besvarelse af de forelagte spørgsmål kan derfor få stor betydning for, hvordan logningsregler kan indrettes i overensstemmelse med EU-retten på en måde, hvor logning fortsat vil udføre et centralt og effektivt efterforskningsredskab.

Regeringens synspunkter i sagen

Det er overordnet regeringens opfattelse, at EU-Domstolen skal opfordres til at genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen. Det bør i den forbindelse fremhæves, at loggede oplysninger udgør et centralt og effektivt redskab for politiet og PET, som i forhold til efterforskning og strafforfølgning af alvorlig kriminalitet og terror er af afgørende betydning.

Der bør efter regeringens opfattelse argumenteres bl.a. på den baggrund for, at EU-retten ikke er til hinder for en generel og udifferentieret logningsforpligtelse, hvis formål bl.a. er at sikre den personlige og nationale sikkerhed, som staten har en positiv forpligtelse til at sikre for alle borgere.

Det er på den baggrund regeringens opfattelse, at de to enslydende spørgsmål, der er forelagt EU-Domstolen, skal besvares bekræftende.

Bilag 15

RIGSPOLITIET

28. september 2019

Redegørelse om teledatasagen

Indholdsfortegnelse

1. Indledning

Justitsministeriet har ved brev af 2. juli 2019 til rigspolitichefen og rigsadvokaten anmodet om en samlet redegørelse om teledatasagen. Justitsministeriet har i sit brev henvist til det brev, som Rigsadvokaturen den 13. juni 2019 sendte til Advokatsamfundet og Landsforeningen af Forsvarsadvokater, hvori Rigsadvokaturen orienterede om, at Rigspolitiet havde konstateret en systemfejl i det it-program, som politiet anvender til at konvertere såkaldte rådata fra teleselskaberne i forbindelse med indhentning af teleoplysninger i straffesager.

Det fremgår af Justitsministeriets brev, at Rigspolitiet den 30. juni 2019 har oplyst, at Rigspolitiet desuden i perioder fra visse teleselskaber har modtaget mangelfulde rådata om kommunikation ved brug af nyere samtaletjenester mv. Det har medført, at sådanne rådata har manglet i konkrete straffesager.

Justitsministeriet har på den baggrund anmodet rigspolitichefen og rigsadvokaten om at redegøre for alle relevante forhold i teledatasagen, herunder:

- En redegørelse for det faktiske forløb i sagen, herunder orienteringen af forsvarerne og domstolene, samt for tidsforløbet i forhold til afholdelsen af folketingsvalget den 5. juni 2019.
- En redegørelse for, hvordan verserende straffesager er blevet håndteret.
- En redegørelse for fremgangsmåden i forbindelse med indhentning af teleoplysninger i straffesager.
- En redegørelse for kontrollen med og kvalitetssikringen af indhentede teleoplysninger.
- En redegørelse for, hvordan teleoplysninger anvendes af politiet og anklagemyndigheden under efterforskningen og straffesagsbehandlingen, herunder hvordan anklagemyndigheden løbende sikrer overholdelse af objektivitetsprincippet.

Ved brev af 14. august 2019 til Folketingets Retsudvalg har justitsministeren orienteret om, at Rigspolitiet har oplyst Justitsministeriet om, at det er Rigspolitiets vurdering, at det er nødvendigt at undersøge, om der vil være behov for at fremfinde sager fra før 2012. Det skyldes ifølge Rigspolitiet, at der er fundet uoverensstemmelser mellem rådata og konverterede data, som giver anledning til at iværksætte en sådan undersøgelse. Der er således

tale om en anden vurdering af den tidsmæssige afgrænsning end den, som Rigspolitiet anlagde i forbindelse med justitsministerens brev af 2. juli 2019. I forlængelse af den nye vurdering har Justitsministeriet bedt rigspolitichefen om i redegørelsen at fastlægge sin vurdering af den relevante tidsmæssige afgrænsning samt at oplyse om baggrunden for denne vurdering.

I et brev af 18. august 2019 til Retsudvalget har justitsministeren oplyst udvalget om, at Rigspolitiet den 16. august 2019 har oplyst til Justitsministeriet, at Rigspolitiet i forbindelse med gennemgangen af de konkrete straffesager, der kan være berørt af fejlen, har identificeret fejl i forbindelse med konverteringen af geografiske koordinater for telemasters placering. Det medfører ifølge oplysningerne fra Rigspolitiet, at der ved behandlingen af straffesager kan være indgået fejlbehæftede masteplaceringer, som er anvendt til at sandsynliggøre en telefons position mv. Det fremgår af brevet, at omfanget af og årsagen til fejlen endnu ikke er afdækket.

Det fremgår endvidere af brevet, at Rigspolitiet den 18. august 2019 har oplyst, at der i forbindelse med gennemgangen af de konkrete straffesager ligeledes er konstateret flere forskellige konkrete fejl i den rådata, som politiet modtager fra teleselskaberne vedrørende teleoplysninger. Det er i den forbindelse anført, at omfanget og betydningen af disse fejl endnu ikke er afdækket.

Det er anført i brevet, at Rigsadvokaturen samme dag – den 18. august 2019 – har udsendt en instruks til landets anklagere om, at rigsadvokaten som en umiddelbar konsekvens har besluttet, at anklagere ikke må anvende teledata under hovedforhandlinger eller retsmøder vedrørende opretholdelse af anholdelse. Det fremgår af brevet, at det midlertidige stop indtil videre vil gælde i 2 måneder.

I forlængelse af de nye oplysninger i sagen er rigspolitichefen og rigsadvokaten anmodet om også at redegøre for alle relevante forhold vedrørende de nye fejl. I lyset af den nye udvikling i sagen har justitsministeren efter anmodning fra rigspolitichefen og rigsadvokaten forlænget fristen for modtagelsen af den samlede redegørelse, således at denne skal være Justitsministeriets departement i hænde inden udgangen af september 2019.

2. Reguleringen af teleoplysninger

2.1. Retsplejelovens regler

Teleoplysninger er oplysninger om kommunikation, som teleudbyderne er i besiddelse af, og som politiet til brug for efterforskningen af primært alvorlige strafbare forhold kan indhente hos teleudbyderne. Efter retsplejelovens § 786, stk. 4, påhviler det således udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af teleoplysninger til brug for efterforskning og retsforfølgning af strafbare forhold.

Når en politikreds, et efterforskningsfællesskab eller en anden kompetent myndighed indhenter teleoplysninger hos teleudbyderne, sker det via Rigspolitiets Telecenter (herefter telecentret). Den praktiske fremgangsmåde er nærmere beskrevet i afsnit 3. Indhentelse af teleoplysninger er et straffeprocessuelt tvangsindgreb, der er omfattet af retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og i et vist omfang retsplejelovens kapitel 74 om edition. Det fremgår af retsplejelovens bestemmelser, at udlevering af teleoplysninger til politiet sker på baggrund af rettens kendelse eller på øjemedet efterfulgt af rettens kendelse, hvis det af efterforskningsmæssige grunde har været nødvendigt at iværksætte indgrebet straks. Herudover vil der kunne indhentes visse teleoplysninger i henhold til et samtykke fra abonnenten, ligesom politiet i helt særlige tilfælde efter nødretlige principper kan indhente teleoplysninger uden rettens kendelse, f.eks. for at yde humanitær hjælp til en selvmordstruet eller helbredsmæssigt svækket person.

Teleoplysninger kan opdeles i tre kategorier. Den ene kategori er i lovgivningen blot benævnt 'teleoplysning' og tilvejebringes af politiet med hjemmel i retsplejelovens § 780, stk. 1, nr. 3. Den type teleoplysning er oplysning om, hvilke telefoner og tilsvarende kommunikationsapparater (f.eks. tablets) der i et bestemt tidsrum har været sat eller sættes i forbindelse med en bestemt telefon eller et andet kommunikationsapparat.

Den anden kategori har betegnelsen 'udvidet teleoplysning' og indhentes med hjemmel i retsplejelovens § 780, stk. 1, nr. 4. De oplysninger, der er omfattet af dette straffeprocessuelle tvangsindgreb, er oplysninger om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der inden for et nærmere angivet geografisk område har været sat eller sættes i forbindelse med telefoner eller andre kommunikationsapparater. I praksis bliver

indgrebet også benævnt 'mastesug', idet de oplysninger, som politiet modtager, er oplysninger om, hvilke mobiltelefoner der inden for et bestemt tidsrum og et bestemt geografisk område har benyttet én eller flere bestemte telemaster til kommunikation.

For begge disse kategorier af teleoplysninger gælder som udgangspunkt et kriminalitetskrav på fængsel i 6 år eller derover, ligesom der er skærpede krav til indhentelse af udvidede teleoplysninger.

Den tredje kategori af teleoplysninger har betegnelsen 'masteoplysninger' og indhentes med hjemmel i retsplejelovens regler om edition, jf. § 804, stk. 1. Disse oplysninger retter sig mod én bestemt telefon og viser, hvilke telemaster telefonen har været registreret på i en given periode. Masteoplysninger indeholder ikke oplysninger om, hvilke andre telefoner mv. der eventuelt har været sat i forbindelse med den specifikke telefon.

Indhentelse af masteoplysninger kan bl.a. ske som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, og derfor kan masteoplysninger også indhentes til brug for sager, hvor strafferammen er under 6 års fængsel.

I det følgende vil 'teledata' blive brugt som en samlet betegnelse for teleoplysning, udvidede teleoplysning og masteoplysninger.

2.2. Logningsreglerne

Efter retsplejelovens § 786, stk. 4, fastsætter justitsministeren efter forhandling med erhvervsministeren nærmere regler om registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Med hjemmel i denne bemyndigelse har Justitsministeriet udstedt bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen). Betingelserne for politiets adgang til at få udleveret de registrerede oplysninger, herunder kriminalitetskravet, er nærmere reguleret i retsplejelovens kapitel 71 og kapitel 74, jf. afsnit 2.1 og 3.1.

Hovedkravet for at være omfattet af logningsforpligtelsen er, at der udbydes elektroniske kommunikationsnet eller -tjenester på kommercielt grundlag til slutbrugere. I praksis er der på nuværende tidspunkt fire teleudbydere, der leverer teleoplysninger til telecentret. Det

drejer sig om TDC, Telenor, Hi3G og Telia. De øvrige teleudbydere lejer sig ind på disse fire udbyderes net, og leverancer fra en af de øvrige teleudbydere vil derfor komme fra en af de fire. De fleste af de øvrige teleudbydere har en aftale om "outsourcing" af forpligtelsen til at levere teleoplysninger. Det betyder, at en rekvisition om levering af teledata går direkte til en af de fire ovennævnte teleudbydere. I de tilfælde, hvor en af de øvrige teleudbydere ikke har indgået en aftale om outsourcing, vil en rekvisition gå til den pågældende udbyder, som herefter vil få en af de fire teleudbydere til at fremsende oplysningerne til telecentret.

I forbindelse med indførelsen af logningsbekendtgørelsen blev det overvejet at stille krav om, at teleudbyderne skulle levere loggede teledata i standardiserede formater. Der blev dog ikke stillet krav herom.

2.2.1. Teledata omfattet af logningsbekendtgørelsen

Teleudbyderne har alene pligt til at logge oplysninger, der genereres eller behandles i udbyderens net, jf. bekendtgørelsens § 1. Logningsreglerne pålægger således ikke udbyderen at generere data alene med det formål at logge dem.

De specifikke typer af teleoplysninger, som udbyderne har pligt til at logge, reguleres i bekendtgørelsens §§ 4-6. Fælles for bestemmelserne er, at udbyderne skal registrere og opbevare oplysninger om kommunikationen, men ikke selve indholdet af kommunikationen – hverken i forbindelse med telefonsamtaler mv., brug af internettet eller brug af udbyderens e-mailtjenester. I afsnittene 2.2.1.1-2.2.1.2 er de enkelte logningspligtige typer teleoplysninger beskrevet.

2.2.1.1. Opkald og SMS

Det følger af bekendtgørelsens § 4, nr. 1-8, at en udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om fastnet- og mobiltelefoni samt
SMS-, EMS- og MMS-kommunikation:

- opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,

- ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- kvittering for modtagelse af meddelelser,
- identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre),
- den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen (masteoplysninger),
- tidspunktet for kommunikationens start og afslutning og
- tidspunktet for første aktivering af anonyme tjenester (taletidskort).

SMS står for "Short Message Service" og er små tekstbeskeder, som kan sendes mellem mobiltelefoner, tablets eller andre lignende enheder. MMS står for "Multimedia Message Service". MMS svarer til SMS-beskeder, men kan ud over tekst også indeholde billeder, video og lyd, ligesom MMS'er kan sendes til almindelige e-mailadresser. EMS, der står for "Enhanced Media Service", er en forældet teknologi, der ikke længere indgår i de teledata, som telecentret modtager fra teleudbyderne.

Et IMSI-nummer (International Mobile Subscriber Identification) identificerer telefonens SIM-kort, mens et IMEI-nummer (International Mobile Equipment Identifier) identificerer den fysiske mobilenhed, dvs. selve mobiltelefonen. For så vidt angår masteoplysninger gælder det, at udbyderne skal logge oplysninger om "den første og sidste mast", dvs. de transmissionsceller, en mobiltelefon har anvendt i forbindelse med en kommunikations begyndelse og afslutning.

Vedrørende opkald og SMS bemærkes det, at sådanne aktiviteter også kan ske gennem anvendelse af nyere samtaletjenester kaldet VoLTE ("Voice over Long Term Evolution") og VoWiFi ("Voice over WiFi").

VoLTE er opkald, der går via 4G-netværket, som tidligere kun blev anvendt til datatrafik og ikke til telefoni. Når abonnenten anvender VoLTE, flyttes forbindelsen til samtale fra 2G- og 3G-netværket over til 4G-netværket. Herved er det muligt at tale i telefon via VoLTE på steder, hvor der udelukkende er 4G dækning og dermed ikke almindelig dækning til samtale via traditionel telefoni på 2G- eller 3G-netværket, ligesom teknologien giver mulighed for at forbedre lydkvaliteten og etablere opkald hurtigere.

VoWiFi er en teknologi, der er meget lig VoLTE. VoWiFi muliggør telefoni, når brugeren kan tilgå internettet via et WiFi-netværk (trådløst internet). Hermed er det muligt bl.a. at foretage telefonopkald og sende SMS, når der ikke er mobildækning, ligesom samtaler kan skifte fra WiFi-netværk til mobilnetværk uden afbrydelser.

2.2.1.2. Internet

Oprindeligt indeholdt logningsbekendtgørelsen regler om logning af en række oplysninger vedrørende internetsessioner, dvs. information om aktivitet på internettet, som udbydere havde pligt til at registrere. Reglerne om sessionslogning blev ophævet ved bekendtgørelse nr. 660 af 19. juni 2014.

De oplysninger, der i dag skal logges vedrørende internetbrug, fremgår af logningsbekendtgørelsens § 5, stk. 1, nr. 1-4. Det følger af denne bestemmelse, at en udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om en brugers adgang til internettet:

- den tildelte brugeridentitet,
- den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,
- navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse (IP-adresse), en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet og
- tidspunktet for kommunikationens start og afslutning.

2.3. Andre datatyper, der ikke er omfattet af logningsbekendtgørelsen

2.3.1. Signaleringsdata

Signaleringsdata er lokaliseringsdata, dvs. oplysninger om placeringen af den sendemast, som en telefon kommunikerer med, og indhentes efter reglerne om edition i retsplejelovens kapitel 74. Signaleringsdata er en særlig aktivitet, som viser en telefons placering, men som ikke indeholder oplysninger om, hvilke telefoner mv. der sættes i forbindelse med en bestemt telefon.

Signaleringsdata adskiller sig bl.a. fra almindelige masteoplysninger ved, at signaleringsdata også viser, når en telefonen kommunikerer/signalerer til mobilnetværket, selv om den person, der er i besiddelse af telefonen, ikke aktivt anvender telefonen på det pågældende

tidspunkt. Det kan f.eks. vise en internetsession, der vedligeholdes på telefonen, eller en telefon, der flytter sig mellem forskellige netværksområder.

Signaleringsdata er en datatype, som ikke er omfattet af logningsbekendtgørelsen, og derfor består der ikke en pligt for teleselskaberne til at logge signaleringsdata. Datatypen registreres af nogle teleudbydere med henblik på at fejlrette og optimere teleudbyderens ydelser og kan derfor i et vist omfang rekvireres af politiet i medfør af reglerne om edition.

2.3.2. Oplysninger om særlige tjenester

Der ses ikke i logningsreglerne at være en pligt for teleudbyderen til at logge oplysninger om brugernes aktivering og deaktivering af forskellige særlige tjenester såsom viderestilling, "banke-på", blokering af nummer mv. I det omfang brugerne har mulighed for at benytte sig af sådanne tjenester, og teleudbyderen samtidig registrerer oplysninger om brugen heraf, vil disse oplysninger kunne indgå i de teledata, der leveres til politiet.

I forbindelse med bestilling af teledata i form af teleoplysninger og udvidede teleoplysninger har en teleudbyder siden 2010 leveret oplysninger om aktivering og deaktivering af forskellige tjenester til telecentret. Datatypen er benævnt "anden aktivitet" i de konverterede datasæt, som telecentret leverer til politikredsene mv., jf. afsnit 6.2.1.2.

3. Fremgangsmåden i forbindelse med indhentning af teledata

3.1. Indhentning af kendelse

De forskellige straffeprocessuelle indgreb giver som nævnt under afsnit 2.1 politiet mulighed for efter rettens kendelse at modtage oplysninger fra teleselskaberne om, eksempelvis hvilke forbindelser et telefonnummer eller en specifik mobiltelefon har haft i en given periode.

I forbindelse med indhentning af kendelser skal politiet indledningsvist vurdere, om retsplejelovens betingelser er opfyldt.

Politiet skal derfor bl.a. vurdere, om der er bestemte grunde til at antage, at der er givet meddelelser til eller fra en mistænkt via de ønskede teleoplysninger (mistankekravet). Altså om der er en konkret sammenhæng mellem den mistænkte og kommunikationen. Derudover skal politiet vurdere, om indhentning af teleoplysningerne er af afgørende betydning for efterforskningen (indikationskravet), og om den efterforskede lovovertrædelses strafferamme er tilstrækkelig høj (kriminalitetskravet). Endelig må der ikke være misforhold mellem på den ene side indgrebets formål og sagens betydning og på den anden side den krænkelse og ulempe, som indgrebet forvolder hos den eller de personer, det rammer (proportionalitetsprincippet). Indhentning af kendelse om udvidede teleoplysninger kræver endvidere, at mistanken vedrører en forbrydelse, som har medført eller kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.

Hvis politiet vurderer, at retsplejelovens betingelser er opfyldt, udfærdiger politiet en efterforskningsrapport, der nærmere redegør for sagen, og for at betingelserne for indhentning af den ønskede kendelse er opfyldt. Politiet afleverer herefter sagen til anklagemyndigheden, der foretager en selvstændig vurdering af, om betingelserne for indhentning af kendelsen er opfyldt. Hvis anklagemyndigheden ikke finder, at betingelserne for indhentning af kendelsen er opfyldt, tilbageleveres sagen til politiet med anmodning om uddybning af materialet, hvis dette er muligt.

Hvis anklagemyndigheden er enig i, at betingelserne for indhentning af den pågældende kendelse er opfyldt, fremsættes anmodningen om kendelse for en dommer, der herefter afsiger en kendelse.

Politiets og anklagemyndighedens vurderinger foretages under iagttagelse af objektivitetsprincippet, hvorefter det ikke blot skal påses, at strafskyldige drages til ansvar, men også at forfølgning af uskyldige ikke finder sted.

3.2. Bestilling af teledata

Efter kendelsens afsigelse indhenter politikredsen den relevante teledata via telecentret, der frem til maj 2014 organisatorisk var en del af Rigspolitiets Koncern IT (KIT). Herefter blev telecentret organisatorisk placeret i Nationalt Cyber Crime Center (NC3) i Politiområdet i Rigspolitiet – senest som en del af afdelingen 'Tele og aflytning'. Denne afdeling blev den 24. juni 2019 flyttet fra NC3 til Nationalt Kriminalteknisk Center (NKC) i Politiområdet. Både NC3 og NKC er en del af National Efterforskningsafdeling (NEA) i Politiområdet i Rigspolitiet.

Teleoplysninger bestilles af politikredsene, efterforskningsfællesskaberne mv. (efterfølgende benævnt rekvirenten) hos telecentret i henhold til reglerne beskrevet i kapitel 2. I praksis er det sagsbehandleren i politikredsen mv., der håndterer bestillingen.

Bestillingen indeholder bl.a. angivelse af, hvilke selskaber teledata skal indhentes hos, og hvilken periode bestillingen vedrører. Telecentret formidler herefter bestillingen til de relevante teleudbydere med anmodning om levering af teledata.

3.3. Telecentrets konvertering af rådata

Når en teleudbyder har modtaget bestillingen fra Rigspolitiet, indhenter teleudbyderen de bestilte teledata i sit netværk og leverer herefter teleoplysningerne som rådata til telecentret.

Rådata leveres af teleudbyderen i form af et eller flere regneark. Hvert regneark indeholder et antal rækker, hvor hver række repræsenterer en aktivitet i form af en bestemt datatype. Én aktivitet i rådata er udtryk for én aktivitet på en telefon eller en telemast, dvs. ét opkald, én sms mv.

Når telecentret efterfølgende leverer teledata videre til rekvirenten, består telecentrets leverance af en vejledning og to datasæt; et datasæt med rådata og et datasæt med konverterede teledata. Telecentret foretager ikke ændringer i de rådata, som telecentret har modtaget

fra teleudbyderne og leverer til rekvirenten. Rådata leveres således til rekvirenten på den måde, som det modtages fra teleudbyderne. Det betyder bl.a., at de enkelte datatyper i rådata ikke i alle tilfælde er benævnt på samme måde, jf. nærmere om datatyper i afsnit 2.2 og 2.3. Telecentret leverer derfor også et sæt behandlede (konverterede) data til rekvirenten.

Konverteringen indebærer en ensretning af beskrivelsen af de datatyper, der er indeholdt i rådatasættet, således at hver enkelt datatype bliver benævnt på samme måde, uafhængigt af hvilken teleudbyder data kommer fra. Herudover ensrettes de kolonner og overskrifter, som er anvendt i rådatasættet, samt de koordinatsystemer og formater for landekoder, som teleudbyderne anvender. Formålet med telecentrets konvertering af teledata er at sikre, at oplysningerne fremstår ensartede og genkendelige under efterforskningen og i forbindelse med en eventuel efterfølgende fremlæggelse af oplysningerne i retten.

De konverterede teledata leveres i et eller flere regneark, og datasættet skal bestå af det samme antal rækker som i rådatasættet for at være komplet. Det gælder dog ikke, hvis rådata f.eks. indeholder flere rækker med de samme oplysninger (dubletter), blanke rækker eller flere ens linjer med overskrift. I sådanne tilfælde er konverteringsprogrammet kodet til at filtrere disse overflødige rækker fra ved konverteringen, hvorved der opstår en divergens mellem antallet af rækker i rådata og konverterede data, uden at der derved mangler teledata i det konverterede datasæt.

Inden konverteringen af rådata bliver påbegyndt i telecentret, bliver rådatafilen kopieret, hvorefter den originale rådatafil bliver gemt i telecentrets system. Filens stamoplysninger så som dele af filnavnet og antallet af rækker med data registreres automatisk i systemet. Kopien af rådatafilen opdeles i datatyper, og konverteringen sættes i gang.

Når konverteringen er afsluttet, dannes en fil, som indeholder 1) de konverterede teledata, 2) en kopi af rådata og 3) en vejledning om den praktiske håndtering af teledata (vejledningen er endvidere beskrevet i afsnit 6.4), som telecentret fremsender pr. e-mail til rekvirenten. Herudover kan rekvirenten selv downloade teleoplysninger fra telecentrets system. Teledata, der hentes derfra, er identiske med de teledata, der leveres til rekvirenten. Endvidere kan rekvirenten tilgå de konverterede teledata i et særligt analyseværktøj, jf. nærmere herom i afsnit 6.2.1.3.

3.4. Konverteringssystemets etablering

Der er ikke fastsat regler om, at teleudbyderne skal levere teledata til Rigspolitiet i standardiserede formater. Rigspolitiet konverterer derfor teleudbydernes rådata til et standardiseret format med henblik på levering til rekvirenterne.

Rigspolitiet indkøbte omkring 2007 et system til at konvertere historiske teleoplysninger, herunder en særlig konverteringsplatform. Systemet blev sat i drift i Rigspolitiet i starten af november 2010, og telecentret har siden leveret konverterede teleoplysninger til politikredsene mv. Fra dette tidspunkt og frem til efteråret 2016 blev systemet suppleret af et egenudviklet system, der i denne periode har understøttet dele af den samlede proces vedrørende konvertering af teleoplysninger.

Konverteringsplatformen blev i efteråret 2016 erstattet af et egenudviklet konverteringsprogram, som er en videreudvikling af det støttesystem, der har været anvendt siden november 2010. Denne løsning blev valgt af Rigspolitiet på grund af manglende fleksibilitet i den oprindelige konverteringsplatform.

3.5. Sletning af teledata i telecentret

Der er i retsplejelovens § 791 fastsat regler om sletning af materiale, som er tilvejebragt ved indgreb i meddelelseshemmeligheden. Teledata indhentet efter retsplejelovens § 780, stk. 1, nr. 3 og 4, er omfattet af disse regler. Efter retsplejelovens § 791, stk. 1, skal materialet tilintetgøres, hvis der ikke rejses sigtelse mod nogen, eller hvis påtale senere opgives. Retten kan dog efter § 791, stk. 2, bestemme, at tilintetgørelse kan undlades eller udsættes. Efter § 791, stk. 4, skal politiet i øvrigt tilintetgøre materiale, som tilvejebringes ved indgreb i meddelelseshemmeligheden, og som viser sig ikke at have efterforskningsmæssig betydning.

Ved instruks af 12. juli 2017 har Rigsadvokaturen præciseret, at det er den enkelte politikreds, der skal sørge for, at materialet slettes i overensstemmelse med gældende ret. Ifølge instruksen skal sletningen ske ved, at politikredsen indsender en sletterekvisition til telecentret, samtidig med at politikredsen sørger for, at eventuelle kopier af materialet, der opbevares lokalt i kredsen, også slettes.

Særligt for telecentret bemærkes det, at teledata lagres i telecentret efter afslutning af databehandlingen. De rådata, der opbevares, skal slettes, hvis rekvirenten anmoder herom. For så vidt angår konverterede teledata er telecentret – når en databehandling er afsluttet – i besiddelse af to eksemplarer af de konverterede teledata. Af kapacitetsmæssige årsager har telecentret fastsat en forretningsproces, hvorefter disse teledata burde slettes automatisk, medmindre rekvirenten, der har anmodet om oplysninger, før udløbet af denne frist har meddelt telecentret, at sletningen skal udsættes. Sletningen af det ene eksemplar af de konverterede datasæt skal ske efter et år, og det andet eksemplar skal slettes efter yderligere et år. Telecentret har imidlertid i midten af september 2019 i forbindelse med teledatasagen konstateret, at sletningen af konverterede teledata efter to år ikke er sket i fuldt omfang, og at der tilsyneladende fortsat opbevares ca. 75 pct. af disse datasæt i telecentret. Den automatiske sletning af eksemplarer af konverterede teledata efter et år ses at være sket.

4. Anvendelse af teledata

Teledata i form af teleoplysninger, udvidede teleoplysninger og historiske masteoplysninger kan grundlæggende anvendes på to forskellige måder; dels under efterforskningen, hvilket beskrives under afsnit 4.1, dels under straffesagsbehandlingen, som beskrives under afsnit 4.2.

Som det fremgår ovenfor under afsnit 2.2.1, indeholder teledata oplysninger *om* telekommunikation eller lignende i modsætning til oplysninger om *indholdet* af telekommunikation. Med andre ord viser oplysningerne, *at* der er kommunikeret, men ikke *hvad* der er kommunikeret om.

4.1. Anvendelse af teledata under efterforskningen

Politiet anvender historiske teledata i efterforskningen af alvorlig kriminalitet, jf. nærmere om kriminalitetskravene i afsnit 2.1, og formålet med anvendelsen afhænger af de efterforskningsmæssige behov og udfordringer, som kendetegner den konkrete sag. Der er dog grundlæggende tale om et efterforskningsskridt, som anvendes til at målrette og fokusere efterforskningen, idet teledata giver politiet indikationer om relevante personers kontaktflader, relationer og færden og dermed kan medvirke til at be- eller afkræfte hypoteser om en forbrydelses mulige omstændigheder.

Politiets brug af teledata er således blot ét ud af en ofte lang række efterforskningsskridt, som iværksættes i sager om alvorlig kriminalitet, herunder oplysninger indhentet fra tv-overvågning, ransagninger, aflytninger, vidneforklaringer, kriminaltekniske undersøgelser og efterretninger fra relevante kriminelle miljøer. Selvom teledata i det følgende flere steder er beskrevet løsrevet fra andre efterforskningsmidler, kan dette derfor ikke tages som udtryk for, at teledata kan stå alene i politiets efterforskning.

4.1.1. Analytisk anvendelse

Politiet anvender teledata på forskellige stadier af en efterforskning. I den indledende fase af en efterforskning kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikation og på den baggrund danne et overblik over personernes kommunikationsmønstre. Herved er det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke personer fra efterforskningen, hvis de vurderes ikke at have relevans for sagen.

Som eksempel på politiets behov for i sager om alvorlig kriminalitet at kunne adskille mulige gerningspersoner fra sagens øvrige personer kan der peges på efterforskningen af drabssager. Erfaringsmæssigt har gerningsmanden til et drab ofte en nær relation til afdøde, og derfor vil politiets efterforskning som udgangspunkt indledningsvist have fokus på afdødes familie og/eller vennekreds. Henset til sagens alvor, herunder at flere personer uafhængigt af hinanden kan være under mistanke for at stå bag drabet, er det centralt, at politiet har redskaber, der kan bistå med at fastlægge, hvilke efterforskningsretninger der skal forfølges yderligere, og hvilke der kan afvises. Samtidig er det vigtigt af hensyn til de efterladte, at der ikke opstår unødig tvivl om et familiemedlems eller en vens involvering i drabet ved, at politiet hurtigst muligt afklarer eventuel mistanke mod afdødes nære relationer.

Teledata kan være med til bl.a. at målrette politiets indsamling af andre beviser på et tidligt stadie af efterforskningen, herunder videoovervågning, f.eks. for hurtigt at finde og identificere en ellers ukendt gerningsmand. I tilfælde hvor den formodede gerningsmand er kendt af politiet, men forsvundet, kan teledata også bidrage til at opspore den mistænkte. En analyse af indhentede teledata kan også resultere i nye efterforskningsveje eller kaste lys over andre forhold, der gør det nødvendigt at indhente yderligere teledata.

Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan teledata bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes teledata til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

4.1.2. Understøttelse af øvrige efterforskningsskridt

Teledata kan anvendes til at understøtte de øvrige efterforskningskridt, politiet iværksætter. Det gælder eksempelvis i forhold til de afhøringer, som politiet foretager. Teledata kan således danne grundlag for at afhøre en mistænkt om dennes færden, ligesom teledata kan styrke eller svække troværdigheden af den mistænktes forklaring, herunder særligt om relationer og kontaktflader. Oplysningerne vil således navnlig kunne anvendes til enten at styrke eller svække en mistanke over for den pågældende. Oplysningerne kan på samme måde bidrage til at underbygge vidners og forurettedes forklaringer.

I kombination med andre relevante efterforskningsskridt og værktøjer, som eksempelvis ANPG-systemet, kan teledata navnlig være med til at belyse mistænktes bevægelsesmønstre, bl.a. i de tilfælde, hvor en mistænkt ikke ønsker at udtale sig til politiet.

Teledata kan på den måde – sammenholdt med et eller flere andre beviser – indikere, at en mistænkt har været i nærheden af et gerningssted. Omvendt kan oplysningerne også være med til at understøtte, at en mistænkt ikke har været på et gerningssted, og dermed – i hvert fald umiddelbart – indikere, at den pågældende ikke har relevans for efterforskningen. Dette kan eksempelvis være tilfældet, hvis teledata forbinder den mistænktes telefon med en anden lokalitet end gerningsstedet på gerningstidspunktet.

Omvendt kan politiet ikke alene på baggrund af fravær af teledata, der forbinder en telefon til en bestemt lokalitet, udelukke, at en person kan have været på den pågældende lokalitet. Fraværet af teledata kan således skyldes, at der ikke har været aktivitet på telefonen, herunder at personen har holdt den slukket, eller at personen ikke har medbragt sin mobiltelefon.

Teledata i form af kaldsdata, herunder længden af foretagne opkald, og masteoplysninger kan også bidrage til at klarlægge forurettedes bevægelsesmønstre. En sådan afdækning kan bl.a. være relevant i forhold til at tids- og stedfæste en forbrydelse, afdække forurettedes færden mv.

4.1.3. Udvidede teleoplysninger

Udover at angå kommunikation i forhold til en bestemt telefon mv. kan teledata også angå et nærmere angivet område (udvidet teleoplysning eller 'mastesug'). Indhentelse af udvidede teleoplysninger anvendes til at identificere telefonnumre af interesse for politiets efterforskning, hvorefter efterforskningen kan målrettes indsamling af andre bevismidler, herunder historiske teleoplysninger.

Et af områderne for anvendelse af udvidede teleoplysninger er sager, hvor et antal ukendte personer, der mistænkes for at have begået en alvorlig forbrydelse, vurderes at have kommunikeret med hinanden umiddelbart før og efter den pågældende forbrydelse, muligvis via mobiltelefoner, og hvor den eneste efterforskningsmulighed er at få oplysninger fra den nærmeste sendemast i forhold til gerningsstedet og dermed se, hvilke telefoner der har kommunikeret via masten. Udvidede teleoplysninger kan have stor betydning i forbindelse med efterforskning af grov kriminalitet som f.eks. terror, drab, røveri mv. og i forbindelse med målrettede eftersøgninger i denne sammenhæng.

4.2. Anvendelse af teledata under straffesagsbehandlingen

4.2.1. Grundlæggende principper af betydning for anklagemyndighedens anvendelse af teledata

Det følger af retsplejelovens § 96, stk. 1, at det er de offentlige anklageres opgave sammen med politiet at forfølge forbrydelser efter reglerne i retsplejeloven. Anklagemyndigheden skal herved påse, at strafskyldige drages til ansvar, men også at forfølgning af uskyldige ikke finder sted, jf. § 96, stk. 2. Denne regel er udtryk for et objektivitetsprincip, der er et grundlæggende princip i strafferetsplejen, og som anses for en af de vigtigste retssikkerhedsgarantier.

Objektivitetsprincippet indebærer, at anklagemyndigheden og politiet ved efterforskningen af en sag både er forpligtet til at tage alt i betragtning, som kan tale for, at en mistænkt har begået en forbrydelse, men også har pligt til at tage enhver omstændighed, der tyder på en mistænkts uskyld, i betragtning.

Herudover gælder der i straffeprocessen et almindeligt princip om, at enhver rimelig tvivl skal komme den anklagede til gode ("in dubio pro reo").

Objektivitetsprincippet og princippet om, at enhver rimelig tvivl skal komme den anklagede til gode, gælder bl.a., når anklagemyndigheden skal tage stilling til spørgsmålet om tiltale, og indebærer, at anklagemyndigheden er forpligtet til at tage enhver omstændighed, der tyder på en mistænkts uskyld, i betragtning, samt ikke at rejse tiltale, medmindre anklagemyndigheden skønner, at tiltalerejsning vil føre til domfældelse.

Under hovedforhandlingen af en straffesag indebærer objektivitetsprincippet bl.a., at anklageren skal fremlægge beviserne på en saglig og objektiv måde og sikre, at også oplysninger, der kan tale imod tiltaltes skyld, kommer frem.

Et andet vigtigt princip i straffeprocessen er princippet om den fri bevisbedømmelse, jf. retsplejelovens § 880, 2. pkt., som spiller en central rolle ved behandlingen af straffesager. Det skal ses i lyset af, at domstolene i straffesager i dag ofte præsenteres for en række oplysninger, indicier og beviser, jf. herom bl.a. Ulla Staal i TfK 2018 s. 1. Ud over vidneforklaringer vil der ofte være en række andre beviser, f.eks. dna-spor, telefonaflytninger, sms-korrespondance, masteoplysninger, kriminaltekniske undersøgelser, retskemiske undersøgelser, erklæringer fra Retslægerådet mv.

Da bevisbedømmelsen er fri, skal retten ved afgørelsen af, om det er bevist, at tiltalte er skyldig, forholde sig til alt, der er kommet frem under bevisførelsen. Det er således op til retten at forholde sig til betydningen af de enkelte beviser ved afgørelsen af, om det er bevist, at tiltalte er skyldig, eller om der er begrundet tvivl.

4.2.2. Fremgangsmåden ved anklagemyndighedens anvendelse af teledata

Når politiets efterforskning er afsluttet, afleveres sagen til anklagemyndigheden. Anklagemyndigheden gennemgår herefter sagens beviser og vurderer, om der skal rejses tiltale i sagen. Hvis der rejses tiltale i sagen, fremlægger anklagemyndigheden sagens beviser for retten under en hovedforhandling.

Rigsadvokaturen har udarbejdet både en intern og ekstern vejledning til anklagemyndigheden om forberedelse og præsentation af teleoplysninger i retten. Vejledningerne er udarbejdet med henblik på at forbedre kvaliteten og skabe mere ensartethed i behandlingen og præsentationen af teledata i retten.

Til vejledningerne er endvidere knyttet en række bilag, der bl.a. beskriver de tekniske forhold omkring masteoplysninger, herunder bl.a. at fysiske forhold som høje bygninger mv. eller overbelastning af en sendemast kan medføre, at en mobiltelefon 'finder' til anden 'ledig' mast i området (mastespring).

Den interne vejledning anvendes bl.a. i forbindelse med undervisningen på Rigsadvokaturens kurser "Teleoplysninger i retten". Kurset, der udbydes årligt, er rettet mod anklagere og har til formål at give deltagerne en dybere forståelse af teknikken bag tilvejebringelse af teledata og forståelse af de informationer, som kan fås via teledata. Endvidere giver kurset indblik i konkrete redskaber og præsentationsmåder i forbindelse med fremlæggelse af teleoplysninger i retten.

4.2.2.1. Vurdering af teledata ved tiltalerejsning

I forbindelse med afgørelsen af tiltalespørgsmålet vil anklageren, som omtalt ovenfor, gennemgå sagens beviser og vurdere, om bevisbyrden kan løftes, så det udover enhver rimelig tvivl kan bevises, at den sigtede er skyldig i den rejste sigtelse.

Som led i vurderingen af tiltalespørgsmålet vil anklagemyndigheden bl.a. tage stilling til den bevismæssige værdi af teledata indhentet under efterforskningen. Det vil ske på baggrund af sagens samlede materiale, herunder f.eks. oversigter, pivottabeller, analyserapporter og efterforskningsrapporter mv. Teledata vil som omtalt altid indgå som ét blandt flere beviser i en sag, og den bevismæssige betydning af teledata vil derfor bero på en konkret vurdering af dels det enkelte teledatabevis, dels sagens samlede omstændigheder i øvrigt. Anklageren vil i medfør af objektivitetsprincippet i den forbindelse skulle tage enhver omstændighed, der tyder på en mistænkts uskyld, i betragtning.

Finder anklageren, at den foreliggende teledata er ufuldstændig i forhold til sagens bevistemaer, eller hvis der opstår spørgsmål af teknisk karakter, vil anklageren anmode politiet om at belyse de rejste spørgsmål gennem yderligere efterforskning eller analyse.

4.2.2.2. Anvendelse af teledata under hovedforhandling

I tilfælde, hvor teledata skal anvendes som bevis under straffesagens hovedforhandling, vil anklageren i forbindelse med forberedelsen af hovedforhandlingen skulle overveje, på hvilken måde præsentationen af teledata i sagen skal foregå.

Ofte vil det i retten være tilstrækkeligt i papirform at fremlægge de analyser og andet materiale, der er udfærdiget på baggrund af teledata i sagen. I lidt større sager kan det være relevant at overveje at visualisere analyser og kort, f.eks. på storskærm for retten, sådan at dokumentationen af teledata bliver så effektiv og ressourcebesparende som muligt. I meget store sager vil teknisk support i forbindelse med præsentation af teledata typisk være nødvendig.

Navnlig i større sager, hvor teledata spiller en central rolle, kan det være nødvendigt for anklageren at indkalde vidner i form af teknikere eller efterforskere vedrørende bearbejdningen af teledata i sagen. I andre sager kan der være behov for, at anklagemyndigheden forud for sagens hovedforhandling indhenter sagkyndige udtalelser om komplicerede tekniske forhold vedrørende tele- og masteoplysninger f.eks. fra en teleteknikker fra et teleselskab.

Under hovedforhandlingen vil anklageren foretage dokumentation af relevant teledata og ofte også inddrage teledata i afhøringen af tiltalte og vidner. Det gælder både teledata, der taler for og imod tiltaltes skyld, jf. objektivitetsprincippet.

I det omfang, der er indkaldt vidner, f.eks. teleteknikere eller efterforskere, som skal afgive forklaring om tekniske begreber, forståelsen af teledata og analysen af teledata i sagen mv., vil der ske afhøring af vidnerne.

Det følger af det almindelige kontradiktionsprincip, at forsvareren under hovedforhandlingen – på lige fod med anklageren – vil kunne foretage dokumentation af teledata og stille spørgsmål til vidner mv. Retten vil endvidere være berettiget og forpligtet til at stille spørgsmål til vidner, som afhøres, når som helst der i sandhedens interesse er grund til dette.

I det omfang anklageren eller forsvareren under hovedforhandlingen finder, at der er behov for at få teledata yderligere belyst, vil såvel anklageren som forsvareren kunne anmode om supplerende bevisførelse, f.eks. indkaldelse af yderligere vidner. Retten vil også selv kunne beslutte, at yderligere beviser skal føres, hvis retten anser det for nødvendigt for sagens fuldstændige oplysning.

4.2.2.3. Tidligere kendte fejl, fejlkilder og usikkerheder i teledata

Det er ikke ukendt, at der kan optræde fejl, fejlkilder eller usikkerheder i teledata, som anvendes under straffesager. Aktørerne i straffeprocessen har således – også før den konkrete sag opstod – været opmærksomme på forskellige forhold, som kan have betydning for forståelsen og validiteten af teledata som bevis.

Som omtalt i Justitsministeriets besvarelse af 20. oktober 2015 af spørgsmål nr. 182 (Alm. del) fra Folketingets Retsudvalg har det bl.a. været kendt, at Rigspolitiet tidligere i nogle tilfælde har konstateret, at teleudbydernes mastelister ikke har været korrekte og løbende ajourført, at der har været fejl i teleudbydernes historiske fortegnelser over masteplaceringer, og at der ikke er sket en retvisende registrering af de transmissionsceller, som en mobiltelefon har anvendt i forbindelse med datatrafik. Rigspolitiet har senest den 13. og 16. september 2019 modtaget henvendelser fra to teleudbydere, der bl.a. via mastedatabasen.dk er blevet opmærksomme på, at deres mastelister til politiet i nogle tilfælde er påført forkerte adresser.

Som det også fremgår af besvarelsen af 20. oktober 2015 af spørgsmål nr. 182 (Alm. del) fra Folketingets Retsudvalg, har der tidligere været konkrete tilfælde, hvor der har indgået unøjagtige masteoplysninger. Eksempelvis opdagende man i en konkret sag fejl i forbindelse med udarbejdelsen af et mastekort, idet mastepositionerne i de modtagne teleoplysninger fra teleudbyderen var så springende inden for meget korte tidsintervaller, at det ikke ville have været fysisk muligt at flytte sig så hurtigt med telefonen mellem masterne.

Som anført i samme besvarelse har det også været kendt, at der kan være forskellige fysiske forhold, som gør, at en mobiltelefon f.eks. springer til en anden mast, jf. også Rigsadvokaturens eksterne vejledning om præsentation af teleoplysninger omtalt i afsnit 4.2.2.

For så vidt angår de fejl, fejlkilder og usikkerheder mv. i teledata, som er fremkommet under teledatasagen, henvises til kapitel 6.

5. Det tidsmæssige forløb i sagen

Telecentret har løbende håndteret henvendelser om mulige fejl, unøjagtigheder, fejlkilder mv. i teledata, som rekvirenterne har modtaget fra telecentret. Henvendelserne har hovedsageligt været håndteret ved fornyet behandling af de pågældende teledata i telecentret og blev af telecentret primært opfattet som brugerfejl og periodiske tekniske udfordringer frem for systematiske fejl vedrørende teledata. Telecentret modtog således eksempelvis i både februar, maj, august og september 2018 henvendelser fra rekvirenter, der konstaterede manglende historiske teleoplysninger i konverterede datasæt, hvilket blev håndteret i de konkrete tilfælde, men uden at det gav anledning til en mere systematisk gennemgang af data. I de tilfælde, hvor fejlindmeldingerne har omhandlet mangelfulde oplysninger i rådata, har telecentret oftest håndteret det ved at kommunikere med den relevante teleudbyder om de konkrete manglende oplysninger og dermed heller ikke behandlet det som mulige systematiske fejl. Henvendelserne er efter det oplyste blevet håndteret af medarbejdere i telecentret med vekslende inddragelse af de daværende chefer for telecentret.

Der er imidlertid også eksempler på, at problemstillinger vedrørende teledata er blevet håndteret på højere ledelsesniveau. Således blev der eksempelvis i 2012 afholdt møde mellem bl.a. den daværende politidirektør for Politiområdet og et teleselskab vedrørende uregelmæssigheder og mangler vedrørende telemasters placering, som der efterfølgende blev rettet op på fra teleselskabets side.

I det følgende redegøres for hændelsesforløbet startende i november 2018, hvor telecentret efter det oplyste for første gang handlede på en mistanke om, at der kunne være en generel konverteringsfejl i det it-program, der blev anvendt til at konvertere rådata fra teleudbyderne, og frem til den 18. august 2019, hvor justitsministeren bad rigspolitichefen og rigsadvokaten redegøre for alle relevante forhold vedrørende teledatasagen.

5.1. Fra november 2018 til februar 2019

På baggrund af en konkret verserende efterforskning i en politikreds fik telecentret i november 2018 mistanke om, at der kunne være en generel konverteringsfejl i det it-program i telecentret, som konverterede rådata og videreformidlede disse data til den relevante rekvirent. Der var i den konkrete sag konstateret umiddelbart uforklarlige uoverensstemmelser mellem rådata og konverterede data, således at dele af rådata ikke indgik i den konverterede data, som blev formidlet fra telecentret til politikredsen. Den daværende chef for

NEA og chefen for NC3 blev medio november 2018 orienteret om de manglende teleoplysninger i den konkrete sag.

På baggrund af henvendelsen til telecentret om uoverensstemmelser mellem rådata og konverterede data i den konkrete efterforskning foretog telecentret i november 2018 en stikprøve med henblik på afklaring af, om der umiddelbart var tegn på en generel fejl. Stikprøvekontrollen omfattede 60 tilfældigt udvalgte sager – 30 fra 2017 og 30 fra 2018. Kontrollen – som ikke er dokumenteret og dermed ikke mulig at genskabe – viste angiveligt, at langt hovedparten af de kontrollerede sager var korrekt konverteret, mens der i få tilfælde bestod en forskel mellem rådata og konverterede data med op til fire linjers forskel i de respektive regneark.

Telecentret vurderede på baggrund af stikprøvekontrollen, at de forskelle, som stikprøven viste, ikke tydede på en generel systemfejl, samt at konverteringsfejlen i den konkrete sag skyldtes de store datafiler, der var indhentet til den pågældende sag, og som havde et meget stort omfang.

Telecentret indsatte den 28. november 2018 et nyt afsnit i den vejledning, som blev leveret til rekvirenten sammen med filerne med rådata og konverterede data, jf. afsnit 3.3 og 6.4. I det nye afsnit blev det anført, at rekvirenten inden brugen af konverterede data altid skulle sikre sig, at antallet af rækker med aktiviteter i de to datasæt var overensstemmende. Rekvirenterne blev dog ikke gjort særskilt opmærksom på ændringen i vejledningen.

Den daværende chef for NEA modtog efter anmodning den 14. januar 2019 en beskrivelse af telecentrets håndtering af historiske teledata. Det fremgik bl.a. heraf, at der i forbindelse med konverteringen af visse meget store filer kunne mangle oplysninger i de datasæt, som rekvirenten modtog fra telecentret. Det fremgik også, at et fuldt datasæt efterfølgende blev leveret til rekvirenten, og at Rigspolitiet i den forbindelse medsendte en vejledning om anvendelse af teledata, hvoraf det bl.a. fremgik, at rekvirenten altid skulle kontrollere, om der manglede data. Telecentrets beskrivelse af håndteringen af teledata gav ikke anledning til, at der på dette tidspunkt blev iværksat yderligere undersøgelser, idet den daværende chef for NEA afventede en uddybet gennemgang af teledata i den konkrete straffesag, som i november 2018 var årsagen til, at telecentret foretog stikprøven.

Den 5. februar 2019 blev telecentret kontaktet af en rekvirent vedrørende samme problemstilling i en anden efterforskning, og på den baggrund iværksatte telecentret en systematisk gennemgang af alle rekvisitioner i perioden fra januar 2017 til februar 2019 for at afdække, om der kunne konstateres en generel fejl i konverterede data. Den daværende chef for NEA blev den 20. februar 2019 orienteret om den nye henvendelse, og om at gennemgangen på det foreløbige grundlag viste, at der formentlig var tale om en generel fejl i konverteringen af rådata. Der forelå dog ingen endelige resultater af undersøgelsen på dette tidspunkt.

Den daværende chef for NEA blev i slutningen af februar 2019 oplyst om, at den fulde gennemgang af sagerne fra januar 2017 til februar 2019 havde identificeret flere sager, hvor der var konstateret uoverensstemmelser mellem rådata og konverterede data. Den daværende chef for NEA og chefen for NC3 aftalte at påbegynde forberedelsen af en orientering til politikredsene om problemstillingen indeholdende en anmodning til kredsene om at undersøge de identificerede sager i hver enkel kreds med henblik på en konkret vurdering af teledataenes betydning for efterforskningen.

Den 27. februar 2019 bragte den daværende chef for NEA sagen op på et møde i Politirådets øverste ledelse. På mødet oplyste den daværende chef for NEA, at der var konstateret mangler i teledata i en større efterforskning, og at der var noget, som tydede på, at der også kunne være mangler i andre sager. Det blev i den forbindelse aftalt, at der skulle udarbejdes et notat om sagen.

5.2. Marts 2019

I starten af marts 2019 arbejdede telecentret videre med at identificere mulige årsager til, at der i visse konverterede datasæt manglede teledata. Den 8. marts 2019 vurderede telecentret, at det angiveligt var en timer i it-systemet, der var årsag til konverteringsproblemet. Timeren blev fjernet samme dag, og telecentret indførte kontrolprocedurer for at sikre, at eventuelle mangelfulde konverterede data fremover ville blive konstateret, inden rekvirenterne tog dem i anvendelse. I den e-mail, ved hvilken de konverterede teledata samt kopien af rådata fremsendtes til rekvirenten, jf. afsnit 3.3, blev der samme dag indsat en standardtekst med henblik på at tydeliggøre vigtigheden af, at modtageren kontrollerede, at antallet af aktiviteter i rådata svarede til antallet af aktiviteter i det bearbejdede data, før analyse og behandling af teledata blev iværksat. Denne standardtekst svarede indholdsmæssigt til den justerede vejledning af november 2018.

På det foreliggende grundlag kunne telecentret dog ikke udelukke, at manglerne i de konverterede datasæt kunne bero på andre forhold end timer-funktionen, ligesom det mulige omfang af mangelfulde teledata fortsat var uafklaret, idet det bl.a. stadig var uvist, hvornår problemet var opstået.

Den 13. marts 2019 blev det drøftet mellem politidirektøren for Politiområdet (herefter politidirektøren) og Rigspolitiets databeskyttelseschef, hvorvidt teledatasagen ville have betydning for Justitsministeriets daværende overvejelser om en mulig revision af lognings-reglerne. På den baggrund blev der den 13. marts 2019 afholdt et internt møde i Politiområdet med deltagelse af bl.a. politidirektøren, chefen for NEA, chefen for National Efterforskningscenter (herefter NEC), chefen for NEA's juridiske sekretariat og databeskyttelseschefen samt medarbejdere i telecentret. På mødet gennemgik telecentret problemet med konverteringen af teledata. Telecentret kunne på mødet ikke konkludere, hvor længe konverteringsfejlen kunne have stået på, men at det kunne have været flere år. Telecentret oplyste desuden, at den type teledata, der benævnes særlige tjenester, ikke i alle tilfælde indgik i konverterede teledata, men at der på det foreliggende grundlag ikke var klarhed over, om det kunne være en del af forklaringen på, at der i visse sager manglede konverterede teleoplysninger, ligesom det var uklart, hvad der var årsag til, at særlige tjenester ikke indgik i alle konverterede datasæt.

Politidirektøren har oplyst, at det på mødet – efter en faglig diskussion om de mulige konsekvenser af manglende teledata, herunder om potentielle fejl i domstolsafgørelser – stod klart, at der kunne blive tale om et stort oprydningsarbejde, og at det blev på baggrund af mødet besluttet, at Rigsadvokaturen og Justitsministeriet skulle orienteres om sagen.

Politidirektøren har endvidere oplyst, at han samme dag drøftede sagen med Rigspolitiets koncernstyringsdirektør (herefter koncernstyringsdirektøren), og at de i enighed konkluderede, at en orientering af rigspolitichefen kunne vente, til rigspolitichefen var hjemme fra ferie. Koncernstyringsdirektøren har dog oplyst, at de ikke drøftede selve indholdet i sagen, og at han ikke fik det indtryk, at sagen var så presserende, at den ikke kunne afvente, at rigspolitichefen var tilbage fra ferie.

Politidirektøren har derudover oplyst, at han samme dag over for en afdelingschef i Justitsministeriet oplyste, at der i en stor efterforskning havde vist sig at mangle teledata, og at årsagen skulle findes i Rigspolitiets konverteringssystem, samt at det efterfølgende havde

vist sig, at der også var konverteringsfejl i andre sager. Politidirektøren har i den forbindelse oplyst, at han orienterede afdelingschefen om, at telecentret i februar 2019 konstaterede, at der var tale om systematiske konverteringsfejl, der kunne have stået på i årevis, og at årsagen til konverteringsfejlen ifølge telecentret skulle være rettet den 8. marts 2019, så konverterede datasæt efter denne dato ville være fuldstændige. Politidirektøren har endvidere oplyst, at de i samtalen herefter drøftede spørgsmålet om, at manglende teledata potentielt kunne have betydet, at skyldige var gået fri, men også potentielt kunne have ført til forkerte afgørelser ved domstolene, og at der derfor kunne blive tale om et meget stort oprydningsarbejde. Politidirektøren har afslutningsvis oplyst, at det blev aftalt med afdelingschefen i Justitsministeriet, at Rigspolitiet skulle udarbejde et notat om sagen, og at sagen skulle drøftes på et møde. Mødet blev efterfølgende kalendersat til den 27. marts 2019.

Af et tidligere udkast til redegørelse om tidsforløbet, som politidirektøren den 5. august 2019 sendte til rigspolitichefen og koncernstyringsdirektøren, fremgik det, at det den 13. marts 2019 blev tilkendegivet over for både Rigsadvokaturen og Justitsministeriet, at Rigspolitiet endnu ikke havde et overblik over sagens nærmere omstændigheder, herunder fejlens karakter, hvor længe fejlen havde eksisteret, det mulige antal berørte straffesager, og at Rigspolitiet derfor ville skulle bruge tid på at få sagen tilstrækkeligt oplyst med henblik på stillingtagen til det videre forløb, og hvilke tiltag der burde iværksættes. Endelig fremgik det af udkastet, at det over for Justitsministeriet blev betonet, at der alene var tale om en foreløbig orientering, og at Rigspolitiet ville vende tilbage over for ministeriet, når det blev muligt at redegøre mere udførligt for sagens indhold og omfang, hvilket Justitsministeriet tog til efterretning.

Samme dag – den 13. marts 2019 – orienterede chefen for NEA telefonisk en vicestatsadvokat i Kvalitetsafdelingen hos Rigsadvokaturen (herefter vicestatsadvokaten) om sagen. Det blev oplyst, at Rigspolitiet i november 2018 var blevet opmærksom på fejl i forbindelse med konverteringen af teledata i en større efterforskning. Rigspolitiet havde i slutningen af februar 2019 konstateret mulige fejl i andre sager. Fejlene vedrørte – som sagen var oplyst – situationer, hvor der var indhentet meget store mængder teledata gennem såkaldte "mastesug". Der var herefter enighed om, at problemstillingen som udgangspunkt vedrørte uopklarede sager – og ikke urigtige domfældelser – da oplysninger indhentet gennem mastesug almindeligvis ikke anvendes som bevis i retten, men derimod som grundlag for indhentning af andre teleoplysninger under efterforskningen. Det blev videre oplyst, at Rigspolitiets

vurdering var, at fejlen formentligt skyldtes en fejl i timeropsætningen i konverteringssystemet, som havde medført, at konverteringen af data var "stoppet" efter én time, og at dele af rådata derfor ikke var kommet med, men at fejlen var rettet, og at Rigspolitiet nu var i færd med at kigge bagudrettet på sager. Chefen for NEA oplyste endvidere, at problemstillingen var blevet yderligere aktualiseret som følge af Justitsministeriets overvejelser om revision af logningsreglerne. Justitsministeriet var derfor nu orienteret om sagen og havde anmodet Rigspolitiet om at beskrive problemet nærmere. Chefen for NEA gav afslutningsvist udtryk for, at der var tale om en foreløbig orientering, og at Rigsadvokaturen ville blive indkaldt til et møde i Justitsministeriet med henblik på en uddybende orientering.

Rigsadvokaturen har supplerende oplyst, at chefen for NEA på forespørgsel oplyste, at det på daværende tidspunkt var meget vanskeligt at vurdere, hvor mange sager der kunne være berørt af fejlen, men et muligt gæt kunne være i omegnen af 100 sager.

I de efterfølgende dage arbejdede telecentret videre med at fastlægge problemets mulige årsag og omfang, ligesom Rigspolitiet arbejdede på et foreløbigt udkast til teknisk notat om sagen. En første og foreløbig version af notatet dateret den 17. marts 2019 blev drøftet i Politiområdet den 19. marts 2019, hvor bl.a. politidirektøren, chefen for NEA og en række centerchefer var til stede. Det fremgik bl.a. af notatudkastet, at NC3 havde identificeret flere sager, hvor det blev vurderet, at politikredsene kunne have modtaget datasæt, hvor antallet af rækker med aktiviteter i konverteret data ikke var overensstemmende med det tilsvarende sæt rådata. Telecentret pegede – ud over fejl i timeropsætningen i konverteringssystemet – på fem forskellige mulige fejlkilder, herunder særligt på konvertering af særlige tjenester samt overførsel af teledata til politikredsene. Telecentret var dog ikke på daværende tidspunkt i stand til at afdække antallet af fejlbehæftede sager.

Den 20. marts 2019 deltog politidirektøren og chefen for NEA i et møde hos rigspolitichefen, som blev orienteret om sagen. Politidirektøren har oplyst, at rigspolitichefen blev orienteret grundigt om sagen og den konstaterede fejl i konverteringssystemet og om, at Justitsministeriet og Rigsadvokaturen blev orienteret straks efter, at Rigspolitiet blev opmærksom på sagens alvor den 13. marts 2019. Politidirektøren har endvidere oplyst, at rigspolitichefen blev orienteret om det planlagte møde mellem Justitsministeriet og Rigspolitiet den 27. marts 2019, hvor Justitsministeriet ifølge politidirektøren skulle gives en grundig indføring i sagen, og hvor de potentielle konsekvenser af de manglende data i konkrete straffesager skulle drøftes.

Rigspolitichefen har oplyst, at han på mødet den 20. marts 2019 blev orienteret om, at telecentret havde identificeret et antal sager, hvor politikredsene havde modtaget datasæt, hvor antallet af rækker i konverteret data ikke var i overensstemmelse med antallet af rækker i de tilsvarende sæt rådata. Telecentret vidste ikke, hvornår eller præcist hvordan uoverensstemmelsen var opstået, men vurderede, at det var sandsynligt, at en timer i konverteringssystemet var hovedårsagen til problemet. Timeren var nu fjernet. Man vidste ikke, hvor mange sager det drejede sig om. Rigspolitichefen har endvidere oplyst, at det ikke på mødet kunne oplyses, om diskrepansen mellem antallet af rækker havde haft reelle konsekvenser i de omfattede sager. Det blev på mødet særligt beskrevet, at der ikke var tale om egentlige fejl – men om, at der manglede oplysninger. Rigspolitichefen har derudover oplyst, at det på mødet blev understreget, at telecentret havde indført kontrolprocedurer, der ville sikre, at antallet af aktiviteter i rådata svarede til antallet af aktiviteter i konverterede data før videre sagsbehandling. Det blev på mødet aftalt hurtigst muligt at afdække problemets årsager, omfang og konsekvenser.

Den 22. marts 2019 forelå et revideret udkast til notatet af 17. marts 2019, hvor det bl.a. fremgik, at telecentrets undersøgelser havde vist, at der i perioden fra starten af 2012 til starten af marts 2019 kunne være sager, hvor politikredsene havde modtaget ufuldstændige teledatasæt fra Rigspolitiet. Om omfanget af problemstillingen fremgik det af notatet, at telecentret havde identificeret ca. 600 sager i 2017 og 2018, hvor politikredsene havde modtaget datasæt, hvor antallet af rækker med aktiviteter i konverteret data ikke var overensstemmende med antallet af rækker med aktiviteter i det tilsvarende sæt rådata. En yderligere gennemgang af telecentrets arkiv for teledata indikerede ifølge notatet, at der i årene fra 2012 til 2015 i gennemsnit var mindst 150 sager årligt med mangelfuld konverteret data. Det var dog telecentrets vurdering, at divergensen for årene 2012-2015 ikke reelt dækkede over en forskel mellem aktiviteter i rådata og konverteret data, da størsteparten af de identificerede sager dækkede over en sammenstillingsfejl på én række, og at dette var en kendt datasammenstillingsudfordring. Det konkluderedes i notatet, at fejlene i en meget stor del af de identificerede sager vedrørte særlige tjenester, og at konverteringen af særlige tjenester kunne have været ufuldstændig i perioden fra november 2016 til juni 2018.

Mødet mellem Rigspolitiet og Justitsministeriet, der var kalendersat til den 27. marts 2019, blev aflyst, og der blev efterfølgende aftalt et nyt møde om sagen til den 4. april 2019, som Rigsadvokaturen også blev indkaldt til.

5.3. April 2019

Den daværende chef for telecentret blev den 1. april 2019 midlertidigt overført til andet arbejde i Politiområdet. Baggrunden var, at flere medarbejdere opfattede, at den pågældende chef på et internt møde i telecentret den 27. marts 2019 havde bedt dem om at oplyse, at der blev gennemført kontroller, uanset om kontrollerne rent faktisk blev gennemført. Den pågældende chef søgte sin afsked og fratrådte den 31. maj 2019.

Chefen for NEA har oplyst, at det efterfølgende blev undersøgt, om de pågældende kontroller reelt var blevet udført, og at dette blev efterfølgende bekræftet af både telecentret og chefen for NC3.

Rigspolitichefen har oplyst, at teledatasagen – som et blandt flere emner – kort blev berørt i en telefonsamtale primo april 2019 med en afdelingschef i Justitsministeriet. Rigspolitichefen bekræftede, at der var ledelsesmæssigt fokus på sagen.

Mødet mellem Rigspolitiet, Justitsministeriet og Rigsadvokaturen, der var kalendersat til den 4. april 2019, blev aflyst. Der blev i stedet aftalt et nyt møde den 26. april 2019 mellem Rigspolitiet og Justitsministeriet. Rigsadvokaturen blev ikke indkaldt til dette møde.

Politidirektøren har oplyst, at han som følge af de aflyste møder med Justitsministeriet besluttede at arrangere et møde med Rigsadvokaturen om sagen. Mødet blev afholdt den 11. april 2019 med deltagelse af bl.a. politidirektøren, chefen for NEA og chefen for NC3. Fra Rigsadvokaturen deltog bl.a. statsadvokaten og vicestatsadvokaten. Politidirektøren har derudover oplyst, at Rigspolitiet på mødet oplyste om konverteringsfejlen på baggrund af den aktuelle viden, herunder at konverteringsfejlen kunne opstå i sager med mange data, men potentielt også i situationer, hvor mange sager med få data blev indlæst i systemet samtidig. I hvor lang en periode, fejlen havde stået på – og dermed hvor mange sager, fejlen potentielt kunne vedrøre – var på dette tidspunkt ikke klarlagt. På mødet oplyste Rigspolitiet derudover, at konverteringsfejlen var rettet, og at der var indført kontrolprocedurer, og man var i færd med at fremfinde data. Der fremkom på mødet ikke nærmere oplysninger om omfanget af sager med fejl, idet det blev oplyst, at Rigspolitiet fortsat arbejdede på at afdække fejlenes årsag, omfang og betydning.

Rigsadvokaturen har supplerende oplyst, at emnet blev drøftet som det sidste af to dagsordenspunkter på mødet den 11. april 2019, og at Rigspolitiet på mødet i al væsentlighed gentog indholdet af telefonsamtalen den 13. marts 2019, ligesom der blev redegjort for de tekniske aspekter i forbindelse med politiets indhentning og konvertering af teledata. Rigsadvokaturen har endvidere oplyst, at Rigspolitiet på mødet oplyste, at hovedmistanken fortsat var rettet mod en timerfejl, men at man også havde set indikationer på andre mulige fejl. En del mulige fejl viste sig dog ikke at være reelle fejl, når de blev undersøgt nærmere.

På mødet blev det bl.a. fremhævet af Rigsadvokaturen, at sagen ikke kun rejste spørgsmål om uopklarede sager, men også retssikkerhedsmæssige aspekter. Selv om risikoen var lav, ville det i sager baseret på indicier ikke kunne udelukkes at have haft bevismæssig betydning, hvis der havde manglet oplysninger om aktiviteter i den konverterede teledata, som f.eks. underbyggede et alibi. Der kunne derfor, afhængig af fejlenes karakter og betydning, potentielt opstå spørgsmål om sager, som skulle ankes eller genoptages. Derudover var der en drøftelse af, hvordan sager med fejl ville skulle håndteres, herunder rollefordelingen mellem Rigspolitiet, politikredsene og anklagemyndigheden.

Rigspolitiet arbejdede på daværende tidspunkt ud fra en forventning om, at gennemgangen af sager kunne være afsluttet inden sommerferien. Det blev endvidere oplyst, at der var aftalt møde med Justitsministeriet om sagen efter påske, hvor også Rigsadvokaturen ville blive indkaldt. Ved afslutningen af mødet udleverede Rigspolitiet to tekniske notater udarbejdet af Politiområdet dateret henholdsvis samme dag og den 9. april 2019 samt Rigspolitiets vejledning, som fremsendes til rekvirenter af teledata. Det udleverede materiale blev ikke nærmere gennemgået.

Af notatet af 11. april 2019 fremgik det bl.a., at særligt store datasæt kunne være et problem for politiets konverteringssystem som følge af en timerindstilling. Det fremgik endvidere, at timerindstillingen kunne betyde, at konverteringsfejlen ligeledes kunne opstå, hvor mange datasæt – uanset størrelse – skulle konverteres i forlængelse af hinanden, således at der var dannet en kø i konverteringssystemet. Disse forhold vurderedes afhjulpet, og det var således vurderingen, at disse ikke ville kunne give anledning til problemer fremadrettet. Om omfanget af problemstillingen fremgik det af notatet – i lighed med den foreløbige version af 22. marts 2019 – at telecentret havde identificeret ca. 600 sager i 2017 og 2018, hvor politikredsene havde modtaget mangelfulde datasæt. Det vurderedes i notatet, at den manglende data i en meget stor del af de identificerede sager vedrørte datatypen særlige

tjenester, og at konverteringen af datatypen kunne have været ufuldstændig i perioden fra november 2016 til juni 2018. I notatet blev det fremhævet, at det ikke var muligt med sikkerhed at fastslå, om de identificerede problemer i konkrete tilfælde reelt havde påvirket politiets efterforskning. Notatet oplyste herudover om fejl i tilfælde, hvor samme telefon kunne være registreret på flere forskellige master på samme tidspunkt, trods stor indbyrdes afstand mellem masterne.

Den 17. april 2019 fremsendte chefen for NC3 et udkast til en plan for gennemgang af historiske sager til chefen for NEA. Planen var dateret til den 15. april 2019, og det fremgik bl.a. heraf, at der blev lagt op til at etablere et såkaldt 'digitalt rejsehold' for henholdsvis Østdanmark og Vestdanmark, som skulle bistå med at udfinde og gennemgå relevante straffesager samt genskabe teledatahistorik i muligt omfang. Af planen fremgik det bl.a., at arbejdet skulle vedrøre rekvisitioner for perioden fra den 1. januar 2012 til den 8. marts 2019. Telecentrets undersøgelser pegede på, at fejlen kunne være opstået i 2013. For at afklare, om denne antagelse var korrekt, skulle sager fra 2012 også gennemgås. Til brug for arbejdet skulle der indledningsvis foretages genindlæsning af historiske teleoplysninger indhentet i den pågældende periode. Genindlæsningen af data var påbegyndt i telecentret i begyndelsen af april 2019 og forventedes at være afsluttet i midten af april 2019. Herudover blev der lagt op til, at telecentret ville indhente erfaringer fra Københavns Vestegns Politi og Midt- og Vestsjællands Politi, som ifølge det oplyste af egen drift i marts 2019 og begyndelsen af april 2019 havde gennemgået et antal ældre sager med telerekvisitioner. På baggrund af erfaringerne i Københavns Vestegns Politi og Midt- og Vestsjællands Politi skulle det digitale rejsehold påbegynde arbejdet i henholdsvis Østjyllands Politi og Københavns Vestegns Politi i uge 19 og Københavns Politi i uge 20. Der var lagt op til, at indsatsen herefter skulle evalueres, og at alle øvrige kredse ville få besøg af det digitale rejsehold inden udgangen af uge 26.

Den 26. april 2019 blev der afholdt møde mellem Justitsministeriet og Rigspolitiet om sagen. Rigsadvokaturen blev ikke indkaldt til mødet. På mødet deltog bl.a. politidirektøren, chefen for NEA, chefen for NC3 samt en afdelingschef og flere kontorchefer fra Justitsministeriet. Politidirektøren har oplyst, at Rigspolitiet på mødet grundigt redegjorde for sagen, herunder om hvordan fejlen opstod. Politidirektøren har oplyst, at Rigspolitiet endvidere oplyste, at det på dette tidspunkt fortsat ikke var afklaret, hvor lang tid fejlen havde stået på. Politidirektøren har endvidere oplyst, at han – som følge af, at Rigsadvokaturen ikke var repræsenteret på mødet – nævnte den bekymring, som Rigsadvokaturen havde rejst på

mødet den 11. april 2019 om, at de manglende teledata kunne have haft betydning for domstolenes afgørelse i sager, hvor afgørelsen baserede sig på en sum af indicier. Politidirektøren har desuden oplyst, at det var hans vurdering, at politiet derfor potentielt stod over for at skulle gennemgå en meget stor mængde af sager. Politidirektøren har endelig oplyst, at Justitsministeriet på mødet tilkendegav, at ministeriet ønskede en oversigt over og vurdering af betydningen for drabssager, hvor der var rekvireret teledata. Politidirektøren har afslutningsvis oplyst, at det blev aftalt at afholde et møde mellem Justitsministeriet og Rigspolitiet om teledatafejlenes betydning for drabssager.

Rigspolitiet iværksatte efter mødet med Justitsministeriet en gennemgang af drabssager, hvor politiet i perioden fra den 1. januar 2012 til den 8. marts 2019 som led i efterforskningen havde indhentet teledata. Arbejdet med at identificere disse sager i telecentrets system blev afsluttet den 9. maj 2019, hvor der var identificeret i alt 124 drabssager i den pågældende periode, hvori der var indhentet teleoplysninger.

5.4. Maj 2019

Den 1. maj 2019 drøftede chefen for NC3 og vicestatsadvokaten kort muligheden for at arrangere et fælles møde med Østjyllands Politi med henblik på at udmønte Rigspolitiets plan for gennemgang af historiske sager. Chefen for NC3 oplyste, at Rigspolitiet under mødet med Justitsministeriet den forudgående uge havde orienteret Justitsministeriet om problematikken og Rigspolitiets foreløbige overvejelser om processen for gennemgang af berørte sager.

Den 2. maj 2019 blev sagen, som tidligere havde været kort omtalt for rigsadvokaten, drøftet på et internt møde i Rigsadvokaturen. I mødet deltog statsadvokaten, vicestatsadvokaten og rigsadvokaten. Der var på mødet enighed om, at forsvarere og domstolene ville skulle orienteres om fejlen, ligesom der ville være behov for generelt at melde ud om konverteringsfejlen hos Rigspolitiet.

I forlængelse heraf meddelte vicestatsadvokaten den 3. maj 2019 chefen for NC3, at Rigsadvokaturen ville udarbejde en orienteringsskrivelse til forsvarerne og domstolene om konverteringsfejlen og de mulige konsekvenser heraf, og at der ville være behov for at melde generelt ud om problemstillingen. Denne beslutning førte ikke til ændringer i Rigspolitiets plan om at påbegynde en gennemgang af muligt berørte straffesager.

Den 3. maj 2019 orienterede Rigsadvokaturen de regionale statsadvokater om sagen.

Den 7. maj 2019 holdt bl.a. chefen for NEA, chefen for NC3, repræsentanter fra telecentret og en repræsentant fra Rigsadvokaturen møde med chefpolitiinspektøren og chefanklageren ved Østjyllands Politi med henblik på hurtigst muligt at iværksætte sagsgennemgangen. Chefen for NEA tilkendegav på mødet, at Rigspolitiet foreløbigt ønskede at forholde sig reaktivt rent pressemæssigt. Repræsentanten fra Rigsadvokaturen tilkendegav, at Rigsadvokaturen ville sende et orienteringsbrev til forsvarerne. Chefen for NEA bemærkede i forbindelse med mødet, at politidirektøren ønskede at blive orienteret, inden Rigsadvokaturen sendte orienteringsbrevet.

Den 9. maj 2019 blev chefen for NEA og chefen for NC3 – som opfølgning på mødet i Justitsministeriet den 26. april 2019 – indkaldt til møde i Justitsministeriet om teledata. Mødet blev aftalt til den 16. maj 2019. Mødet blev efterfølgende flyttet til den 27. maj 2019.

Den 9. maj 2019 sendte NC3 en opgørelse over relevante historiske sager i perioden fra 2017 til 2019 til Østjyllands Politi med henblik på, at kredsen kunne gennemgå sager fra denne periode.

Den 10. maj 2019 blev et tillægsnotat til notatet af 11. april 2019 om teledata fremsendt til politidirektøren og chefen for NEA. Det fremgik bl.a. af tillægsnotatet, at en opdateringsfil i konverteringssystemet vurderedes at være årsagen til de konverteringsfejl, der var beskrevet i notatet af 11. april 2019. Det fremgik desuden af tillægsnotatet, at opdateringsfilen i Rigspolitiets konverteringssystem kunne være indlæst i perioden fra den 24. maj 2013 til den 25. februar 2014. Det bemærkedes afslutningsvist i tillægsnotatet, at timeren blev fjernet den 8. marts 2019.

Som følge af tillægsnotatet blev det af politidirektøren besluttet, at undersøgelsesperioden skulle gå tilbage til og med 2012 fra det tidspunkt, hvor det eksisterende rekvisitionssystem blev etableret. Derved sikredes en kontrolperiode for hypotesen om, at systemopdateringsfejlen fra 2013 var årsagen til konverteringsfejlen.

Den 10. maj 2019 drøftede chefen for NC3 og vicestatsadvokaten mere generelt status i sagen. Vicestatsadvokaten har oplyst, at politidirektøren deltog under den sidste del af telefonsamtalen, og at politidirektøren i den forbindelse spurgte til behovet for at orientere forsvarerne, hvis det f.eks. viste sig, at fejlene var uden betydning. Vicestatsadvokaten oplyste, at det var besluttet af rigsadvokaten og skulle ses i lyset af forsvarerens ret til aktindsigt i alle oplysninger tilvejebragt til brug for en straffesag.

Samme dag drøftede politidirektøren sagen med statsadvokaten i kanten af et andet møde.

Politidirektøren tilkendegav, at Rigspolitiet ønskede at igangsætte forundersøgelsen i Østjyllands Politi, for over to uger at få erfaringer med, hvordan processen med fremfinding og gennemgang af sager kunne gennemføres for hele landet. Rigsadvokaturen har supplerende oplyst, at politidirektøren også tilkendegav, at Rigspolitiet ønskede et bedre vidensgrundlag, inden Rigsadvokaturen orienterede forsvarerne. Politidirektøren fandt derfor, at udsendelsen af orienteringsbrevet skulle afvente resultaterne fra sagsgennemgangen i Østjyllands Politi, som forventedes at foreligge inden for to uger. Statsadvokaten tog dette til efterretning.

Den 13. maj 2019 gik Rigsadvokaturen i gang med at udarbejde et foreløbigt udkast til orienteringsbrev til forsvarere og domstolene.

Den 16. maj 2019 orienterede vicestatsadvokaten de regionale statsadvokater om, at Rigspolitiet havde oplyst, at gennemgangen af sager i Østjyllands Politi blev forsinket, men at Rigsadvokaturen fortsat håbede at kunne sende et generelt orienteringsbrev til forsvarerne den følgende uge.

Den 21. maj 2019 anmodede Rigsadvokaturen om Rigspolitiets eventuelle bemærkninger til et første udkast til orienteringsbrev.

Den 23. maj 2019 forespurgte vicestatsadvokaten politidirektøren til, om Rigspolitiet havde bemærkninger til det fremsendte brev, idet Rigsadvokaturen gerne ville sende brevet samme uge. Politidirektøren bemærkede dertil, at Rigspolitiet ville sætte pris på, hvis Rigsadvokaturen kunne vente til den følgende uge, når Rigspolitiet var færdige med gennemgangen i Østjyllands Politi. Vicestatsadvokaten anmodede om en uddybning af baggrunden for at vente, da Rigsadvokaturen fortsat ønskede at sende brevet ud så tidligt som muligt.

Samme dag kontaktede kommunikationschefen hos Rigsadvokaturen vicestatsadvokaten og oplyste, at Rigspolitiets kommunikationsdirektør (herefter kommunikationsdirektøren) over for ham havde rejst spørgsmålet om, hvorvidt Rigspolitiet og Rigsadvokaturen kunne udsende brevet til forsvarerne under valgkampen.

Politidirektøren blev ligeledes kontaktet af kommunikationsdirektøren med henblik på at høre politidirektørens vurdering af, om Statsministeriets skrivelse om den parlamentariske situation efter udskrivelse af valg havde betydning for, hvornår Rigsadvokaturen kunne sende et brev om teledatasagen til forsvarsadvokaterne mv. Politidirektøren afviste i den forbindelse, at Statsministeriets skrivelse kunne have betydning herfor.

Senere samme dag drøftede politidirektøren og vicestatsadvokaten processen vedrørende orienteringsbrevet. Der var under samtalen enighed om, at valgkampen var uden betydning for orienteringen af forsvarerne. Derudover blev den videre proces drøftet.

Rigsadvokaturen har oplyst, at politidirektøren fastholdt, at resultaterne fra sagsgennemgangen i Østjyllands Politi var afgørende for at kunne informere ordentligt om sagen og tilrettelægge en hensigtsmæssig fremadrettet proces, hvilket vicestatsadvokaten tog til efterretning.

Efterfølgende orienterede vicestatsadvokaten statsadvokaten om samtalen.

Den 24. maj 2019 orienterede statsadvokaten på forespørgsel rigsadvokaten om den planlagte proces i det, der internt hos Rigsadvokaturen blev omtalt som 'mastesugsagen'. Statsadvokaten oplyste, at Rigspolitiet fortsat var usikre i forhold til problemets omfang, og at man afventede sagsgennemgangen i Østjyllands Politi. Planen var, at orienteringsbrevet til forsvarerne skulle udsendes i starten af den følgende uge. Der var enighed om, at det gav god mening at blive klogere på problemets omfang og mulige konsekvenser, før at man meldte ud, men at det samtidig var en balance.

Den 27. maj 2019 efterspurgte vicestatsadvokaten Rigspolitiets bemærkninger til udkastet til orienteringsbrevet. Vicestatsadvokaten tilkendegav i den forbindelse, at Rigsadvokaturen meget gerne ville have bemærkninger samme dag, da Rigsadvokaturen ville udsende brevet den følgende dag. Politidirektøren fremsendte kort efter Rigspolitiets bemærkninger

til brevet. Af bemærkningerne fremgik det bl.a., at Rigspolitiet foreslog, at oplysningen i brevet om, at sagsgennemgangen forventedes at vare 2-3 måneder, blev ændret til 4-5 måneder. I forbindelse med fremsendelsen af bemærkningerne oplyste politidirektøren, at han ønskede 'at vende timing mv. endnu en gang', inden Rigsadvokaturen sendte brevet. Rigsadvokaturen svarede kort efter, at man havde indarbejdet ændringerne, idet tidshorisonten for sagsgennemgangen dog var ændret til 'hurtigst muligt'.

Det planlagte møde i Justitsministeriet med Rigspolitiet den 27. maj 2019 blev aflyst.

Rigsadvokaturen har oplyst, at politidirektøren den 28. maj 2019 kontaktede statsadvokaten og oplyste, at Rigspolitiet ønskede det tekniske afsnit om it-fejlen i orienteringsbrevet udbygget. Rigspolitiet ønskede endvidere, at det af brevet fremgik, at konverteringsfejlen var rettet.

Samme aften anmodede vicestatsadvokaten efter aftale med statsadvokaten politidirektøren om at fremsende Rigspolitiets uddybende tekniske beskrivelse af it-fejlen og nærmere oplysninger, om hvordan fejlen var rettet, med henblik på at oplysningerne kunne indgå i orienteringsbrevet til forsvarerne.

Dagen efter drøftede rigsadvokaten og statsadvokaten sagen. Det blev besluttet at igangsætte orienteringsprocessen af forsvarerne ved at indkalde til et ekstraordinært møde i Kontaktudvalget mellem Advokatrådet, Landsforeningen af Forsvarsadvokater og anklagemyndigheden (herefter Kontaktudvalget). Rigsadvokaturen foreslog den 6. og 11. juni 2019 som mulige mødedatoer. Af mødeindkaldelsen fremgik det, at formålet med mødet var at drøfte en 'særlig problemstilling'. Statsadvokaten orienterede samme dag en afdelingschef i Justitsministeriet om indkaldelsen.

Senere samme uge kontaktede Advokatrådets repræsentant statsadvokaten for at høre til, hvad mødet handlede om. Statsadvokaten oplyste, at det drejede sig om fejl i teleoplysninger.

5.5. Juni 2019

Den 3. juni 2019 blev teledatasagen og Rigspolitiets foreløbige presseberedskab drøftet ved et møde hos rigspolitichefen. På mødet deltog foruden rigspolitichefen også kommunikationsdirektøren, politidirektøren og chefen for NEA. I kanten af mødet blev det drøftet, at

det ikke kunne udelukkes, at konverteringsfejlen gik længere tilbage end 2012, men at der på daværende tidspunkt var enighed om, at der ikke var grundlag for, at telecentrets undersøgelse – på baggrund af centrets daværende hypoteser – gik længere tilbage end 2012.

Statsadvokaten oplyste den 3. juni 2019 politidirektøren og chefen for NEA om, at der var aftalt et møde med forsvarerne den 6. juni 2019, og at Rigsadvokaturen ønskede, at Rigspolitiet deltog i mødet med henblik på at orientere om sagen og svare på spørgsmål.

Samme dag orienterede chefen for NEA vicestatsadvokaten om de foreløbige resultater af sagsgennemgangen hos Østjyllands Politi, som ikke havde givet den forventede afklaring.

Chefen for NEA har oplyst, at han den 4. juni 2019 deltog i et møde med to afdelingschefer i Justitsministeriet, hvor bl.a. teledatasagen og Rigspolitiets udkast til plan for gennemgang af sager, hvor der var rekvireret historiske teledata, blev drøftet. Chefen for NEA har endvidere oplyst, at der – som aftalt på mødet – efterfølgende blev udleveret et udkast til Rigspolitiets presseberedskab i teledatasagen til Justitsministeriet den 6. juni 2019 i forbindelse med et andet møde mellem Justitsministeriet og Rigspolitiet.

Den 5. juni 2019 forelå tillægsnotat nr. 2 til Rigspolitiets notat af 11. april 2019. Tillægsnotatet omhandlede fejl i konverteringen af historiske teledata i de tilfælde, hvor politikredsene alene havde anvendt et separat analyseværktøj, som var til rådighed i kredsene, frem for alene anvende materiale modtaget fra telecentret, der indlæste rådata i analyseværktøjet. Det fremgik endvidere af tillægsnotatet, at tre aktivitetstyper (”særlige tjenester”, ”tjenesteydelser” og ”masteoplysning”) ikke blev indlæst i det separate analyseprogram i forbindelse med modtagelsen af historiske teleoplysninger og historiske masteoplysninger, og at efterforskere, der alene anvendte oplysninger fra dette analyseværktøj, således potentielt ikke havde modtaget det fulde datasæt. Det vurderedes, at der var tale om fejl i ca. 40 rekvisitioner, og det blev anført i notatet, at analyseværktøjet forventedes opdateret snarest muligt, og at fejlen dermed forventedes rettet.

Rigspolitiet færdiggjorde ligeledes samme dag en justeret tidsplan for processen med gennemgang af sager, hvor der var rekvireret historiske teledata. NC3 vurderede i den forbindelse, at der var behov for en gennemgang af 10.776 sager i perioden fra 2012 til 2019 indeholdende ca. 40.000 rekvisitioner af teledata.

Den 5. juni 2019 modtog rigspolitichefen, politidirektøren og Rigspolitiets kommunikationsdirektør fra chefen for NEA – som forberedelse til koncernledelsesmødet dagen efter – planen for håndteringen af de historiske straffesager indeholdende teledatarekvisitioner. Endvidere modtog de pågældende Rigspolitiets opdaterede presseberedskab og udkastet til orienteringsbrev til forsvarerne.

Samme dag fremsendte Rigspolitiet supplerende bemærkninger til Rigsadvokaturens udkast til orienteringsbrev til forsvarerne med bl.a. en uddybning af det tekniske afsnit og de gennemførte undersøgelser.

Den 6. juni 2019 blev der afholdt møde i koncernledelsen for politiet og anklagemyndigheden, hvor rigspolitichefen orienterede om sagen, herunder at der var konstateret uoverensstemmelser mellem rådata indhentet fra teleselskaberne og konverterede data i Rigspolitiet. Det blev oplyst, at fejlen var blevet rettet, men at de konstaterede uoverensstemmelser betød, at der skulle gennemgås godt 10.000 straffesager i politikredsene fra 2012 og frem med henblik på at undersøge, om tilvejebragt teledata i fuldt omfang var indgået i sagen. Rigspolitichefen gennemgik kort det forestående omfattende arbejde inkl. tidsplanen herfor og oplyste, at alle kredse i uge 24 ville blive orienteret nærmere. I forlængelse heraf oplyste rigsadvokaten, at anklagemyndigheden ville tage hånd om den nødvendige orientering af forsvarsadvokaterne.

Mødet i Kontaktudvalget blev afholdt samme dag. På mødet deltog bl.a. rigsadvokaten, statsadvokaten, vicestatsadvokaten, statsadvokaten i København, chefanklageren i Københavns Politi, chefen for NEA samt repræsentanter fra Advokatrådet og Landsforeningen af Forsvarsadvokater. På mødet orienterede chefen for NEA om konverteringsfejlen, resultaterne fra sagsgennemgangen i Østjylland, og om at Rigspolitiet vurderede, at der var behov for en gennemgang af 10.776 sager i perioden fra 2012 til 2019. Tilrettelæggelsen af sagsgennemgangen blev drøftet med forsvarsadvokaterne, og det blev bl.a. aftalt, at sager med aktuelt frihedsberøvede skulle prioriteres først.

På baggrund af mødet i Kontaktudvalget blev Rigspolitiets plan for gennemgang af straffesager i politikredsene justeret, således at alle sager med afsonere og varetægtsfængslede ville blive gennemgået først. NC3 gennemførte særskilte videomøder den 11. og 12. juni 2019 med hver politikreds med henblik på orientering om teledatasagen og håndtering af den forestående opgave med at identificere og gennemgå muligt berørte straffesager.

I dagene efter mødet den 6. juni 2019 blev udkastet til Rigsadvokaturens orienteringsbrev til forsvarerne justeret, bl.a. under henvisning til de tilkendegivelser om sagernes prioritering, som blev fremsat på mødet. Endvidere blev det tilføjet, at fejlen vurderedes at være opstået i perioden fra 2012 til 2019.

Rigspolitiet præciserede ved e-mail af 7. juni 2019 det tekniske afsnit med beskrivelse af fejlen i udkastet til orienteringsbrev til forsvarerne, ligesom det blev tilføjet, at fejlen var rettet i starten af marts 2019, og at der var indført en manuel kontrolprocedure. I de følgende dage blev det præciseret, at fejlen var rettet den 8. marts 2019, ligesom Rigsadvokaturen efter nærmere overvejelser besluttede, at uddybningen af det tekniske afsnit burde udgå.

Efter justeringerne af udkastet til orienteringsbrevet til forsvarerne, jf. ovenfor, fremsendte Rigsadvokaturen den 11. juni 2019 en revideret version af brevet til de regionale statsadvokater og Rigspolitiet med henblik på deres eventuelle bemærkninger. Efter indarbejdelse af bemærkninger blev udkastet forelagt rigspolitichefen og rigsadvokaten. Centrale dele af udkastet til brevet blev desuden læst op for formanden for Landsforeningen af Forsvarsadvokater.

Orienteringsbrevet til forsvarerne blev afsendt den 13. juni 2019 med kopi til Domstolsstyrelsen. Samme dag udsendte Rigsadvokaturen en instruks til alle embeder om gennemgangen af straffesager, hvori der indgik teleoplysninger. Det fremgik af instruksen, at konverteringsfejlen alene medførte, at der kunne mangle teleoplysninger, men ikke at der var indholdsmæssige fejl i teleoplysninger.

Chefen for NC3 sendte den 13. juni 2019 en e-mail til samtlige politikredse om status på arbejdet med teledatasagen i forhold til den gennemgang af straffesager, som politikredsene skulle i gang med. I e-mailen blev det oplyst, hvordan politikredsene skulle prioritere sagerne, herunder at sager med frihedsberøvede personer skulle gennemgås først.

Samme dag forelå Rigspolitiets endelige udkast til presseberedskaber med bemærkninger fra Rigsadvokaturen indarbejdet. Det fremgik bl.a. af presseberedskabet, at Rigspolitiet havde konstateret en konverteringsfejl vedrørende teledata, og at Rigspolitiet vurderede, at der var tale om en teknisk fejl i det dataprogram, der blev anvendt til at konvertere teledata. Det fremgik endvidere, at fejlen udsprang af en opdatering af systemet, og at data kunne

have været ufuldstændige. Om omfanget af fejlen fremgik det bl.a. af presseberedskabet, at NC3 havde foretaget en gennemgang af alle teledatarekvisitioner i 2018, og at der var konstateret forskel i optællingen i 417 rekvisitioner, svarende til knap 10 pct. af alle rekvisitioner i 2018. I samarbejde med Østjyllands Politi havde NC3 for årene 2017-2019 kortlagt uoverensstemmelser i 24 af 75 sager.

Samtidig med afsendelsen af den endelige godkendelse af presseberedskabet modtog chefen for NEA en skriftlig orientering fra chefen for NC3, hvoraf det fremgik, at telecentret den 12. juni 2019 var blevet opmærksom på, at det i en konkret straffesag i Østjyllands Politi, hvori der blev foretaget aflytning, var konstateret, at der fremgik opkald, som ikke var at finde i de historiske konverterede teledataoplysninger. Efter dialog med det relevante teleselskab kunne telecentret konstatere, at alle bestillinger af historiske teleoplysninger fra det konkrete teleselskab i perioden fra den 1. august 2018 til den 10. januar 2019 manglede oplysninger om nyere internetbaserede samtaletjenester. Fra den 10. januar 2019 havde det pågældende teleselskab dog opdateret de historiske teledata for disse former for samtaletrafik tilbage til primo november 2018. Ved en rundringning til de øvrige teleselskaber kunne det konstateres, at et andet teleselskab heller ikke leverede fuldstændige datasæt fra disse tjenester.

Chefen for NEA orienterede den 13. juni 2019 politidirektøren samt en række centerchefer om sagen. Chefen for NEA informerede endvidere samme dag vicestatsadvokaten telefonisk om problemstillingen. Den samlede problemstilling blev endvidere beskrevet i et notat af 1. juli 2019 om nyere internetbaserede samtaletjenester i historiske teleoplysninger.

De følgende dage arbejdede NC3 videre med tilrettelæggelsen af sagsgennemgangen i politikredsene. Chefen for NEA blev endvidere interviewet af pressen om teledatasagen og tilkendegav, at Rigspolitiet i november 2018 var blevet bekendt med, at de konverterede teleoplysninger i en konkret sag havde været mangelfulde.

Den 17. juni 2019 holdt Rigsadvokaturen et videomøde med deltagelse af bl.a. de regionale statsadvokater og chefanklagere fra alle politikredse om bl.a. håndtering af verserende sager.

På baggrund af gengivelsen i pressen af oplysningen om, at Rigspolitiet i november 2018 var blevet bekendt med, at de konverterede teledata i en konkret sag havde været mangelfulde – og drøftelser på et møde for alle landets chefpolitiinspektører i Rigspolitiet den 19. juni 2019 – gjorde to politikredse den 19. juni 2019 Rigspolitiet opmærksom på, at det var politikredsenes opfattelse, at Rigspolitiet også før november 2018 var bekendt med problemet med manglende oplysninger i konverterede teledata. Således oplyste Østjyllands Politi til chefen for NEA, at kredsen i februar 2018 blev opmærksom på konverteringsfejl, og at politikredsen i februar 2018 indmeldte dette til telecentret. Det blev endvidere anført, at politikredsen mente, at den fejl, der havde været omtalt i medierne, var identificeret i august 2018, og at kredsen også reagerede herpå. Afslutningsvist var det anført, at politikredsen havde konstateret op mod 30 forskellige fejltyper på teledataområdet, som var indmeldt til Rigspolitiet. Det fremgik ikke af henvendelsen, hvilke fejltyper det drejede sig om, ligesom det ikke var anført, om der alene var tale om fejl vedrørende konverterede teledata.

Chefen for NEA orienterede umiddelbart herefter rigspolitichefen og politidirektøren, og der blev samme dag holdt et møde om sagen med yderligere deltagelse af koncernstyringsdirektøren og kommunikationsdirektøren. For bl.a. at afdække, hvornår kendskabet til den udmeldte konverteringsfejl var opstået, blev det besluttet at bede Rigspolitiets Enhed for Tilsyn og Controlling (herefter ToC) om at igangsætte en intern undersøgelse af telecentrets ledelsesmæssige fokus på samt arbejdsgange og kontroller for håndtering af eventuelle kritiske fejl i teledata.

Den 19. juni 2019 gjorde Københavns Politi endvidere Rigspolitiet opmærksom på, at en automatiseret tællekontrol, som blev indført den 8. marts 2019, i en konkret sag ikke i alle tilfælde havde foretaget en korrekt optælling. Telecentret gennemgik på den baggrund alle rekvisitioner for perioden fra den 8. marts 2019 til den 19. juni 2019 og konstaterede herved, at der i ganske få tilfælde havde været fejl i den automatiserede tællekontrol. Sagerne blev derfor efter det oplyste gennemgået på ny for at sikre overensstemmelse mellem antallet af aktiviteter i rådata og konverterede data. Telecentret har oplyst, at tællefejlen i tællemekanismen blev rettet den 19. juni 2019.

Den 20. juni 2019 fremsendtes notatet af 11. april 2019 om visse forhold knyttet til håndtering af teledata i politiet – inkl. tillægsnotat 1 og 2 – for første gang til rigspolitichefen

og koncernstyringsdirektøren. Rigspolitichefen og koncernstyringsdirektøren blev endvidere oplyst, at der i den kommende tid ville blive udarbejdet endnu et tillægsnotat om de såkaldte nyere internetbaserede samtaletjenester som omtalt ovenfor.

Den 21. juni 2019 afholdt Rigspolitiet og Rigsadvokaturen et videomøde med alle politikredsene samt de regionale statsadvokater, SØIK og PET om den videre proces for gennemgangen af de berørte straffesager. Der blev samme dag udarbejdet et faktaark til brug for den lokale anklagemyndigheds anvendelse af teledata under verserende straffesager ved retterne.

Den 23. juni 2019 genfremsendte Østjyllands Politi tre henvendelser til Rigspolitiet af februar, marts og juni 2019, hvor det af henvendelsen af februar 2019 bl.a. fremgik, at politikredsen var blevet opmærksom på, at teleselskaberne ikke kunne fejlrette eller undersøge en fejlagtig masteposition. I henvendelsen af marts 2019 oplyste politikredsen, at et teleselskab ikke gemte masteoplysninger på internetbaserede samtaletjenester. I den tredje henvendelse – af juni 2019 – oplyste politikredsen, at politikredsen i en konkret efterforskning havde oplevet udfordringer med mastepositioner.

Med virkning fra den 24. juni 2019 blev telecentret organisatorisk flyttet fra NC3 til NKC. Samtidig ændredes referenceforholdene, således at chefen for NKC fremadrettet skulle referere til politidirektøren i sager vedrørende telecentret.

Derudover blev en vicepolitiinspektør ansat som chef for telecentret, da politidirektøren ønskede en stærkere lederprofil i telecentret. Samtidig blev der ansat en erfaren projektleder fra Københavns Politi. Politidirektøren har oplyst, at de bl.a. fik til opgave at skabe et struktureret overblik over de udfordringer og unøjagtigheder, som telecentret løbende fik indblik i ved den daglige dialog med politikredsene. Derudover har politidirektøren oplyst, at der var behov for mere struktur ved indsamling og formidling af konstaterede udfordringer og uhensigtsmæssigheder i data, og de to skulle hjælpe centrets medarbejdere til at opbygge et sådant struktureret vidensoverblik.

Umiddelbart efter sin tiltrædelse påbegyndte chefen for telecentret arbejdet med en samlet oversigt over fejlkilder og øvrige udfordringer med teledata.

Den 26. juni 2019 orienterede Justitsministeriet Rigsadvokaturen om, at ministeren påtænkte at nedsætte en uafhængig kontrol- og styregruppe, som skulle godkende de nærmere retningslinjer for politiets og anklagemyndighedens gennemgang af straffesager, hvori teleoplysninger var indgået.

Efterfølgende modtog Rigsadvokaturen og Rigspolitiet et første udkast til kommissorium for den uafhængige gruppe med tilhørende bilag fra Justitsministeriet med henblik på faktatjek.

Den 27. juni 2019 afgav Rigsadvokaturen faktuelle bemærkninger til Justitsministeriet.

Politidirektøren har oplyst, at rigspolitichefen samme dag orienterede ham om, at Justitsministeriet telefonisk havde tilkendegivet, at orientering om større sager – herunder udviklingen i større sager – ikke fremadrettet kunne ske telefonisk. Politidirektøren har oplyst, at orienteringer af den art skulle være tilstrækkeligt belyst til at kunne foreligge skriftligt.

Den 28. juni 2019 modtog Rigspolitiet og Rigsadvokaturen et opdateret kommissorium med tilhørende bilag fra Justitsministeriet. Samtidig oplyste ministeriet Rigsadvokaturen, at ministeren forventede at gå ud med nyheden om nedsættelsen af en uafhængig kontrol- og styregruppe den 1. juli 2019.

Den 30. juni 2019 drøftede statsadvokaten og vicestatsadvokaten, om kommissoriet for en uafhængig kontrol- og styregruppe tog højde for den problemstilling om manglende teledata vedrørende nyere internetbaserede samtaletjenester, som chefen for NEA havde omtalt telefonisk over for vicestatsadvokaten den 13. juni 2019. Drøftelserne førte til, at statsadvokaten og vicestatsadvokaten samme dag kontaktede chefen for NEA og spurgte nærmere ind til betydningen af den omtalte fejl.

Chefen for NEA oplyste under telefonsamtalen bl.a., at han på et møde den 24. juni 2019 havde aftalt med politidirektøren, at politidirektøren ville orientere Rigsadvokaturen om muligt nyt i sagen, og at det derfor undrede ham, at Rigsadvokaturen ikke havde hørt om, at der den 19. juni 2019 var sket en opdateringen i sagen.

Statsadvokaten kontaktede umiddelbart herefter politidirektøren telefonisk. Politidirektøren bekræftede under telefonsamtalen, at han ikke havde orienteret Rigsadvokaturen om

opdateringen i sagen, da der efter hans opfattelse ikke var substantielt nyt i opdateringen af den 19. juni 2019 – i forhold til den opdatering, som Rigsadvokaturen havde fået den 13. juni 2019 – og at fejlene desuden ville blive håndteret i dialog med teleudbyderne og i forbindelse med den iværksatte sagsgennemgang. Rigsadvokaturen har oplyst, at statsadvokaten gav udtryk for, at han ikke mente, at fejlene ville blive opdaget ved sagsgennemgangen, da der var tale om mangler i rådata, og at han derfor ikke var overbevist om, at fejlene var uden betydning.

Statsadvokaten orienterede med det samme rigsadvokaten om samtalen. Det blev aftalt, at statsadvokaten skulle orientere Justitsministeriet om problemstillingen, og at rigsadvokaten skulle orientere rigspolitichefen. Statsadvokaten kontaktede herefter en kontorchef i Justitsministeriet. Rigsadvokaten orienterede samtidig rigspolitichefen. Der var enighed om, at Rigspolitiet måtte vurdere nærmere, om de omtalte fejl var af en sådan karakter, at de efter Rigspolitiets opfattelse kunne have betydning for straffesagsbehandlingen. I så fald skulle Rigsadvokaturen orienteres skriftligt herom, ligesom der også fremadrettet skulle orienteres skriftligt om fejl, som kunne have betydning for straffesagsbehandlingen, sådan at Rigsadvokaturen på baggrund heraf kunne foretage en reel vurdering af fejlenes betydning for straffesagsbehandlingen.

Rigspolitichefen kontaktede efterfølgende politidirektøren og understregede, at Rigsadvokaturen fremadrettet hurtigst muligt skulle orienteres skriftligt om fejl, som kunne have betydning for straffesagsbehandlingen.

Rigspolitichefen har oplyst, at han ønskede friske øjne på sagen og derfor den 30. juni 2019 aftalte med koncernstyringsdirektøren, at koncernstyringsdirektøren skulle koordinere Rigspolitiets bemærkninger til det brev til Folketingets Retsudvalg, som Justitsministeriet forberedte, således at problemstillingen med nyere samtaletjenester også blev reflekteret.

5.6. Juli 2019

Den 1. juli 2019 blev der afholdt et møde mellem bl.a. politidirektøren, koncernstyringsdirektøren og chefen for telecentret. Chefen for NEA deltog indledningsvis og redegjorde for teledatasagens udfordringer. Efterfølgende gennemgik chefen for telecentret en liste over kendte udfordringer og unøjagtigheder i teledata. Politidirektøren har oplyst, at der efter gennemgangen var enighed på mødet om, at listen omhandlede flere væsentlige udfordringer i forhold til brugen af teledata, som det kunne være relevant at nævne i en kommende

redegørelse. Drøftelserne gav ifølge politidirektøren ikke anledning til at foreslå ændringer i Justitsministeriets udkast til kommissorium og brev til Folketingets Retsudvalg. Politidirektøren har derudover oplyst, at det var Rigspolitiets opfattelse, at fokus for den bestilte redegørelse var fejlen i politiets konverteringssystem, som havde skabt ufuldstændige datasæt, og at andre kendte problemstillinger som eksempelvis fortolkningsmæssige udfordringer ved brug af teledata fortsat skulle håndteres i telecentret i samarbejde med politikredsene og teleudbyderne. Politidirektøren har endvidere oplyst, at problematikken om nyere samtaletjenester kunne medtages i brevet, idet der her også var tale om ufuldstændige datasæt, men at årsagen hertil var fra teleudbydersiden. Koncernstyringsdirektøren afgav herefter Rigspolitiets bemærkninger telefonisk til Justitsministeriet i en samtale, hvor politidirektøren deltog på medhør.

Koncernstyringsdirektøren har oplyst, at han på baggrund af aftalen med rigspolitichefen deltog i et møde i Politiområdet den 1. juli 2019, hvor først chefen for NEA redegjorde for sine observationer i teledatasagen, og hvor chefen for telecentret efterfølgende orienterede om og gennemgik et mere systematiseret overblik over de udfordringer vedrørende teledata, som løbende var blevet indmeldt af politikredsene. Koncernstyringsdirektøren har oplyst, at gennemgangen bar præg af, at der ikke var overblik over, hvad de enkelte registreringer dækkede over, og at der var tale om en liste, der endnu ikke var gennemarbejdet og kvalificeret, samt at det var hans opfattelse, at der ikke på mødet blev nævnt problemstillinger som indebar, at der var fejl i rådata, eller som i øvrigt kastede nyt lys over konverteringsfejlen i politiets system. Koncernstyringsdirektøren har afslutningsvis oplyst, at han over for politidirektøren og chefen for telecentret gav udtryk for, at det var fornuftigt, at centret nu var begyndt at danne sig et konsolideret overblik over udfordringer med anvendelse af teledata.

Den 2. juli 2019 orienterede justitsministeren Folketingets Retsudvalg om sagen og nedsatte i samme anledning en uafhængig kontrol- og styregruppe (herefter kontrol- og styregruppen). Gruppen fik et bredt mandat til at kontrollere og styre myndighedernes gennemgang af de konkrete straffesager, der var omfattet af teledatasagen. Samtidig bad justitsministeren rigspolitichefen og rigsadvokaten om en samlet redegørelse for hele forløbet.

Samme dag udsendte Rigsadvokaturen en instruks for behandling af straffesager, hvori der indgik teleoplysninger. I instruksen orienterede Rigsadvokaturen om de nye oplysninger

om mangelfuld rådata vedrørende nyere internetbaserede samtaletjenester mv. Alle anklagere blev i forbindelse med behandlingen af straffesager, hvori der indgik teleoplysninger, instrueret i at udvise betydelig forsigtighed med at tillægge manglende teleoplysninger den betydning, at der ikke havde været telekommunikation. Samtidig fremgik det, at politiet og anklagemyndigheden i forbindelse med efterforskningen skulle være særligt opmærksomme på, at teleoplysninger kunne være mangelfulde, og at det samme gjaldt, når anklagemyndigheden skulle vurdere tiltalespørgsmålet.

Den 3. juli 2019 blev der afholdt møde i koncernledelsen for politiet og anklagemyndigheden. Rigspolitichefen gav i den forbindelse en orientering om teledatasagen.

Den 4. juli 2019 henvendte Østjyllands Politi sig til Rigspolitiet vedrørende en række mulige fejl og unøjagtigheder i rådata mv. Samme dag kontaktede chefen for telecentret Rigsadvokaturen og oplyste om henvendelsen fra politikredsen, som telecentret ville undersøge nærmere og eventuelt vende tilbage om. Senere samme dag orienterede chefen for telecentret bl.a. politidirektøren, chefen for NKC og chefen for NEA's juridiske sekretariat om kontakten til Rigsadvokaturen.

Den 5. juli 2019 blev der afholdt et møde i Rigspolitiet med deltagelse af bl.a. rigspolitichefen, politidirektøren, koncernstyringsdirektøren, chefen for NKC og chefen for telecentret som forberedelse til et møde senere samme dag med kontrol- og styregruppen. Politidirektøren har oplyst, at det på mødet blev aftalt, at han på mødet med kontrol- og styregruppen skulle fremhæve, at beslutningen om at lade undersøgelsesperioden gå tilbage til 2012 var baseret på en hypotese, som ikke var endeligt bekræftet, at Rigspolitiet foreløbigt troede på hypotesen, men at det ikke kunne udelukkes, at der var behov for at gå længere tilbage.

På mødet med kontrol- og styregruppen samme dag – som var første gang, gruppen var samlet – deltog bl.a. rigsadvokaten, vicestatsadvokaten, politidirektøren, koncernstyringsdirektøren, chefen for NKC og to kontorchefer fra Justitsministeriet. Kontrol- og styregruppen blev på mødet orienteret om konverteringsfejlen og de manglende data fra nyere internetbaserede samtaletjenester. Politidirektøren tilkendegav på mødet, at afgrænsningen tilbage til 2012 beroede på en konkret hypotese om årsagen til konverteringsfejlene, som dog ikke var endeligt bekræftet, og det kunne derfor ikke udelukkes, at man ville skulle over-

veje at gå længere tilbage. Derudover tilkendegav politidirektøren, at fejlene i konverteringen ikke havde noget at gøre med andre kendte udfordringer og usikkerheder ved brug af teledata, herunder f.eks. i forhold til mastespring og masternes præcise placering.

Den 8. juli 2019 blev der afholdt et møde i Rigspolitiet med deltagelse af bl.a. rigspolitichefen, politidirektøren, koncernstyringsdirektøren, afdelingschefen for Direktionssekretariatet og chefen for NEA's juridiske sekretariat om udfærdigelsen af redegørelsen om teledatasagen (herefter redegørelsen). På mødet fastlagde rigspolitichefen de overordnede rammer for redegørelsen, og det blev aftalt, at et første fælles udkast i samarbejde med Rigsadvokaturen skulle være klar den 12. august 2019, samt at et første udkast, som alene var baseret på Politiområdets input, skulle drøftes på et møde med rigspolitichefen den 25. juli 2019.

Den 9. juli 2019 blev der afholdt et møde mellem politidirektøren og direktøren for Teleselskabernes brancheorganisation. Politidirektøren har oplyst, at det på mødet blev aftalt, at der i fællesskab skulle arbejdes for at etablere et samarbejde på strategisk niveau mellem Rigspolitiet og teleselskaberne. Formålet herved var at bringe interessenterne tættere på hinanden, så det kunne sikres, at eksempelvis oplysninger om lancering af nye produkter eller om ændringer i registreringspraksis i rådata ville tilgå Rigspolitiet hurtigst muligt. Politidirektøren har endvidere oplyst, at der blev aftalt et første møde på strategisk niveau til den 30. august 2019.

Den 11. juli 2019 blev telecentret opmærksom på, at der kunne være sket konverteringsfejl i det oprindeligt antagne kontrolår, 2012. Telecentret brugte de følgende dage på at undersøge spørgsmålet nærmere og kunne den 16. juli 2019 orientere politidirektøren om, at det foreløbige resultat af undersøgelsen viste, at der også var sket konverteringsfejl i ca. 1 pct. af de undersøgte sager i 2012. Telecentret vurderede, at der var behov for yderligere undersøgelse de fejlbehæftede sager, og at telecentrets delkonklusion stadig var, at det var opdateringen i maj 2013, som var hovedårsagen til den mere systematiske konverteringsfejl. På den baggrund blev det besluttet ikke at orientere øvrige aktører herom, før der var mere klarhed over sagen.

Den 19. juli 2019 anmodede kontrol- og styregruppen Rigspolitiet og Rigsadvokaturen om at besvare en række spørgsmål. Der blev bl.a. spurgt til, hvilke generelle erfaringer og be-

skrivelser, der i øvrigt forelå hos politiet og anklagemyndigheden vedrørende andre relevante konstaterede unøjagtige eller mangelfulde teleoplysninger, herunder vedrørende mastespring, sommer/vintertid, bortkomst af linjer ved sideskift mv. Der blev endvidere spurgt til, om der på et tidspunkt var foretaget en stikprøveundersøgelse af validiteten af teleoplysninger.

Den 22. juli 2019 blev der mellem chefen for telecentret og kontrol- og styregruppen drøftet mulighed for et fysisk besøg i telecentret med henblik på, at kontrol- og styregruppen kunne se telecentrets faciliteter, en udarbejdet indberetningsordning til politikredsene samt en vejledning til denne. Der blev efterfølgende planlagt et besøg i telecentret den 20. august 2019.

Den 25. juli 2019 blev der afholdt et internt møde i Rigspolitiet om et første udkast til redegørelsen. På mødet deltog bl.a. rigspolitichefen, politidirektøren, chefen for NEA, stabschefen for Politiområdet og chefen for NEA's juridiske sekretariat. Af udkastet til redegørelse fremgik under et afsnit om afgrænsning, at det igangsatte arbejde med en beskrivelse af øvrige potentielle fejlkilder på daværende tidspunkt havde udmøntet sig i en liste med ca. 50 fund om mangler mv. ved brug af teledata, hvoraf kun få blev betegnet som kritiske. Det fremgik af udkastet, at alle kritiske forhold fra listen ville skulle indgå i redegørelsen, men at erfaringen havde vist, at det ville være fornuftigt med en tydelig afgrænsning af, hvad der skulle tages med og ikke tages med. Det blev aftalt at mødes igen den 5. august 2019 for en gennemgang af 2. udkast, som fortsat alene skulle være baseret på Politiområdets input.

Den 29. juli 2019 orienterede chefen for telecentret politidirektøren, chefen for NEA, stabschefen for Politiområdet, chefen for NKC og chefen for NEA's juridiske sekretariat om, at der i Nordsjællands Politi var fundet mastekoordinatfejl i en konvertering i en sag fra 2016. Fejlen bestod i, at mastekoordinaterne var forskudt ca. 222 meter i syd-sydvestlig retning, når koordinaterne blev sammenlignet med rådata. Det fremgik bl.a. af orienteringen, at der her ikke var tale om en sletning af rådata i konverteringen, men at konverteringen havde bevirket en 'forvrængning' af data. Telecentret vurderede på daværende tidspunkt, at fejlen ikke var sagskritisk, da det alene omhandlede mastens placering, forskydningen var begrænset, og at data alene viste, hvilken mast telefonen var på – og det dermed ikke var et forsøg på præcis angivelse af, hvor telefonen var. Telecentret vurderede også, at fejlen ikke desto mindre af mere principielle grunde kunne være kritisk. Chefen for telecentret oplyste endvidere, at der herudover eksisterede et antal fejl og mangler i anvendelsen af teledata,

og chefen for telecentret foreslog en gennemgang og drøftelse af disse fejl med henblik på en vurdering af, hvilke der skulle indarbejdes i redegørelsen for teledatasagen.

Chefen for telecentret lagde efterfølgende op til, at kontrol- og styregruppen snarligt skulle orienteres skriftligt om mastekoordinationsfejlen, da den havde en sådan karakter, der tilsagde dette.

Politidirektøren har oplyst, at han vurderede, at mastekoordinatfejlen, herunder årsagen til fejlen, burde undersøges nærmere, inden der blev gået videre med sagen, da der på daværende tidspunkt kun var fundet én fejl, som kunne være enkeltstående. Politidirektøren har endvidere oplyst, at han samtidig vurderede, at fejlen skulle beskrives i redegørelsen og også forelægges for kontrol- og styregruppen på det kommende møde den 20. august 2019. Politidirektøren har yderligere oplyst, at rigspolitichefen på daværende tidspunkt var på ferie, og at politidirektøren derfor vurderede, at rigspolitichefen kunne orienteres om fejlen, når ferien var afsluttet.

Det blev i forlængelse heraf mellem politidirektøren og chefen for telecentret også aftalt at afholde et møde med henblik på at drøfte, hvilke af de øvrige fejl og mangler i teledata, som telecentret på daværende tidspunkt havde afdækket, jf. det arbejde der blev iværksat den 5. juli 2019, der skulle medtages i redegørelsen.

5.7. Frem til den 19. august 2019

Den 1. august 2019 iværksatte telecentret en stikprøvekontrol, som skulle afdække, hvorvidt der var indholdsmæssige forskelle i oprindeligt konverteret data og re-konverteret data (rådata som konverteres igen). Baggrunden herfor var den identificerede indholdsmæssige mastekoordinatfejl, jf. ovenfor, samt at kontrol- og styregruppen havde stillet spørgsmål om mulige stikprøver af konverteringen af teledata. Telecentret igangsatte i alt knap 300 stikprøvekontroller fordelt over perioden 2012-2018, og deadline for disse stikprøvekontroller blev fastsat til ultimo august 2019.

Den 2. august 2019 blev der afholdt et møde om forberedelse af materiale til kontrol- og styregruppen mellem politidirektøren og NEA's juridiske sekretariat. På mødet blev de bestilte dokumenter mv. fra kontrol- og styregruppen gennemgået, og sagen, hvor der var fundet fejl i mastekoordinaterne efter konvertering, blev drøftet. Politidirektøren har oplyst,

at der på dette tidspunkt var meget lidt viden om fejlen, herunder hvorvidt den var enkeltstående, samt at han efter mødet med sekretariatet, bad telecentret udarbejde et notat med henblik på at undersøge det mulige omfang af fejlen.

Den 5. august 2019 blev der afholdt et nyt møde i Rigspolitiet mellem politidirektøren og NEA's juridiske sekretariat om besvarelsen af henvendelsen af 19. juli 2019 fra kontrol- og styregruppen. Mastekoordinatfejlen blev ligeledes drøftet, og det blev besluttet, at det var for tidligt at orientere kontrol- og styregruppen om mastekoordinatfejlen, idet der stadig blev arbejdet på at finde årsagen til fejlen, og at fejlen kun var set i en enkelt sag og derfor fortsat kunne være enkeltstående. Politidirektøren har oplyst, at vurderingen var, at Rigspolitiet ville kunne give en kvalificeret vurdering af fejlen og dens årsag mundtligt på mødet med kontrol- og styregruppen den 20. august 2019.

Samme dag fremsendte politidirektøren 2. udkast til redegørelsen til rigspolitichefen og koncernstyringsdirektøren. Udkastet blev drøftet på et møde i Rigspolitiet samme dag. På mødet deltog bl.a. rigspolitichefen, politidirektøren, koncernstyringsdirektøren og chefen for NEA's juridiske sekretariat. På mødet efterspurgte rigspolitichefen bl.a. dokumentation for den i redegørelsen omtalte stikprøve i november 2018 på 60 sager samt nærmere oplysninger om, hvad fejlene vedrørte. Udkastet til redegørelsen havde på daværende tidspunkt samme omtale som det tidligere udkast om listen med ca. 50 fund om mangler mv. ved brug af teledata, hvoraf de kritiske ville skulle indgå i redegørelsen.

Politidirektøren har oplyst, at han på mødet orienterede rigspolitichefen om den fejl, der var konstateret om ændrede mastepositioner i konverteringen, samt at han i orienteringen understregede, at det var første gang, hvor det var konstateret, at konverteringen havde ændret data, da der hidtil kun havde været tale om ufuldstændige data ved konverteringen. Politidirektøren har endvidere oplyst, at han oplyste, at fejlen kun var set i én sag fra 2016, og at ændringen af masteplaceringen drejede sig om ca. 200 meter i forhold til rådata.

Politidirektøren har desuden oplyst, at alle på mødet var enige om, at det var en central opdagelse, hvis fejlen var udtryk for, at konverteringen også lavede indholdsmæssige ændringer. Politidirektøren har endvidere oplyst, at han på mødet tilkendegav, at Politiområdet arbejdede på at finde årsagen til fejlen, og at det var telecentrets vurdering, at fejlen ikke var sagskritisk, da det alene omhandlede mastens placering, og at forskydningen var

begrænset. Endelig har politidirektøren oplyst, at der var enighed om, at sagen skulle forelægges kontrol- og styregruppen på mødet den 20. august 2019, hvor det var forventningen, at der kunne gives en kvalificeret vurdering af fejlen og dens årsag, og at en beskrivelse af fejlen skulle indgå i redegørelsen.

Rigspolitichefen har oplyst, at mødet i alt væsentligt omhandlede 2. udkast til redegørelse, og at der i den forbindelse blev givet en række bemærkninger til det foreliggende udkast. Rigspolitichefen har endvidere oplyst, at der blev nævnt én mulig fejl, der ikke var konsolideret og skulle undersøges nærmere. Det var rigspolitichefens forståelse, at fejlen, der kun var set i en sag, ikke vurderedes at have betydning for hverken politiets efterforskning eller straffesagsbehandling ved retten.

Senere samme dag besvarede Rigspolitiet kontrol- og styregruppens henvendelse af 19. juli 2019. Det fremgik bl.a. af besvarelsen, at Rigspolitiet på et møde med kontrol- og styregruppen den 20. august 2019 ville redegøre for de generelle erfaringer, der forelå om unøjagtige eller mangelfulde teleoplysninger.

På baggrund af mødet og de umiddelbare bemærkninger til udkastet til redegørelsen udarbejdede Politiområdet et nyt udkast til redegørelse, som den 6. august 2019 blev sendt til bl.a. rigspolitichefen, politidirektøren og koncernstyringsdirektøren.

Den 6. august 2019 blev analysen af mulige konverteringsfejl før 2013 sendt til politidirektøren. Analyserapporten viste, at der i 19 ud af ca. 900 undersøgte rekvisitioner fra 2012 var tegn på fejl i konverteringen. Af de 19 rekvisitioner var det telecentrets vurdering, at 4-5 af disse skyldtes timeren i it-systemet.

Den 12. august 2019 blev der afholdt et internt møde i Politiområdet med deltagelse af politidirektøren, chefen for telecentret samt medarbejdere fra telecentret. På mødet blev analysen om de gennemgåede rekvisitioner i 2012 gennemgået, og politidirektøren har oplyst, at han konkluderede, at resultatet skulle forelægges kontrol- og styregruppen med henblik på en vurdering af, om den historiske gennemgang af sager skulle gå længere tilbage end 2012. Politidirektøren har endvidere oplyst, at chefen for telecentret på mødet gennemgik de udfordringer med teledata, som telecentret på daværende tidspunkt havde afdækket, og som det blev vurderet skulle indgå i redegørelsen og skulle forelægges for kontrol- og

styregruppen. Politidirektøren har oplyst, at chefen for telecentret fremhævede problematikken omkring udlandspræfiks, som ifølge politidirektøren under helt særlige omstændigheder kunne få et udenlandsk nummer til at ligne et dansk nummer, samt at der var set udenlandske telefonnumre gå på master fra to forskellige selskaber samtidig. Endvidere har politidirektøren oplyst, at problematikken omkring manipulerede opkald, hvor man via internettet kan udgive sig for at sende en sms fra en andens telefon, blev nævnt, ligesom politidirektøren har oplyst, at det ved en særlig type samtaletjeneste var set, at A- og B-nummeret kunne blive vendt rundt.

Politidirektøren har oplyst, at der, som han forstod det, ikke var tale om nye udfordringer, men om kendte problematikker, som telecentret havde samlet sammen. Politidirektøren har endvidere oplyst, at de forskellige problematikker blev drøftet, herunder mulighederne for at afdække de enkelte emner i forbindelse med efterforskningen, og at problemerne lignede udfordringerne med mastespring mv., da det handlede om fortolkning af de data, som politiet modtager fra teleudbyderne.

Politidirektøren har oplyst, at han på baggrund af drøftelserne bl.a. bad om, at emnerne skulle undersøges nærmere samt om en beskrivelse af emnerne til brug for redegørelsen og til forelæggelse for kontrol- og styregruppen den 20. august 2019.

Den 13. august 2019 orienterede Rigspolitiet – i forbindelse med et bidrag til besvarelsen af spørgsmål nr. 72 (Alm. del) af 17. juli 2019 fra Folketingets Retsudvalg – Justitsministeriet om, at det var Rigspolitiets vurdering, at det ville være nødvendigt at undersøge, om der ville være behov for at fremfinde sager fra før 2012 til gennemgang. Dette som følge af, at de ovenfor beskrevne undersøgelser havde afdækket uoverensstemmelser mellem rådata og konverterede data før 2013. Der var således tale om en ændret vurdering af den tidsmæssige afgrænsning, som Rigspolitiet havde anlagt i forbindelse med justitsministerens brev til Folketingets Retsudvalg af 2. juli 2019.

Den 15. august 2019 blev der afholdt et videomøde med deltagelse af telecentret, politikredsene, de regionale statsadvokater, SØIK og Rigsadvokaturen. I mødet deltog bl.a. vicestatsadvokaten. På mødet blev det oplyst, at telecentret var blevet opmærksom på en ny fejltype, der omhandlede fejlkonvertering af mastekoordinater, og som kunne føre til, at positionen af en mast blev forskudt med ca. 200 meter. Fejlen var opdaget i en sag fra 2016, og telecentret var nu ved at indkredse fejlperioden.

Umiddelbart efter orienterede vicestatsadvokaten statsadvokaten om den nye indholdsmæssige konverteringsfejl. Statsadvokaten og vicestatsadvokaten var enige om, at der var tale om en ny og alvorlig oplysning, som rigsadvokaten skulle orienteres om, idet det ikke tidligere havde været fremme, at konvertering kunne påvirke indholdet af teledata. Rigsadvokaten blev kort efter orienteret. Det blev i den forbindelse aftalt, at statsadvokaten skulle tage kontakt til politidirektøren for at få en uddybende beskrivelse af fejlen, ligesom Justitsministeriet skulle orienteres om fejlen.

Statsadvokaten kontaktede umiddelbart herefter politidirektøren om fejlen omtalt på videomødet. Rigsadvokaturen har oplyst, at politidirektøren i den forbindelse oplyste, at han havde kendt til fejlen i ca. 3 uger, men at han ikke havde vurderet, at den var vigtig. Rigsadvokaturen har endvidere oplyst, at politidirektøren var enig i, at der var tale om en ny type fejl, idet det ikke tidligere havde været fremme, at konvertering kunne medføre fejl i indholdet af teledata. Rigspolitiets plan var at orientere kontrol- og styregruppen om problemstillingen den 20. august 2019. Statsadvokaten tilkendegav, at der efter hans opfattelse var tale om en ny og alvorlig fejl, idet det indtil nu havde været opfattelsen, at der alene havde manglet teledata, men at der ikke var fejl i indholdet af teledata. Det var således statsadvokatens vurdering, at Justitsministeriet derfor burde orienteres med det samme. Statsadvokaten orienterede umiddelbart efter samtalen en kontorchef i Justitsministeriet om den nye fejl, og om at Rigspolitiet ville orientere ministeriet nærmere. Rigsadvokaten og rigspolitichefen aftalte samme dag, at Rigspolitiet skulle udarbejde en skriftlig beskrivelse af problemstillingen til næste morgen.

Politidirektøren har om samtalen med statsadvokaten oplyst, at statsadvokaten henstillede til, at Justitsministeriet blev orienteret om sagen. Politidirektøren har endvidere oplyst, at han erklærede sig enig i, at det var nyt, hvis konverteringen ændrede data, og oplyste, at det var besluttet på et møde den 5. august 2019, jf. ovenfor, at fejlen skulle indgå i redegørelsen og forelægges kontrol- og styregruppen, og at det – efter det oplyste – fortsat var en fejl, der kun var set i én sag, som ikke blev vurderet at være sagskritisk, og at Rigspolitiet arbejdede på at finde årsagen til fejlen. Politidirektøren tilkendegav samtidig at ville følge op på henvendelsen fra statsadvokaten, men at han først ville ringe til Justitsministeriet, når det var afstemt med rigspolitichefen. Statsadvokaten bad om at blive underrettet, når politidirektøren havde talt med Justitsministeriet.

Telecentret oplyste senere samme dag, at de samme dag havde fundet mastekoordinatfejl i et antal sager. Politidirektøren har oplyst, at telecentret endnu ikke kunne konkludere, om der var tale om egentlige substantielle fejl, og at en afklaring heraf ville kræve en nærmere undersøgelse. Politidirektøren har oplyst, at det var første gang, han hørte, at der kunne være flere fejl end i en enkeltstående sag, og at han spurgte ind til og fik bekræftet, at det ville være muligt at kontrollere alle fundne konverterede datasæt (ca. 24.000) for mastekoordinatfejl.

Efterfølgende samme dag – den 15. august 2019 – talte politidirektøren med rigspolitichefen om mastekoordinatfejlen. Rigspolitichefen var dog allerede blevet kontaktet af Justitsministeriet, da ministeriet havde hørt om problemstillingen fra Rigsadvokaturen. Politidirektøren har oplyst, at han over for rigspolitichefen tilkendegav, at den aftalte plan var at forelægge problemstillingen for kontrol- og styregruppen på mødet den 20. august 2019, og at problemstillingen desuden ville indgå i redegørelsen til Justitsministeriet. Politidirektøren henviste samtidig til Justitsministeriets udmelding om, at der ikke telefonisk måtte meddeles Justitsministeriet om udviklingen i større sager. Disse skulle være tilstrækkelig belyst til at kunne foreligge skriftligt. Politidirektøren har oplyst, at rigspolitichefen erklærede sig enig i politidirektørens tilgang til situationen, men oplyste ifølge politidirektøren, at han var blevet bedt om at orientere Justitsministeriet om sagen dagen efter. Politidirektøren bestilte efterfølgende en foreløbig status på undersøgelsen af mastekoordinatproblemstillingen.

Den 16. august 2019 fremsendtes en foreløbig status på mastekoordinatproblemstillingen til rigspolitichefen fra politidirektøren, hvoraf det bl.a. fremgik, at der på dette tidspunkt var fundet fejl i ca. 60 rekvisitioner, og at de alle vedrørte konverteringer i september og oktober 2016. De ca. 60 fejl, der var identiske med den første kendte konverteringsfejl, hvor mastepositionen var forskudt ca. 200 meter, blev fundet ved kontrol af ca. 1.500 rekvisitioner i en periode på ca. seks måneder i tidsrummet omkring den oprindeligt konstaterede fejl fra september 2016.

Politidirektøren har oplyst, at rigspolitichefen drøftede sagen med rigsadvokaten, og derefter bad politidirektøren om at aftale et møde med kontrol- og styregruppens formand samme dag med henblik på orientering om problemstillingen. Mødet blev afholdt senere samme dag med deltagelse af politidirektøren, statsadvokaten, vicestatsadvokaten og chefen for telecentret.

Politidirektøren og chefen for telecentret mødtes med statsadvokaten og vicestatsadvokaten forud for orienteringen af kontrol- og styregruppen. På mødet blev omfanget og betydningen af den nye fejl drøftet.

På mødet i kontrol- og styregruppen orienterede Rigspolitiet om den nye fejl. Omfanget og betydningen af den nye fejlen blev på ny drøftet.

Rigspolitiet oplyste på mødet, at de identificerede fejl var baseret på en gennemgang af en delmængde af datamaterialet, og at det herefter kunne konkluderes, at der måtte forventes at være flere sager med samme fejl. Rigsadvokaturen har oplyst, at formanden for kontrol- og styregruppen tilkendegav, at hvis man ikke kunne stole på indholdet af rækkerne, var det en ny situation, som ville få konsekvenser. Han tilkendegav samtidig, at han som formand ikke kunne fastlægge nye retningslinjer, men at det ville være klogt at sikre, at der ikke blev sagt noget forkert ved landets domstole, og at sager med frihedsberøvede og udviste burde prioriteres.

Umiddelbart efter mødet i kontrol- og styregruppen blev der afholdt en kort briefing om mødet på rigsadvokatens kontor med deltagelse af rigsadvokaten, rigspolitichefen, politidirektøren, statsadvokaten, vicestatsadvokaten og chefen for telecentret. Herefter blev sagen drøftet med en afdelingschef og kontorchef fra Justitsministeriet på et møde i Justitsministeriet.

På mødet i ministeriet oplyste rigsadvokaten, at det ville være nødvendigt for anklagemyndigheden at reagere straks på de nye oplysninger, som indebar, at der kunne være fejl i indholdet af konverteret teledata (masteplaceringen), som ikke kunne udelukkes at have bevismæssig betydning. Omfanget af fejlen var ikke endelig klarlagt, og der var tale om fejl, som ikke umiddelbart ville kunne identificeres på sagsbehandlerniveau (i modsætning til fejlen vedrørende ufuldstændig konverteret data). Det blev aftalt, at Rigsadvokaturen ville iværksætte nødvendige tiltag.

Senere samme dag sendte politidirektøren en opdateret status om mastekoordinatproblemstillingen til rigspolitichefen. Af denne status fremgik det bl.a., at der nu var gennemgået ca. 6.000 rekvisitioner og fundet potentielle masterkonverteringsfejl i yderligere ca. 30 rekvisitioner, der alle var før september 2016 og alle med samme afvigelse eller mindre end

de hidtidige ca. 200 meter. Rigspolitichefen og politidirektøren vendte kort herefter sagen, og rigspolitichefen meddelte direktøren, at han ikke behøvede at deltage på mødet i Justitsministeriet, som var aftalt til senere samme dag.

I forbindelse med mødet i kontrol- og styregruppen oplyste Rigspolitiet over for Rigsadvokaturen, at telecentret i løbet af dagen havde identificeret yderligere sager med den omtalte fejl.

Samme aften udsendte Rigsadvokaturen en foreløbig instruks gennem de regionale statsadvokater om, at der i forbindelse med behandlingen af straffesager i weekenden (grundlovsforhør mv.), hvori masteroplysninger anvendes som bevis for en telefons position, kun måtte anvendes masteplaceringer baseret på rådata, herunder til udfærdigelse af mastekort eller andre bilag, der skulle illustrere telefonens position eller bevægelse. Endvidere skulle rådata vedlægges. Det blev aftalt med de regionale statsadvokater, at de skulle kontakte chefanklagerne i politikredsene enkeltvis samme aften. Rigsadvokaturen orienterede samtidig PET, SØIK, DUP, Grønlands Politi og Færøernes Politi om den foreløbige instruks. Rigspolitiet modtog også en kopi af den foreløbige instruks, idet Rigsadvokaturen samtidig gjorde Rigspolitiet opmærksom på, at det var Rigspolitiets ansvar at håndtere spørgsmålet om udsendelsessager henover weekenden. Rigsadvokaturen orienterede efterfølgende den uafhængige kontrol- og styregruppe, herunder om at de foranstående myndigheder var orienteret.

Den 17. august 2019 blev der holdt et møde i Justitsministeriet med deltagelse af bl.a. rigspolitichefen, rigsadvokaten, statsadvokaten, vicestatsadvokaten, chefen for telecentret samt en afdelingschef og to kontorchefer fra Justitsministeriet. Politidirektøren deltog ikke i mødet. Rigsadvokaten orienterede om den foreløbige instruks. Det blev herefter drøftet, hvordan der kunne sikres en mere permanent løsning i forhold til de nye usikkerheder, der var opstået i forhold til konverteret teledata. I den forbindelse var der bl.a. en drøftelse af, i hvilket omfang det var muligt at anvende rådata i forbindelse med straffesagers behandling. I løbet af aftenen arbejdede Rigsadvokaturen og Rigspolitiet videre på en mulig model for øget anvendelse af rådata i straffesager.

Den 17. august 2019 blev 3. udkast til redegørelsen sendt til rigspolitichefen, politidirektøren og koncernstyringsdirektøren.

Den 18. august 2019 blev der om formiddagen afholdt et møde i Justitsministeriet med deltagelse af bl.a. rigspolitichefen, rigsadvokaten, statsadvokaten, vicestatsadvokaten, chefen for NEA, chefen for NKC samt en afdelingschef, koncerndatadirektøren og tre kontorchefer fra Justitsministeriet. På mødet blev en mulig model for øget anvendelse af rådata i straffesager præsenteret. Modellen skulle imødegå den øgede usikkerhed, der var opstået om validiteten af konverteret teledata. I slutningen af mødet oplyste chefen for NEA, at man skulle være opmærksom på, at Rigspolitiet havde identificeret flere forskellige konkrete fejl og fejlkilder i den rådata, som politiet modtog fra teleselskaberne. Omfanget og betydningen af disse fejl var endnu ikke afdækket. Det blev besluttet, at Rigspolitiet måtte orientere Rigsadvokaturen nærmere om disse fejl, så væsentlige nye fejl og fejlkilder kunne indgå i overvejelserne om en mulig ny model.

Der blev umiddelbart efter holdt et møde hos Rigsadvokaturen, hvor Rigspolitiet orienterede nærmere om de fejl og fejlkilder i teledata, som Rigspolitiet på det foreliggende grundlag vurderede, var de alvorligste.

I forlængelse heraf blev der holdt et møde mellem rigsadvokaten, rigspolitichefen og statsadvokaten samt departementschefen og to afdelingschefer i Justitsministeriet. På mødet blev situationen drøftet i lyset af de oplysninger, som nu var kommet frem. Rigsadvokaten oplyste, at de nye oplysninger om fejl og fejlkilder i rådata – efter hans opfattelse – satte nye og alvorlige spørgsmålstegn ved kvaliteten af de teledata, som anklagemyndigheden anvendte i straffesager. Situationen gjorde det nødvendigt at indføre et midlertidigt stop på foreløbigt to måneder for anklageres anvendelse af teledata under hovedforhandlinger eller retsmøder om opretholdelse af anholdelse og varetægtsfængsling. Rigspolitichefen var enig i rigsadvokatens vurdering.

Samme aften udsendte Rigsadvokaturen en instruks om det midlertidige stop for brug af teleoplysninger til alle embeder.

Den 19. august 2019 blev politidirektøren flyttet midlertidigt til at varetage strategiske projekter i Koncernstyring i Rigspolitiet. Samtidig blev der indsat en ny midlertidig politidirektør i Politiområdet.

I forlængelse af instruksen den 18. august 2019 orienterede Rigspolitiet og Rigsadvokaturen den 30. august 2019 Justitsministeriet om yderligere skridt i teledatasagen. Af orienteringen fremgik det bl.a., at Rigspolitiet havde igangsat en ekstern undersøgelse af politiets brug og behandling af teledata, som forventedes gennemført inden udgangen af september 2019. Desuden fremgik det, at Rigspolitiet og Rigsadvokaturen havde instrueret politiet og anklagemyndigheden i at udvise øget forsigtighed ved anvendelsen af teledata under efterforskning, indtil der var tilvejebragt den fornødne klarhed over fejl, fejlkilder og usikkerheder.

6. Fejl, fejlkilder og usikkerheder mv. i teledata

I dette kapitel beskrives de fejl, fejlkilder og usikkerheder mv. i teledata, som er blevet afdækket, og som Rigspolitiet og Rigsadvokaturen har vurderet kan have haft en betydning for politiets efterforskning eller straffesagsbehandlingen.

Kapitlet omhandler således primært de fejl, fejlkilder og usikkerheder mv., der er afdækket i tidsforløbet beskrevet under kapitel 5 samt øvrige afdækkede fejlkilder, som har haft en karakter, der gjorde, at de efterfølgende er blevet kommunikeret til politikredsene mv. Endvidere beskrives de kontrolforanstaltninger og retningslinjer, der er fastsat for at imødegå de konstaterede fejl mv. i teledata.

Som det fremgår af kapitel 5, har telecentret løbende håndteret henvendelser om mulige fejl, fejlkilder og usikkerheder mv. i teledata, som rekvirenterne har modtaget fra telecentret. Henvendelserne har hovedsageligt været håndteret ved fornyet behandling af de pågældende teledata i telecentret og blev af telecentret oftest opfattet som periodiske tekniske udfordringer eller brugerfejl frem for systematiske fejl vedrørende teledata. Der er således flere af de fejltyper, der beskrives i det følgende kapitel, som har været behandlet som enkeltstående fejl, og som ikke er blevet behandlet som systematiske fejl, herunder kommunikeret bredt ud til eksempelvis efterforskere og teleanalytikere i politikredsene mv. Fejl mv., der har været fremme tidligere, som f.eks. "mastespring", der er beskrevet i Justitsministeriets besvarelse af 20. oktober 2015 af spørgsmål nr. 182 (Alm. del) fra Folketingets Retsudvalg, jf. afsnit 4.2.2.3 ovenfor, er ikke beskrevet i det følgende.

Et andet eksempel, der har været fremme tidligere, er, at en teleudbyder i oktober 2018 meddelte, at selskabet stoppede med at logge lokaliseringsdata vedrørende MMS på grund af uklarhed om reglerne. Politikredsene mv. blev orienteret om dette i oktober 2018.

Beskrivelsen er i det følgende baseret på Rigspolitiets vurdering og forståelse af de pågældende fejl, fejlkilder og usikkerheder mv. Alle fejl mv., som telecentret har identificeret, er blevet overdraget til kontrol- og styregruppen samt til den uafhængige eksterne undersøgelse, som foretages af revisions- og konsulentfirmaet Deloitte med henblik på en yderligere konsolidering af både kendte og mulige endnu ikke kendte fejl og fejlkilder mv., jf. afsnit 6.1. Således kan beskrivelsen i indeværende kapitel ikke anses som en udtømmende opremsning af alle mulige fejl, fejlkilder og usikkerheder mv.

Omfanget af de beskrevne fejl mv., herunder antallet af sager, hvor der mangler konverterede teledata, er ikke afdækket på nuværende tidspunkt. Det vil ske ved Deloittes undersøgelse og ved politiets og anklagemyndighedens gennemgang af de muligt berørte sager, jf. herom i kapitel 7.

6.1. Den uafhængige eksterne undersøgelse

Rigspolitiet iværksatte den 27. august 2019 en ekstern undersøgelse for hurtigst muligt at skabe tilstrækkelig klarhed over de fejl, fejlkilder og usikkerheder mv., som er forbundet med brug af teledata, så teledata igen kan anvendes som bevis i straffesager. Undersøgelsen bliver foretaget af revisions- og konsulentfirmaet Deloitte.

Undersøgelsen omfatter en validering af telecentrets databehandling og konvertering. Som led i undersøgelsen foretages en sammenligning af alle de rådatasæt og konverterede datasæt, der er til rådighed for analysen, for at afgøre, om der er overensstemmelser mellem de to datasæt. Formålet er at afdække alle uoverensstemmelser, herunder bl.a. om alle aktiviteter og lokaliseringsoplysninger i rådata er medtaget korrekt i de konverterede data.

Den eksterne undersøgelse redegør også for mulige fejlkilder mv., som politiet og anklagemyndigheden, forsvarere og domstole altid bør være opmærksomme på. Derfor har Deloitte gennemgået og analyseret de rådatasæt, der er til rådighed med henblik på at undersøge, hvilken grad af præcision og eventuelle fejl der kan konstateres i disse, herunder de aktiviteter og lokaliseringsoplysninger, som er leveret til politiet.

6.2. Beskrivelse af fejl, fejlkilder og usikkerheder mv.

I dette afsnit beskrives de omtalte fejl, fejlkilder, usikkerheder mv. I afsnit 6.2.1 beskrives de væsentligste konverteringsfejl i teledata. Afsnit 6.2.2 omhandler den mangelfulde rådata om kommunikation ved brug af nyere samtaletjenester (VoLTE og VoWifi). I afsnit 6.2.3 er der redegjort for den fejlagtige konvertering af mastekoordinater. Øvrige fejl, som Rigspolitiet oplyste Justitsministeriet om den 18. august 2019, er beskrevet i afsnit 6.2.4.

6.2.1. Manglende oplysninger i konverterede teledata

Telecentret har siden den 1. november 2010 konverteret de rådata, der er modtaget fra teleudbyderne. Rådata modtages i forskellige formater fra teleudbyderne, og telecentrets systemer konverterer disse oplysninger, således at de for rekvirenterne fremstår i ensartede formater og med ensartede betegnelser, uanset hvilke teleudbydere der har leveret data, jf. nærmere herom i afsnit 3.2 og 3.3. Konverteringen gør det muligt for sagsbehandleren at sammenstille og analysere data på tværs af indhentede oplysninger og sidenhen for anklageren at fremstille oplysningerne på en ensartet måde under en eventuel straffesag.

Telecentret har, som beskrevet i kapitel 5, afdækket flere forhold, der over tid har forårsaget, at der i flere tilfælde har været en forskel mellem rådata og konverterede teledata. Der er afdækket navnlig tre overordnede forhold, der har bevirket, at ikke alle rådata er blevet konverteret. Det drejer sig om en it-systemfejl (afsnit 6.2.1.1), fejl i håndteringen af oplysninger om såkaldte særlige tjenester (afsnit 6.2.1.2) og en fejl i levering af teledata via et analyseværktøj (afsnit 6.2.1.3). Herudover kan en række andre forhold have medført forskelle mellem rådata og konverterede data som f.eks. ændring af de formater, som rådata leveres i, eller beskadiget eller fejlbehæftet rådata i form af ulæsbare karakterer, utilsigtede linjeskift mv.

6.2.1.1. Manglende konverterede teledata relateret til en it-systemfejl

Rigspolitiet afdækkede i foråret 2019, at der var en systematisk fejl i et it-system, der gjorde, at der i flere tilfælde var konstateret forskelle mellem rådata og konverterede data. En hovedårsag til disse forskelle var en fejl i det it-system, som telecentret anvender til at konvertere teledata. Telecentret vurderer, at fejlen bestod af to elementer; dels aktivering af en timer i it-systemet, dels en opdatering af it-systemet. Sammenhængen mellem de to elementer er nærmere beskrevet i det følgende. Fejlen er konstateret i de undersøgte sager fra 2012 og frem til marts 2019, idet det bemærkes, at de konstaterede fejl i 2012 alene relaterer sig til timeren.

I it-systemet, som telecentret bruger til at konvertere teledata, har der været indbygget en egenudviklet timer. Timerens funktion har været at sikre, at data blev sendt til rekvirenten hurtigst muligt, efter at data fra teleudbyderen var modtaget i telecentrets systemer. Timerfunktionen har gjort, at data i nogle tilfælde blev afsendt, selvom den samlede konvertering endnu ikke var færdiggjort, således at der blev leveret ukomplette konverterede datasæt til

rekvirenten. Det var hensigten, at et komplet datasæt i sådanne tilfælde skulle sendes efterfølgende, hvilket dog ikke i alle tilfælde skete, jf. nedenfor.

Timeren har været indstillet forskelligt, og den har været indstillet til at sende data efter både 30 minutter og 1, 3, 6 og 24 timer. Fra 2017 frem til 8. marts 2019 har timeren været indstillet til at sende efter senest 1 time.

En opdatering af it-systemet, der ændrede den måde konverterede teledata blev indlæst i systemet, har medført, dels at indlæsningen blev langsommere, dels at it-systemet sprang sektioner af filer over. Denne opdatering vurderes af telecentret at være sket i maj 2013. Den langsommere dataindlæsning – i kombination med timeren – vurderes at have medført, at it-systemet i øget grad har leveret filer med konverterede data til rekvirenterne, inden al data er kommet med i filerne.

I de tilfælde, hvor der er blevet leveret et ufuldstændigt konverteret datasæt, burde systemet – efter første ufærdige leverance – have færdiggjort konverteringen og fremsendt et fuldt konverteret datasæt til rekvirenten. En sådan automatisk genfremsendelse af teledata ses dog ikke at være sket i alle tilfælde, og politikredsene har derfor i disse sager ikke automatisk modtaget komplette konverterede datasæt.

Telecentret har konstateret, at manglende konverterede teledata som følge af opdateringen af it-systemet og timeren optræder i forskellige sagstyper. Det drejer sig bl.a. om sager, hvor den bestilte datamængde har været så omfangsrig, at den konverterede data ikke i sin helhed har kunnet indlæses med henblik på levering til rekvirenten inden for den tid, som timeren har været indstillet til. Fejlen er også set i sager med datamængder, der hver for sig ville kunne håndteres inden for den tidsbestemte kapacitet, som systemet har været underlagt, men hvor der i tilfælde, når systemet har modtaget mange mindre filer på samme tid, er opstået "kø" i systemet, hvorved al konverteret data ikke er blevet indlæst inden for den fastsatte tidsramme, som timeren har været indstillet til.

Opdateringen af it-systemet har som anført også haft betydning for it-systemets håndtering af sektioner af filer i forbindelse med indlæsning af teledata. I visse situationer er det konstateret, at indlæsningen af en filsektion er standset, før hele filsektionen var indlæst. Telecentrets undersøgelser viser, at systemet ikke har overvåget sådanne hændelser, og derfor

er indlæsningen af data fra den pågældende filsektion ikke blevet genoptaget, og indlæsningen af filsektionen er dermed ikke blevet færdiggjort. I stedet påbegyndte it-systemet behandling af den næste filsektion af teledata. Der kan således være tilfælde, hvor rekvirenten ikke har modtaget alle de konverterede data.

Det er telecentrets vurdering, at fejlkilden med manglende indlæsning af teledata som følge af timerfunktionen blev løst den 8. marts 2019, hvor telecentret har fjernet timerfunktionen i it-systemet. Herudover har telecentret ændret metoden for, hvordan systemet indlæser konverterede data for herved at gøre det muligt at indlæse store mængder data på samme tid. For så vidt angår systemets håndtering af filsektioner, har telecentret foretaget tilpasninger i systemet for at sikre, at systemet ikke springer sektioner af filer over, hvis indlæsningen bliver standset, inden den er færdiggjort.

6.2.1.2. Manglende konverterede oplysninger om særlige tjenester

Ud over fejlkilderne i forbindelse med indlæsning af teledata, der er beskrevet i afsnittet ovenfor, har telecentret afdækket, at visse datatyper kaldet særlige tjenester i en periode ikke er blevet konverteret.

Ved konvertering af teledata anvender telecentret datatypen 'anden aktivitet' som en betegnelse i de konverterede teleoplysninger, der dækker over forskellige særlige tjenester såsom viderestilling, "banke-på" og blokering af nummer. Oplysninger om aktivering og deaktivering af sådanne særlige tjenester har siden 2010 været leveret af én teleudbyder som en del af teledata, jf. afsnit 2.3.2.

På baggrund af en henvendelse i maj 2018 fra et af politiets efterforskningsfællesskaber blev enkelte medarbejdere i telecentret opmærksomme på, at oplysninger om særlige tjenester på daværende tidspunkt indgik i rådata, men ikke i konverterede teledata. Det blev vurderet, at den manglende konvertering af særlige tjenester skyldtes en ændring i telecentrets it-system, som betød, at datatypen blev sorteret fra i forbindelse med konverteringen, således at oplysninger alene fremgik af de rådata, som rekvirenten modtog.

Telecentret vurderer, at fejlen kunne være opstået i november 2016, hvor systemændringen blev foretaget. Telecentret rettede fejlen i juni 2018. Det har betydet, at oplysninger om særlige tjenester fra en teleudbyder ikke indgår i konverterede datasæt, der er rekvireret i

perioden fra november 2016 til juni 2018. Efter dette tidspunkt har særlige tjenester været leveret som en del af konverterede teledata.

I juni 2018 blev det pågældende efterforskningsfællesskab orienteret om, at fejlen var rettet, men andre rekvirenter og eksterne interessenter, herunder anklagemyndigheden, ses ikke at være blevet orienteret om fejlen, ligesom der ikke fra Rigspolitiets side blev iværksat yderligere tiltag i forhold til håndteringen af eventuelle manglende oplysninger i konverterede datasæt i andre sager end den pågældende konkrete sag.

6.2.1.3. Manglende levering af konverterede teledata via et analyseværktøj

Rekvirenter med særlige brugerrettigheder har siden januar 2017 kunnet tilgå konverterede teledata via et separat analyseværktøj i telecentrets it-system, hvori de konverterede oplysninger indlæses, og som kan anvendes til behandling af historiske teledata.

I august 2018 konstaterede telecentret, at oplysninger i konverterede teledata om datatyperne "anden aktivitet" og "tjenesteydelser" (hovedsageligt SMS-tjenester i form af f.eks. SMS-billetter, SMS-donationer mv.), der leveres til politiet af en teleudbyder, ikke var blevet indlæst i analyseværktøjet. Herudover konstaterede telecentret, at konverterede masteoplysninger ikke blev indlæst i analyseværktøjet, når der var tale om datasæt, som kun omhandlede oplysninger om bestemte telefonnumres masteplaceringer. Telecentrets undersøgelser har vist, at det er hele datasæt med konverterede masteoplysninger fra alle fire teleudbydere, der ikke er blevet gjort tilgængelige i analyseværktøjet.

Den daværende chef for telecentret blev i august 2018 orienteret om problemet, og der blev indledt en dialog med leverandøren af analyseværktøjet. På baggrund heraf blev der igangsat en opdatering af værktøjet med henblik på at sikre, at alle datatyper bliver indlæst i analyseværktøjet. Brugerne af analyseværktøjet blev orienteret om problemet den 17. juni 2019. Herudover har telecentret nu identificeret knap 40 rekvisitioner, hvor det ikke kan udelukkes, at rekvirenten alene har arbejdet med konverterede teledata via analyseværktøjet. Telecentret har i disse sager ligeledes rettet henvendelse til rekvirenterne og orienteret om problemet.

6.2.2. Manglende oplysninger i rådata om VoLTE- og VoWifi-aktiviteter

Som anført i afsnit 2.2.1.1 kan opkald og SMS ske gennem anvendelse af nyere samtaletjenester (VoLTE og VoWiFi). På baggrund af en konkret efterforskning, hvor der manglede oplysninger i rådata, er det i juni 2019 konstateret, at ikke alle teleudbydere leverer eller har leveret alle oplysninger om disse nye datatyper.

Den teleudbyder, der leverede oplysninger i den pågældende sag, har efter det oplyste siden den 1. august 2018 tilbudt VoLTE og VoWiFi til egne kunder, men havde først fra den 10. januar 2019 leveret oplysninger om disse aktiviteter til politiet. På den baggrund identificerede telecentret i juni 2019 de sager, hvor der kunne mangle oplysninger fra den pågældende teleudbyder. Der blev herefter fremsendt nye rådata til politikredsene mv. i de sager, hvor der manglede oplysninger om disse aktiviteter, og hvor politikredsene mv. ikke selv tidligere havde rekvireret nye datasæt. Det har efterfølgende vist sig, at en del af de pågældende aktiviteter var med i de oprindelige datasæt, der var blevet sendt til politikredsene mv., men at aktiviteterne ikke var benævnt korrekt.

Teleudbyderen har i august 2019 på ny rettet henvendelse til telecentret vedrørende den pågældende problemstilling, idet udbyderen har afdækket, at antallet af muligt berørte sager er højere end først antaget, herunder at der også kan have manglet oplysninger efter 10. januar 2019.

Den pågældende teleudbyder har sammen med telecentret gennemgået rådatasæt og har identificeret yderligere ca. 60 sager, hvor der har manglet oplysninger om de pågældende aktiviteter. I disse sager er der leveret nye rådatasæt til politikredsene mv.

Herudover har en anden teleudbyder omkring månedsskiftet juni/juli 2019 oplyst telecentret om, at udbyderen fra omkring april/maj 2017 begyndte udrulning af VoLTE- og VoWiFi-aktiviteter til sine abonnenter. Udbyderen har imidlertid ikke logget oplysninger om disse aktiviteter, når der var tale om indgående opkald til kunder med et særligt erhvervsabonnement. Disse oplysninger har således ikke indgået i rådata fra april/maj 2017 og frem til midten af august 2019, hvor teleudbyderen har oplyst at have korrigeret sine registreringer med henblik på at sikre, at oplysninger om VoLTE- og VoWiFi-aktiviteter leveres til politiet uanset abonnementstype.

6.2.3. Fejl i konvertering af mastekoordinator

På baggrund af en henvendelse fra Nordsjællands Politi den 25. juli 2019 konstaterede telecentret efterfølgende, at de konverterede geografiske koordinater for mastepositionerne i en sag fra 2016 var blevet ændret, således at masternes placering i de konverterede oplysninger ikke stemte overens med masternes placering i rådata.

Telecentret vurderer, at de konstaterede fejl i de konverterede geografiske koordinater for mastepositioner skyldes fejl i de it-systemer i telecentret, der har oversat koordinaterne fra teleudbyderens format til det format, som politiet anvender. Derudover kan konverteringsfejlen skyldes mangelfuld kommunikation med teleudbydere, der kan have medført, at der ikke har været klarhed over det format, der skulle konverteres.

Det er telecentrets vurdering, at fejlen kunne være forekommet i perioden fra september 2014, hvor der blev foretaget en ændring af det anvendte system, og frem til november 2016, hvor telecentret var blevet opmærksom på fejlen og foretog systemmæssige tilpasninger, der skulle sikre en korrekt oversættelse. Telecentret ses ikke på daværende tidspunkt at have orienteret politikredsene mv. om problemet.

For at udfinde de sager, hvor der er fejl i de konverterede mastekoordinater, har telecentret i august 2019 foretaget en elektronisk gennemgang af mastepositionerne i samtlige datasæt, som telecentret på dette tidspunkt havde fremfundet.

På baggrund af den elektroniske gennemgang af datasæt har telecentret identificeret knap 350 dataleverancer, hvor fejlen optræder. Det drejer sig dels om knap 130 tilfælde, hvor oplysningerne er leveret af en teleudbyder i perioden fra slutningen af august 2016 til slutningen af oktober 2016, dels om ca. 220 tilfælde, hvor oplysningerne er leveret af en anden teleudbyder i perioden fra omkring midten af marts 2015 til midten af juni 2016. I de konverterede datasæt, som telecentret har undersøgt, er alle mastepositionerne ændret med en længde af ca. 100 meter og op til ca. 220 meter i forhold til oplysningerne i rådata. Fejlen er ikke konstateret i datasæt, der er leveret i andre perioder end de ovennævnte, herunder perioden fra september 2014 og frem til juni 2015. Der er dog fundet enkeltstående eksempler på, at en rekvirent i henholdsvis 2012 og 2014 har konstateret en konverteringsfejl. Det er endnu ikke afklaret, om det skyldes fejl i it-systemet eller mangelfuld kommunikation om format med udbyder.

De pågældende identificerede sager er blevet sendt til politikredsene mv.

6.2.4. Øvrige fejl, fejlkilder og usikkerheder mv. oplyst den 18. august 2019

Rigspolitiet oplyste den 18. august 2019 Rigsadvokaturen og Justitsministeriet om, at Rigspolitiet havde konstateret flere forskellige konkrete fejl i rådata. I de følgende beskrives disse fejl. Flere af fejlene er konstateret omkring januar 2019, hvor de også efter det oplyste er blevet rettet. Alle oplysninger om fejl mv. er overdraget til Deloitte, som skal validere og konsolidere fejlene mv. samt undersøge omfanget heraf. Derudover er politikredsene mv. blevet orienteret om fejlene.

6.2.4.1. Viderestillede VoLTE-opkald

På baggrund af en henvendelse fra en politikreds konstaterede telecentret i januar 2019, at der i teledata fra én teleudbyder i visse tilfælde var blevet byttet om på retningen for viderestillede VoLTE-opkald. Det betyder, at opkald, der blev viderestillet til f.eks. en telefonsvarer eller til en anden telefon, i rådata er blevet vist som udgående opkald i stedet for indgående opkald. Teleudbyderen har rettet fejlen i januar 2019.

6.2.4.2. Udenlandske telefonnumre

Telecentret har i slutningen af 2018 eller i januar 2019 konstateret, at én teleudbyder igennem flere år i visse tilfælde, hvor oplysningerne vedrørte en udenlandsk telefon, har registreret landekoden for Danmark i rådata i stedet for hjemlandets landekode. For at imødegå denne fejl har telecentret siden februar 2019 udeladt kolonnen med landekoder i forhold til den pågældende teleudbyder.

Endvidere er det i maj 2019 konstateret, at der hos en anden teleudbyder i visse tilfælde kan være risiko for forveksling mellem udenlandske og danske telefonnumre, når der er tale om et ottecifret udenlandsk telefonnummer. For at undgå, at oplysninger om udenlandske telefonnumre, der leveres af den pågældende teleudbyder, forveksles med danske telefonnumre, har telecentret anmodet teleudbyderen om, at udbyderen skal undersøge, om der findes et tilsvarende dansk registreret telefonnummer, når der leveres teleoplysninger vedrørende udenlandske telefonnumre med otte cifre.

Herudover har telecentret i februar 2019 afdækket en fejl, hvor et udenlandsk nummer hos forskellige teleudbydere med få minutters mellemrum har været aktiv på flere master i Danmark med stor indbyrdes afstand.

6.2.4.3. Manipulerede opkald

I forbindelse med opkald og afsendelse af SMS er det ved brug af hjemmesider eller apps muligt at ændre visningen af det anvendte telefonnummer (A-nummeret) til et andet telefonnummer, således at det for modtageren af opkaldet eller SMS'en (B-nummeret) fremstår som et andet telefonnummer, der står bag aktiviteten, end den app eller lignende, som reelt er anvendt. Flere teleudbydere advarer på deres hjemmesider deres kunder om sådanne manipulerede opkald.

Aktiviteten bliver registreret i teledata vedrørende B-nummeret som en aktivitet, der er sket fra det misbrugte A-nummer. Aktiviteten bliver derimod ikke registreret i teledata vedrørende det misbrugte A-nummer, idet nummeret ikke har været anvendt til den pågældende aktivitet.

6.2.4.4. Manglende signaleringsdata

Telecentret har konstateret, at signaleringsdata i nogle sager ikke er fuldkomne. Signaleringsdata er ikke omfattet af logningsbekendtgørelsen, og der er således ikke en pligt for teleselskaberne til at logge signaleringsdata. Disse data kommer fra systemer hos teleudbyderne, der anvendes til fejlretning, og disse systemer har ikke samme høje oppetid som de systemer, der logger teledata omfattet af logningsbekendtgørelsen.

Signaleringsdata bliver indhentet særskilt fra de teleudbydere, som måtte lagre disse data og kan på nuværende tidspunkt rekvireres fra tre af de fire teleudbydere, som i dag har ansvaret for at levere teleoplysninger til politiet. Rekvirenterne kan indhente oplysningerne via telecentret, men telecentret konverterer ikke denne type data, som således sendes videre til rekvirenten i det format, som data modtages i.

Henset til at der ikke stilles særlige krav til teleudbyderens indsamling af signaleringsdata, og at der derfor kan være data, som ikke er indsamlet af teleudbyderen, kan det ikke lægges til grund, at de oplysninger om signaleringsdata, som politiet modtager, indeholder al data for den periode, som politiets anmodning vedrører.

6.3. Andre fejl, fejlkilder og usikkerheder mv., som kan have betydning for efterforskningen

Dette afsnit beskriver en række konkrete fejlkilder mv. i teledata, som politikredsene og den uafhængige kontrol- og styregruppe blev orienteret om i september 2019. Rigspolitiet foretog således i september 2019 en vurdering af, om der var fejlkilder mv. på den liste, som telecentret har udarbejdet over mulige fejl, fejlkilder og usikkerheder mv. – som politikredsene ikke tidligere var orienteret bredt om – og som det blev vurderet var tilstrækkeligt oplyst og validerede, og som det blev vurderet, at politiet på teknikerniveau burde være opmærksom på i forbindelse med igangværende og kommende efterforskninger, uagtet de tiltag der var iværksat med Rigspolitiets og Rigsadvokaturens instrukser, jf. afsnit 6.4.

De omtalte fejlkilder mv. har været drøftet med Rigsadvokaturen og herefter oplyst til politikredsene på teknikerniveau. Den uafhængige kontrol- og styregruppe er tillige orienteret om listen over mulige fejl, fejlkilder, usikkerheder mv., og om de fejlkilder mv., som politikredsene særskilt blev orienteret om i september 2019. Det er vurderingen, at de omhandlede fejlkilder mv. vil kunne opfanges ved de tiltag, der er iværksat med Rigspolitiets og Rigsadvokaturens instrukser. Fejlkilderne er af forskellig karakter og vedrører dels fejlkilder i rådata, dels konverteringsfejl.

En af fejlkilderne vedrører fejl i rådata, hvor mastekoordinater i rådata ikke passer med den tilknyttede adresse for masten. I nogle tilfælde er forskellen på over 100 km. Dette kan skyldes fejlopdateringer fra teleudbyderne, hvorfor der ikke er overensstemmelse mellem adresse og koordinater, jf. også afsnit 4.2.2.3 ovenfor. En anden fejlkilde i rådata er, at en teleudbyder anfører forkert start- eller slutmast, og hvor den geografiske afstand mellem masterne ikke er realistisk.

Der er også oplyst om en potentiel fejlkilde, hvor en udbyder ved opkald af en varighed på over 10 minutter begynder registrering af en ny aktivitet hvert 10. minut, så et opkald kan blive fordelt på oplysninger om flere aktiviteter. Det kan give anledning til den misfortolkning, at der er tale om flere opkald med samme startmast, selvom der rettelig alene er tale om ét opkald.

Herudover er der oplyst om fejl, der opstår ved afrundinger mv. af data i Excel. Ved numre på over 15 cifre sker der således i nogle tilfælde en afrunding. Det kan have haft betydning for den korrekte gengivelse af IMEI-numre, der i nogle tilfælde kan have en længde på op

til 16 cifre. Det er kun de først 14 cifre, der anvendes, men hvis der sker oprunding af de to sidste cifre, vil det kunne have en indholdsmæssig betydning. En anden fejlkilde i Excel er, at et foranstillet "0" i nogle tilfælde vil kunne blive fjernet, og det vil også kunne have en betydning for den korrekte gengivelse af IMEI-numre.

Der er endvidere informeret om en fejlkilde, der vedrører manglende konvertering eller fejlagtig konvertering af længden af aktiviteter. Det kan have betydning for brugen af teleoplysninger, hvis det er tillagt betydning, hvor længe aktiviteten har varet.

Det bemærkes, at ovenstående ikke er en udtømmende beskrivelse af mulige fejl, fejlkilder og usikkerheder mv. i teledata. Der er således tale om Rigspolitiets vurdering og forståelse af de pågældende fejl, fejlkilder, usikkerheder mv., og at oplysningerne herom – samt oplysninger om alle øvrige fejl og fejlkilder mv., som telecentret har identificeret – er blevet overdraget til den uafhængige eksterne undersøgelse som foretages af Deloitte med henblik på en konsolidering af både kendte og endnu ikke kendte fejl og fejlkilder mv. Derudover er der i flere tilfælde tale om unøjagtigheder mv. ved teledata, som både politiet, anklagemyndigheden, forsvarerne og domstolene altid bør være opmærksomme på, men som dog ikke er blevet kommunikeret klart ud til disse aktører.

6.4. Iværksatte kvalitetskontroller mv. og instrukser om brug af teledata

Rigspolitiet og Rigsadvokaturen har iværksat flere tiltag for at imødegå de konstaterede fejl.

Den 28. november 2018 ændrede telecentret den vejledning, som leveres til rekvirenten sammen med rådata og konverterede teledata, for at gøre rekvirenten opmærksom på at kontrollere, at de konverterede data var komplette.

Endvidere iværksatte telecentret i marts 2019 en automatisk tællekontrol, der har til formål at sikre, at der i de enkelte rekvisitioner er overensstemmelse mellem antallet af rækker data i rådata og konverteret data. Det fremgår herefter af en e-mail, der ledsager den fil med teledata, der leveres til rekvirenten, at modtageren manuelt skal kontrollere, om antallet af aktiviteter i rådata stemmer overens med antallet af aktiviteter i det konverterede data, før der iværksættes analyse og behandling af teledata. Meddelelsen gør samtidig modtageren opmærksom på det konkrete antal aktiviteter (rækker i regnearket) i de rådata og konverte-

rede data, som leverancen indeholder, herunder om antallet af rækker i de respektive datasæt stemmer overens. Hvis antallet af rækker i de leverede datasæt ikke stemmer overens, er dette særligt fremhævet i meddelelsen til modtagerne af datasættene.

Som supplement til den manuelle kontrol i politikredsene mv. har telecentret fra den 24. april 2019 indført en systematisk manuel kontrol af de datasæt, der er leveret til politikredsene mv., hvor det kontrolleres om antallet af rækker i de respektive datasæt stemmer overens. Hvis det konstateres, at der mangler oplysninger, bliver politikredsen mv. kontaktet hurtigst muligt.

Københavns Politi gjorde den 19. juni 2019 telecentret opmærksom på, at de ved en manuel kontrol havde konstateret en fejl i en meddelelse, de havde fået sammen med konverterede data. Det fremgik af meddelelsen, at rådata og konverterede data bestod af lige mange rækker, hvilket ikke var tilfældet. Telecentret konstaterede herefter, at der var fejl i den automatiske kontrol, der blev iværksat den 8. marts 2019. Telecentret gennemgik på den baggrund alle rekvisitioner for perioden fra den 8. marts 2019 til den 19. juni 2019 og konstaterede herved, at der i få tilfælde havde været fejl i den automatiserede tællekontrol. Rekvirenterne i de omhandlede sager blev efterfølgende underrettet herom, og komplette konverterede datasæt blev sendt. Telecentret har oplyst, at fejlen blev rettet den 19. juni 2019.

Rigsadvokaturen instruerede ved instruks af 2. juli 2019 alle anklagere om, at der i forbindelse med behandlingen af straffesager, hvori der indgår teleoplysninger, generelt skal udvises betydelig forsigtighed med at tillægge manglende teleoplysninger den betydning, at der ikke har været telekommunikation eller lignende. Rigsadvokaturen gjorde endvidere opmærksom på, at politiet og anklagemyndigheden i forbindelse med efterforskningen skal være særligt opmærksomme på, at teleoplysningerne kan være mangelfulde, og at det samme gælder, når anklagemyndigheden skal vurdere tiltalespørgsmålet og ved sagernes behandling i retten.

Rigsadvokaturen udsendte efterfølgende den 18. august 2019 en instruks til landets anklagere om, at anklagere ikke må anvende teledata, herunder signaleringsdata og teleobservation, under hovedforhandlinger eller retsmøder vedrørende opretholdelse af anholdelse. Det fremgår af brevet, at det midlertidige stop indtil videre vil gælde i 2 måneder. Rigsadvokaturen har ved brev af 13. september 2019 til alle embeder præciseret, at det midlertidige stop for brug af teledata ikke omfatter oplysninger indhentet af politiet via GPS-enheder,

idet disse oplysninger håndteres i Rigspolitiets særskilte system herfor og ikke behandles som teleoplysninger.

For så vidt angår anvendelsen af teledata under andre dele af efterforskningen end som grundlag for varetægtsfængsling, har Rigspolitiet ved brev af 30. august 2019 til politikredsene mv. og i instruks af 18. september 2019 fastsat retningslinjer for politiets anvendelse af teledata under efterforskningen. Heri instrueres sagsbehandlere i at udvise særlig opmærksomhed ved gennemgangen, kontrollen og brugen af teledata, og herunder være særligt opmærksomme på de fejl, fejlkilder og usikkerheder, der foreløbigt er konstateret. Ved retsmøder under efterforskningen, hvor der fremsættes anmodning om tvangsindgreb, skal anmodninger fremover basere sig på rådata. Det betyder, at anmodninger kan fremsættes direkte på baggrund af rådata, eller på baggrund af konverteret data som hjælpebilag, når der samtidig er anført krydshenvisninger til rådata. Rigsadvokaturen udsendte ligeledes en instruks af 30. august 2019 med henvisning til Rigspolitiets retningslinjer af samme dato, hvor alle anklagere tilsvarende blev instrueret i, at anmodninger om tvangsindgreb under efterforskningen skal basere sig på rådata.

I forlængelse af ovenstående tiltag iværksatte Rigspolitiet den 27. august 2019 en ekstern undersøgelse for hurtigst muligt at skabe tilstrækkelig klarhed over de fejl, fejlkilder og usikkerheder, som er forbundet med brug af teledata, så teledata igen kan anvendes som bevis i straffesager, jf. afsnit 6.1 ovenfor.

7. Håndtering af verserende og afsluttede straffesager

I dette kapitel beskrives, hvilke retningslinjer Rigsadvokaturen og Rigspolitiet har fastsat for processen for gennemgang af de straffesager, hvori der er indgået teledata. I afsnit 7.1 beskrives de retningslinjer, der blev fastsat forinden nedsættelsen af kontrol- og styregruppen den 2. juli 2019, hvorefter der i afsnit 7.2 følger en kort beskrivelse af kontrol- og styregruppens opgaver samt de retningslinjer, Rigsadvokaturen og Rigspolitiet har fastsat efter nedsættelsen af kontrol- og styregruppen.

7.1. Perioden før 2. juli 2019

Som anført i Rigsadvokaturens orienteringsbrev til Advokatrådet og Landsforeningen af Forsvarsadvokater, som blev sendt i kopi til Domstolsstyrelsen, igangsatte Rigsadvokaturen og Rigspolitiet den 13. juni 2019 en gennemgang alle straffesager, hvori konverteringsfejlen potentielt kunne være opstået.

Til brug for gennemgangen havde telecentret identificeret ca. 10.700 sager (journalnumre), hvor der i perioden fra 1. januar 2012 til 8. marts 2019 var indhentet teledata.

Det blev i forbindelse med gennemgangen besluttet at skelne mellem følgende sagskategorier:

1) Sager, der aktuelt verserer ved domstolene, f.eks. hvor sigtede er varetægtsfængslet, hvor der er berammet retsmøde i sagen, eller hvor sagen er under anke.
2) Sager, der er afsluttet ved domstolene, hvor den domfældte enten
    a. afsoner en frihedsstraf mv., eller
    b. er underlagt en foranstaltning, undergivet tilsyn, prøvetid eller vilkår mv., eller har et aktivt indrejseforbud til Danmark.
3) Sager, der er afsluttet ved domstolene, hvori den domfældte er blevet idømt en sanktion, der nu er udstået.
4) Sager, der er afsluttet ved domstolene eller af politiet eller anklagemyndigheden, og hvori der er sket frifindelse af tiltalte, påtaleopgivelse over for sigtede, eller hvor efterforskningen er indstillet.
5) Sager, der aktuelt efterforskes af politiet.

Det blev besluttet, at sagstyperne nævnt under pkt. 1) og 2a) skal have høj prioritet. Det blev desuden besluttet, at der skal være særlig opmærksomhed på sager, hvori der allerede er konstateret uoverensstemmelse mellem rådata fra teleselskaberne og de konverterede data, eller det i øvrigt er konstateret, at der mangler teleoplysninger, eller hvor forsvareren har rettet henvendelse til politiet vedrørende problemstillingen.

Den 17. juni 2019 indskærpede Rigsadvokaturen over for de regionale statsadvokater og lokale anklagemyndigheder, at anklagerne i sager, der aktuelt verserede ved domstolene, hvori teledata indgik som bevis, før der skulle afholdes retsmøde i sagen, skulle sikre, at det var undersøgt og dokumenteret, at der ikke var uoverensstemmelse mellem rådata og konverterede data, som indgik i sagen.

Den 21. juni 2019 blev der udsendt nærmere retningslinjer for sagsgennemgangen af de regionale statsadvokater.

Retningslinjerne, der i vidt omfang fortsat er gældende, indebærer bl.a., at der i *verserende* sager udarbejdes en efterforskningsrapport om den fornyede gennemgang af teleoplysningerne til sagen, som sendes til forsvareren og retten. Hvis der konstateres uoverensstemmelse mellem rådata fra teleselskaberne og de konverterede data, eller der i øvrigt mangler teledata, vurderer anklagemyndigheden, om de nu foreliggende oplysninger har betydning for sagens behandling, herunder om der skal fremsættes begæring om udsættelse af sagen og eventuelt ske løsladelse af varetægtsarrestanter. I alle *afsluttede* sager med manglende oplysninger udarbejdes der også en efterforskningsrapport, som ligeledes sendes til forsvareren, når det konstateres, at der mangler oplysninger. For så vidt angår sager, der er afsluttet ved domstolene, og hvor den dømte er frihedsberøvet mv., udarbejdes efterforskningsrapporten om den fornyede gennemgang af de relevante teledata til sagen hurtigst muligt. Hvis der konstateres uoverensstemmelse mellem rådata fra teleselskaberne og de konverterede data, eller der i øvrigt mangler teledata, vurderer anklagemyndigheden, om fejlen er af en sådan karakter, at det har betydning for sagens behandling, herunder om der er grundlag for, at anklagemyndigheden begærer straffesagen genoptaget. Hvis det konstateres, at der i en straffesag har manglet teledata, fremsendes de manglende data til forsvareren sammen med efterforskningsrapporten.

Anklagemyndighedens vurdering af sager omfattet af teledatasagen vil ske med udgangspunkt i reglerne i retsplejelovens §§ 976 og 977, som omhandler genoptagelse af en afsluttet straffesag på begæring af rigsadvokaten eller en domfældt. Det fremgår af retsplejelovens § 976, at genoptagelse af en afsluttet straffesag, hvorunder den tiltalte er blevet frifundet, kan finde sted efter rigsadvokatens begæring, bl.a. når det ifølge en tilståelse, tiltalte senere har afgivet, eller andre beviser, der senere er kommet for dagen, må antages, at tiltalte har begået forbrydelsen. Det fremgår bl.a. af retsplejelovens § 977, at genoptagelse på begæring af den domfældte af en pådømt sag kan finde sted, når nye oplysninger tilvejebringes, og det skønnes antageligt, at disse, hvis de havde foreligget under sagen, kunne have bevirket frifindelse eller anvendelse af en væsentlig mildere bestemmelse. Genoptagelse kan endvidere ske, når der foreligger særlige omstændigheder, der gør det overvejende sandsynligt, at de foreliggende bevisligheder ikke har været rigtigt bedømt. Begæring om genoptagelse fremsættes for Den Særlige Klageret, som træffer afgørelse i sagen ved kendelse, jf. retsplejelovens § 982. Anklagemyndigheden kan efter fast praksis også begære en fældende dom genoptaget, selvom dette ikke fremgår direkte af ordlyden af retsplejelovens § 977, stk. 1.

Når anklagemyndighedens vurdering af, om der er grundlag for at søge sagen genoptaget på anklagemyndighedens foranledning, foreligger, skal forsvareren orienteres herom. Det gælder både, når sagen søges genoptaget, og når der ikke er fundet grundlag herfor. Beslutninger om ikke at søge genoptagelse skal i givet fald begrundes i orienteringen.

Den 21. juni 2019 udsendte Rigspolitiet også en vejledning til politikredsene om håndteringen af sagerne. Det fremgår bl.a. heraf, at der er udarbejdet en online indberetningsoversigt til brug for politikredsenes gennemgang, ligesom det er beskrevet, hvordan gennemgangen skal foretages. Det fremgår også, at telecentret indledningsvist foretager en maskinel test, hvorefter kredsene manuelt skal kontrollere sagerne og udfærdige rapporter om gennemgangen og resultatet heraf. Rigspolitiets vejledning blev efterfølgende udbygget den 12. juli 2019 og igen den 5. september 2019.

I tilknytning til retningslinjerne udsendte Rigspolitiet i slutningen af juni 2019 og begyndelsen af juli 2019 forskellige koncepter til brug for udfærdigelse af de efterforskningsrapporter, der skal dokumentere den gennemgang, der foretages i den konkrete straffesag.

7.2. Perioden fra 2. juli 2019

Den 2. juli 2019 nedsatte justitsministeren en uafhængig kontrol- og styregruppe, der har fået et bredt mandat til at kontrollere og styre myndighedernes sagsgennemgang.

Det følger af kommissoriet for kontrol- og styregruppen, at den skal føre kontrol med og styre myndighedernes gennemgang af de pågældende straffesager. Derudover skal gruppen fastsætte de nærmere retningslinjer for processen og kriterierne for den indledende screening af straffesager, hvori teleoplysninger er indgået.

Endvidere kan kontrol- og styregruppen anbefale fremsættelse af lovforslag, hvis de retningslinjer, som gruppen fastsætter for gennemgangen af straffesager, hvori der er indhentet teleoplysninger, indebærer, at der er behov for lovændringer, herunder i forhold til reglerne om genoptagelse.

Kontrol- og styregruppen tilkendegav allerede dagen efter udpegning af gruppens medlemmer overfor Rigspolitiet og Rigsadvokaturen, at myndighedernes allerede trufne foranstaltninger med henblik på at rette op på de begåede fejl og for at forhindre kommende fejl kan fortsætte, indtil den uafhængige kontrol- og styregruppe træffer andre beslutninger. Eksempelvis vil gruppen kunne bestemme, at der skal ske en fornyet gennemgang af sager, som myndighederne har gennemgået.

Samme dag udstedte Rigsadvokaturen en instruks til alle anklagere, hvoraf det bl.a. fremgår, at der i forbindelse med behandlingen af straffesager, hvori der indgår teleoplysninger, generelt skal udvises betydelig forsigtighed med at tillægge manglende teleoplysninger den betydning, at der ikke har været telekommunikation eller lignende.

Den 3. juli 2019 udsendte de regionale statsadvokater supplerende retningslinjer og brevskabeloner til brug for sagsgennemgangen. Heraf fremgår bl.a., at den anklagerfaglige vurdering af de konkrete straffesager, hvor politiet har konstateret uoverensstemmelse mellem rådata og de konverterede data, forestås af de embeder, der anklagerfagligt har håndteret sagerne.

Kontrol- og styregruppen fastsatte den 19. juli 2019 retningslinjer for gennemgangen af straffesager, der er omfattet af teledatasagen. Heraf følger bl.a., at Rigspolitiet og Rigsad-

vokaturen som udgangspunkt skal forelægge påtænkte ændringer af eksisterende retningslinjer eller udstedelse af nye retningslinjer for kontrol- og styregruppen. Den påtænkte retningslinje kan herefter som hovedregel sættes i kraft en uge efter, at underretningen er sendt til den uafhængige kontrol- og styregruppe, hvis ikke gruppen inden udløbet af fristen meddeler, at retningslinjen ikke kan sættes i kraft. Vurderes det, at det undtagelsesvis er nødvendigt at sætte retningslinjen i kraft øjeblikkeligt, eller at fristen undtagelsesvis skal være kortere end en uge, kan retningslinjen om ikrafttrædelse fraviges. Dette forudsætter, at Rigspolitiet og Rigsadvokaturen over for den uafhængige kontrol- og styregruppe nærmere begrunder, hvorfor der foreligger en undtagelsessituation. Det fremgår endvidere, at Rigspolitiet og Rigsadvokaturen løbende skal orientere kontrol- og styregruppen om status over politiets og anklagemyndighedens sagsgennemgang, og at Rigspolitiet og Rigsadvokaturen skal fremsende eksisterende og kommende skriftligt materiale, som kan have betydning for kontrol- og styregruppens arbejde.

Rigspolitiet og Rigsadvokaturen har siden den 19. juli 2019 løbende oversendt forskellige retningslinjer til kontrol- og styregruppen, jf. den fastsatte procedure. Det drejer sig bl.a. om retningslinjer for håndtering af sager med domfældte, der endnu ikke er indkaldt til afsoning, håndtering af sager med udviste, der endnu ikke er udsendt, håndtering af sager med kendelser om varetægtsfængsling in absentia, håndtering af sager hos SØIK, Grønlands Politi og Færøernes Politi, og håndtering af sager, der indledningsvist er efterforsket af Politiets Efterretningstjeneste. Kontrol- og styregruppen har indtil videre ikke haft bemærkninger til de tilsendte retningslinjer.

I forbindelse med nye oplysninger fra Rigspolitiet i teledatasagen, herunder om fejl i forbindelse med konverteringen af geografiske koordinater for telemasters placering og konkrete fejl, fejlkilder og usikkerhed i rådata, udstedte Rigsadvokaturen den 18. august 2019 en instruks, der indførte et midlertidigt stop for anklageres anvendelse af teledata under hovedforhandlinger eller retsmøder vedrørende varetægtsfængsling og opretholdelse af anholdelse.

Den 13. september 2019 præciserede Rigsadvokaturen, at oplysninger indhentet af politiet via GPS-enheder, og som håndteres i Rigspolitiets særskilte system, som følge deraf ikke er omfattet af det midlertidige stop for brug af teledata.

Som følge af fejlen i forbindelse med konverteringen af geografiske koordinater for telemasters placering sendte Rigspolitiet den 16. august 2019 en foreløbig liste over de journalnumre, hvor Rigspolitiet havde identificeret fejl i forbindelse med konverteringen af geografiske koordinater for telemasters placering.

Den 17. august 2019 kategoriserede Rigsadvokaturen de fremsendte journalnumre, så de kunne indgå i kredsenes prioriterede sagsgennemgang. Herefter fremsendte Rigsadvokaturen den kategoriserede liste til de regionale statsadvokater med henblik på videresendelse til politikredsene.

Denne proces fortsatte i takt med, at Rigspolitiet identificerede de berørte journalnumre.

Den 28. august 2019 havde Rigspolitiet gennemgået al data til rådighed for fejlen med konvertering af de geografiske koordinater og sendte de foreløbigt sidste journalnumre til Rigsadvokaturen.

Den 29. august 2019 havde Rigsadvokaturen kategoriseret de senest modtagne journalnumre med fejlen i konvertering af de geografiske koordinater og sendte herefter journalnumrene til de regionale statsadvokater med henblik på videresendelse til politikredsene.

Den 30. august 2019 udsendte Rigsadvokaturen en instruks for anklageres anvendelse af teledata under efterforskningen til alle embeder. Det fremgår bl.a. af instruksen, at ved retsmøder under efterforskningen, hvor der fremsættes anmodning om tvangsindgreb, skal anmodninger fremover basere sig på rådata. Det betyder, at anmodninger kan fremsættes direkte på baggrund af rådata, eller på baggrund af konverteret data som hjælpebilag, når der samtidig er anført krydshenvisninger til rådata.

Samme dag udsendte Rigspolitiet retningslinjer for politiets anvendelse af teledata under efterforskningen. Heraf fremgår bl.a., at politiet fortsat kan anvende teledata i efterforskningen, men at politiet på efterforskningsstadiet skal udvise forsigtighed ved anvendelsen af teledata. Som følge af at anmodninger om tvangsindgreb fremover skal basere sig på rådata, skal der fremover som hovedregel ved udfærdigelse af efterforskningsrapporter, hvor der refereres fra konverteret teledata, anføres en krydshenvisning til rådata.

Der var vedlagt et enslydende bilag til begge skrivelser om foreløbigt konstaterede fejl, fejlkilder og usikkerheder i teledata. Bilaget skal både anvendes af sagsbehandlerne under efterforskningen og vedlægges anmodninger om tvangsindgreb til retten.

Den 18. september 2019 udsendte Rigspolitiet en instruks for politiets anvendelse af teledata til brug for retsmøder under efterforskningen, der fastsætter de nærmere krav til politiets anvendelse af og kontrol med teledata samt dokumentation for sammenhængen mellem rådata og konverteret data i de tilfælde, hvor teledata skal anvendes i retsmøder under efterforskningen.

Det kan herudover oplyses, at Rigspolitiet og Rigsadvokaturen løbende har afholdt videomøder med alle embeder med henblik på at afklare usikkerheder om håndteringen af sagsgennemgangen og herunder besvare spørgsmål om forståelsen af de udsendte retningslinjer.

8. Kontrol og kvalitetssikring

Rigspolitiets Enhed for Tilsyn og Controlling (herefter ToC) har i perioden ultimo juni til 25. september 2019 undersøgt telecentrets håndtering og behandling af teledata med særligt fokus på proces- og arbejdsgange, kvalitetssikringsaktiviteter og kontroller, opsamling på identificerede fejl samt ledelsesmæssig orientering og håndtering af identificerede fejl. I afsnit 8.1 redegøres for de væsentligste observationer i ToC's undersøgelse. I afsnit 8.2 sammenfattes de observationer og resultater, som ToC's undersøgelse har givet anledning til.

ToC er politiets interne kontrol og tilsynsenhed, der på anmodning eller af egen drift kan iværksætte undersøgelser af alle aspekter af politiets virksomhed. For at sikre enhedens uafhængighed refererer enheden direkte til Rigspolitiets direktion. Den konkrete undersøgelse af telecentret blev indledt i dagene efter mødet den 19. juni 2019 hos rigspolitichefen, jf. afsnit 5.5.

Den uafhængige eksterne undersøgelse forestået af Deloitte skal også foretage en uafhængig gennemgang af den nuværende kvalitetskontrol, der udføres i forhold til de teledata, der modtages, opbevares og behandles i telecentret fra de modtages fra teleudbyderne til de afleveres til politikredsene mv. Det er hensigten, at gennemgangen skal munde ud i anbefalinger til, hvorledes kvalitetskontrollen kan styrkes. For så vidt angår den uafhængige eksterne undersøgelse henvises til Deloittes rapport.

Rigspolitiet og Rigsadvokaturen har endvidere bl.a. fra Justitsministeriet modtaget oplysninger fra en tidligere medarbejder i telecentret om en række udfordringer med bl.a. de it-systemer, der anvendes i telecentret, herunder at de er baseret på gammel software og forældet infrastruktur. Oplysningerne er videregivet til Deloitte med henblik på, at oplysningerne skal indgå og konsolideres i den eksterne undersøgelse.

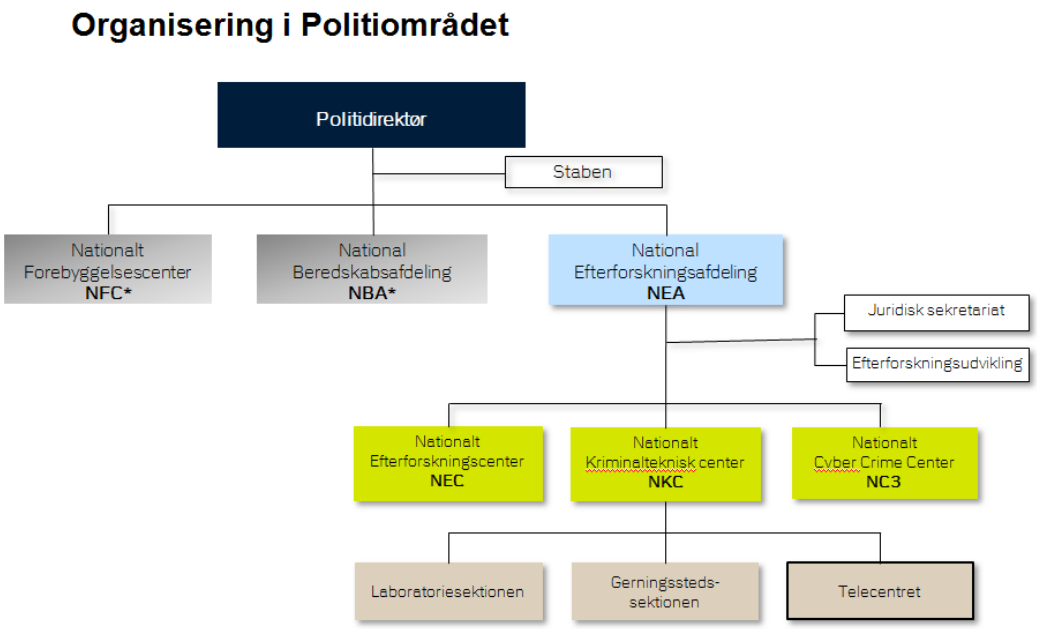
8.1. Enheden for Tilsyn og Controllings undersøgelse

I de følgende afsnit er de faktuelle forhold, der fremgår af ToC's undersøgelse, gengivet. Afsnit 8.1.1 omhandler telecentrets organisatoriske placering, og afsnit 8.1.2 omhandler retningslinjer, vejledninger og procedurer for håndtering af teledata. I afsnit 8.1.3 gengives ToC's beskrivelse af dokumentation af systemer og systembeskrivelser, og i afsnit 8.1.4 gengives beskrivelsen af kontrol- og kvalitetssikringsaktiviteter i forhold til teledata. Afsnit

8.1.5 gengiver beskrivelsen af telecentrets opsamling og opfølgning på fejl, afsnit 8.1.6 gengiver beskrivelsen af samarbejde med og orientering af relevante aktører, herunder politikredsene og teleudbyderne, og afsnit 8.1.7 gengiver ToC's beskrivelse af den ledelsesmæssige orientering og håndtering af potentielle og identificerede fejl.

8.1.1. Rigspolitiets Telecenters organisatoriske placering

Frem til maj 2014 var telecentret en del af KIT. Den 1. maj 2014 blev størstedelen af telecentret flyttet til Politiområdet i Rigspolitiet som en del af det nyoprettede NC3. Den 24. juni 2019 blev telecentret organisatorisk flyttet til NKC.



*Underliggende organisationsstruktur i NFC og NBA er ikke illustreret

Enkelte medarbejdere, der arbejder med telecentrets tekniske infrastruktur, er fortsat organisatorisk placeret i KIT. Medarbejderne i KIT er fast dedikerede ressourcer, der håndterer infrastrukturen i it-systemerne relateret til teledata. De tilhørende applikationer, herunder udvikling og fejlretning af funktionaliteten i de anvendte applikationer, håndteres af telecentrets tekniske medarbejdere i Politiområdet.

En sådan placering af drift og udvikling af it-applikationer i et forretningsområde følger ikke den sædvanlige organisering i Rigspolitiet ved drift af it-systemer, men den var baseret på et ønske om en tæt tilknytning til det politifaglige forretningsområde og sikkerhedsmæssige hensyn.

8.1.2. Retningslinjer, vejledninger og procedurer for håndtering af teledata

ToC har konstateret, at der i undersøgelsesperioden ikke har været skriftlige retningslinjer, vejledninger eller procedurer til internt brug i telecentret i relation til håndtering af teledata.

Rigsadvokaturens vejledning om forberedelse og præsentation af teleoplysninger i retten fra 14. marts 2014 med tilhørende bilag, der er tilgængelig på politiets intranet, beskriver, hvordan teledata modtaget fra telecentret bedst muligt kan fremstilles visuelt med henblik på efterfølgende præsentation i retten. Vejledningen er senest opdateret den 31. januar 2018.

Der er ikke i undersøgelsesperioden udarbejdet nationale retningslinjer for, hvordan politikredsene skal håndtere og kvalitetssikre data, der modtages fra telecentret. Telecentret sender en teknisk vejledning til rekvirenten sammen med fremsendelse af data. Vejledningen indeholder bl.a. oplysninger om, hvilke data de modtagne filer indeholder, og hvordan filerne åbnes og efterfølgende indlæses. Den tekniske vejledning er ikke dateret, og det er dermed ikke klart, hvornår vejledningen har været gældende fra.

Den senest opdaterede tekniske vejledning er taget i brug i december 2018. I den opdaterede vejledning fremgår det som noget nyt, at rekvirenten altid skal kontrollere, om antallet af aktiviteter i rådata er overensstemmende med de konverterede data.

Enkelte politikredse har udarbejdet lokale vejledninger for deres behandling af teleoplysninger. De lokale vejledninger har primært fokus på at fastsætte og præcisere fremgangsmåden ved indgreb i meddelelseshemmeligheden og destruktion af materiale fra indgreb i meddelelseshemmeligheden.

Det er oplyst, at der i NC3 siden 2017 har været et generelt fokus på at øge graden af skriftlighed og dokumentation. Telecentret har dog oplyst, at de ikke har oplevet, at dette fokus har været rettet mod telecentrets arbejde.

8.1.3. Dokumentation af systemer og systembeskrivelser

ToC har konstateret, at der i undersøgelsesperioden ikke har været systembeskrivelser af de it-systemer og databaser, der bruges i telecentret i forbindelse med håndteringen af teledata.

Telecentret har i 2011 udarbejdet en flowbeskrivelse for telecentrets egenudviklede it-løsning, der indhenter data fra leverandøren og afsender det bestilte data til rekvirenten. Den egenudviklede løsning er siden 2011 blevet videreudviklet, men uden en tilhørende opdatering af flowbeskrivelsen.

Der blev ikke udarbejdet en kravsspecifikation for løsningen, da telecentret i januar 2015 påbegyndte udviklingen af en ny egenudviklet platform til konverteringen af teledata, der blev afsluttet i november 2016. Det er derfor af den tilgængelige information uklart, hvad behovet var, og om den udviklede løsning mødte behovet.

Rigspolitiet har igangsat et arbejde med at udvikle et nyt og mere tidssvarende system til konvertering og lagring af teledata. Der er ikke udarbejdet projektinitieringsdokument, business case, kravsspecifikation eller lignende, hvilket ellers er udgangspunktet i Rigspolitiet ved udvikling eller tilpasning af allerede eksisterende it-systemer.

8.1.4. Kontrol- og kvalitetssikringsaktiviteter af teledata

8.1.4.1. Telecentrets kontrol af data

ToC konstaterer, at de eksisterende kontroller i telecentret primært har haft fokus på at sikre, at data kan leveres til rekvirenten med den fornødne hurtighed af hensyn til den igangværende efterforskning og sagsbehandling, og i mindre grad på at validere kvaliteten af data. Det understøttes af følgende:

- der er etableret en automatiseret teknisk kontrol, der registrerer, om der er afvigelser i modtagne rådata fra teleudbyderen. I disse tilfælde flyttes filen til en mappe med afviste filer med en tilhørende fejllog. Det kan være afvigelser som følge af linjeskift i en datarække eller en ikke læsbar karakter i datasættet. Kontrollen fungerer dermed som en teknisk validering af filen inden den efterfølgende konvertering,

- i forbindelse med indlæsning af konverterede data i telecentrets database gennemfører telecentrets egenudviklede applikation hvert 10. minut en automatisk kontrol af, om indsatte konverterede data i databasen har samme antal rækker som rådata. Kontrollens funktion er dog primært at sikre, at data bliver afsendt til rekvirenten, så snart data er blevet importeret, snarere end at sikre overensstemmelsen mellem rådata og konverterede data.

En timerfunktion i telecentrets egenudviklede applikation har sikret, at data blev sendt til rekvirenten senest 60 minutter efter, at data fra leverandøren var blevet kendt i telecentrets systemer. Timerfunktionen medførte, at data blev sendt, selvom der ikke var overensstemmelse mellem antal rækker i rådata og konverteret data. Det vil sige, at den eventuelle effekt af ovenstående 10 minutters kontrol blev tilsidesat.

Timeren har haft til formål at sikre, at data sendes hurtigst muligt til rekvirenten. Timeren er på baggrund af tilbagemeldinger fra politikredsene flere gange blevet ændret med forskellige indstillinger og har været indstillet til at sende data efter både 30 minutter og 1, 3, 6 og 24 timer. I perioden fra december 2012 til og med januar 2017 har timeren været indstillet til at sende data efter 30 minutter. Fra januar 2017 har timeren været indstillet til 1 time. Det har været intentionen, at det fuldstændige datasæt automatisk skulle fremsendes senere, hvis rekvirenten ikke havde modtaget det fulde datasæt i første omgang. Det er uklart, om og eventuelt i hvilket omfang denne funktionalitet har fungeret i undersøgelsesperioden.

Telecentret har i marts 2019 fjernet timerfunktionen. Telecentret har derudover i marts 2019 tilføjet et afsnit i den e-mail, der sendes til rekvirenten sammen med data. I e-mailen fremgår antallet af aktiviteter/rækker i henholdsvis modtagne rådata og konverteret data.

Ultimo 2018 opsatte telecentret derudover en øget fejllogning i forbindelse med import af konverterede data til deres database.

8.1.4.2. Politikredsenes kontrol af modtagne data

Af Rigspolitiets kundgørelse B nr. 31 om it-kriminalitet mv., hvor it-kriminalitet bl.a. defineres som værende *"kriminalitet, hvor digitale spor indgår i efterforskningen"*, og dermed også omhandler teledata, fremgår der passager om kvalitetssikring.

Det fremgår af kundgørelsen, at der er et delt ansvar mellem politikredsene og NC3, hvor telecentret i størstedelen af undersøgelsesperioden har været organisatorisk forankret, for at sikre kvaliteten af teledata, der anvendes til efterforskning og efterfølgende bevisførelse. NC3 er ansvarlig for at sikre, at de metoder og systemer, der anvendes til indhentning og bearbejdning af digitale spor, er velfungerende og har den fornødne kvalitet. Politikredsene er ansvarlige for at foretage den endelige kvalitets- og legalitetskontrol af efterforsknings- og bevismaterialet.

Politiområdet har medio 2019 hørt politikredsene om kredsenes kontrol og kvalitetssikring af teledata fra telecentret. Enkelte politikredse har angivet, at de ved modtagelse af teledata har særskilte arbejdsgange for at sikre kontrol med og kvalitetssikring af indhentede teledata. En politikreds har i høringssvaret angivet, at årsagen til, at kredsen ikke har haft særskilte kontroller med indhentede teleoplysninger er, at de ikke har haft anledning til at sætte spørgsmålstegn ved validiteten af modtagne teleoplysninger fra telecentret før orienteringen om de nu identificerede fejl i teledata.

Kredsenes høringssvar viser endvidere, at politikredsenes efterforskere erhverver kompetencer i forhold til teledata til brug for efterforskning ved enten sidemandsoplæring eller på kurser om teledata.

Kurserne er dog som udgangspunkt henvendt til kredsenes tele- og dataanalytikere og ikke til efterforskere og er først blevet udbudt i starten af 2018. En stor del af efterforskernes kompetenceopbygning synes derfor baseret på sidemandsoplæring, hvilket kan betyde, at politikredsenes efterforskere ikke nødvendigvis har kompetencerne til at kunne kontrollere kvaliteten af de modtagne datasæt. Det kan i denne sammenhæng nævnes, at Rigsadvokaturen årligt udbyder kurset "Teleoplysninger i retten", målrettet anklagere.

8.1.5. Opsamling og opfølgning på fejl

Der er som beskrevet i kapitel 6 identificeret fejlkilder ved håndteringen af teledata, som politikredsene modtager til deres efterforskning.

Der har i størstedelen af ToC's undersøgelsesperiode ikke været en fast praksis eller procedure i telecentret for at notere eller dokumentere indmeldte fejl og tilhørende beskrivelse af eventuel fejlløsning i et centralt system eller dokument.

Telecentret har oplyst, at det er muligt at indrapportere fejl i modtagne data på forskellig vis:

- e-mail til telecentrets funktionspostkasse,
- opkald pr. telefon til telecentrets it-support,
- e-mail direkte til medarbejdere i telecentret,
- opkald direkte til medarbejdere i telecentret eller
- via en informationsportal på politiets intranet.

Telecentret har i størstedelen af undersøgelsesperioden ikke haft en fast praksis eller procedure for at notere og dokumentere indmeldte fejl i et centralt system eller dokument, hvor man ligeledes kunne beskrive en eventuel fejlløsning. Telecentret har dog forklaret, at de i en 2-årig periode i årene mellem 2011-2014 har anvendt en HP-servicemanager til fejlhåndteringsprocesser.

Ultimo 2018 har NC3 oprettet en side på intranettet, der indeholder information om de fejl, som enten politikredsene eller telecentret har konstateret siden december 2018. Af siden fremgår, hvornår fejlen er blevet meldt ind og status for udbedring af fejlen. Det bemærkes, at ikke alle potentielle modtagere af teledata har adgang til oplysninger på siden, da adgang kræver særlige rettigheder.

I de tilfælde, hvor der er blevet indmeldt et problem med et datasæt fra en rekvirent, er det blevet oplyst fra telecentret, at dette ofte er blevet løst ved, at den pågældende fil er blevet gennemgået, og telecentret herefter har foretaget en genkørsel af anmodningen. Rekvirenten har herefter modtaget datasættet på ny. Som eksempel er fejlmeldinger vedrørende konverteringsfejl som udgangspunkt blevet løst teknisk ved, at telecentret fejlsøger problemet, retter den konkrete fejl om muligt, genkonverterer data og genfremsender data til rekvirenten.

Medarbejderne i telecentret har således i hele undersøgelsesperioden løbende løst rekvirenternes problemer med data. Disse er samtidig søgt løst hurtigst muligt, således at den igangværende efterforskning ikke forsinkes unødigt.

Metoden til løsning af problemet har været individuel og er ikke dokumenteret.

Telecentret har samtidig oplyst, at hvis et problem har optrådt flere gange, har medarbejderne forsøgt at finde en løsning, der kunne forhindre problemet i at optræde fremadrettet. Der har dog i mindre grad været en fælles refleksion over de konstaterede fejl, og det har medvirket til, at fejl blev løst, uden at det blev undersøgt, hvorfor fejl forekom igen og igen.

8.1.6. Samarbejde og orientering af relevante aktører, herunder politikredsene og teleudbyderne

8.1.6.1. Samarbejde og orientering af politikredsene mv.

Telecentret har via centrets egen nyhedsportal løbende informeret og gjort politikredsene mv. opmærksomme på forskellige typer af information og nyheder, der både vedrører identificerede fejl i telecentrets egne systemer, informationer, der vedrører teleudbyderen, og nyheder, der kan have betydning for rekvirering af teledata.

I de tilfælde, hvor informationen vedrører identificerede fejl i eksempelvis telecentrets egne systemer eller i teleudbyderens data, vil det af nyheden som udgangspunkt fremgå, hvis den identificerede fejl er blevet løst hos enten telecentret eller teleudbyderen.

Telecentret har i 2010, 2015 og 2017 oprettet brugerfora med deltagelse af alle politikredse, task-forces og efterforskningsfællesskaber m.fl. og planlagt nyhedsbreve.

I relation til samarbejdet med politikredsene blev der medio 2017 i regi af NEC oprettet en erfa-gruppe for tele- og dataanalytikere i politikredsene og efterforskningsfællesskaberne. Baggrunden for oprettelsen var, at NEC i starten af 2017 havde afholdt et opstartsmøde med tele- og dataanalytikere, der havde efterspurgt et formelt mødeforum, der gav mulighed for at fremlægge generelle problemstillinger, intern sparring og udveksling af information. Erfa-gruppen har en målsætning om at mødes minimum en gang årligt.

Derudover er der i september 2018 etableret en møderække med repræsentanter fra Særlig Efterforskning Øst (SEØ), Særlig Efterforskning Vest (SEV), NEC og NC3/telecentret. På møderne er der primært blevet drøftet udfordringer med teledata og arbejdet med at finde løsninger.

Efter oprettelse af netværket har der været fokus på at bruge netværket til at holde brugerne informeret om fejl, problemstillinger og udviklinger på området.

8.1.6.2. Samarbejdet med teleudbyderne

Telecentret har i de tilfælde, hvor en fejlindmelding har omhandlet mangelfulde oplysninger i rådata fra leverandøren, kommunikeret direkte med teleudbyderne med henblik på at udbedre fejlen.

ToC's undersøgelse viser samtidig, at politikredsene i nogle tilfælde har taget direkte kontakt til teleudbyderen – uden indledende kontakt til telecentret – hvis de har konstateret fejl i rådata.

Telecentret har derudover oplyst, at der i en periode omkring 2014/2015 jævnligt blev gennemført bilaterale møder med teleudbyderne, hvor udvikling, samarbejde og eventuelle fejl blev drøftet. Telecentret har ikke siden afholdt lignende regelmæssige møder med teleudbyderne.

De nuværende årlige bilaterale møder med teleudbyderne omhandler udelukkende ydelser og prissætning i forhold til samarbejds- og ydelsesaftalerne med leverandørerne.

Ud over de bilaterale møder mødes politiet og alle teleudbydere et antal gange årligt. Møderne arrangeres af Teleindustrien. Fokus på møderne har primært været drøftelser om juridiske, tekniske og praktiske forhold, som samarbejdet mellem politiet, anklagemyndigheden og teleudbyderne, har givet anledning til.

8.1.7. Ledelsesmæssig orientering og håndtering af potentielle og identificerede fejl mv.

ToC anfører, at der ved søgninger i referater fra direktionsmøder, koncernledelsesmøder, møder i øverste ledelse og udvidede møder i øverste ledelse i Politiområdet samt referater fra forum for chefpolitiinspektører i politiet ikke er fundet oplysninger, der viser, at potentielle og identificerede fejl i teledata har været forelagt og drøftet på de nævnte møder i undersøgelsesperioden.

Der er dog eksempler på fejl, der i 2012 og 2015 gav anledning til drøftelser og handlinger på øvre ledelsesniveauer om kvaliteten af teledata. I sagen fra 2012 nævnes det bl.a., at manglende data potentielt kan resultere i, at tilliden til anvendelse af kaldsdata i retten kan blive undermineret. Derfor blev der også som opfølgning på den pågældende sag i 2012 afholdt møde mellem bl.a. den daværende politidirektør for Politiområdet og et teleselskab vedrørende uregelmæssigheder og mangler vedrørende telemasters placering, som der efterfølgende blev rettet op på fra teleselskabets side.

ToC har ikke fundet dokumentation for, at fejlen i relation til uoverensstemmelse i antallet af aktiviteter mellem rådata og konverterede data har været ledelsesmæssigt behandlet på

et niveau over telecentrets ledelse før november 2018. Undersøgelsen viser samtidig, at viden om, at der var tale om en systematisk fejl i forbindelse med konverteringen, først bliver kendt i den øverste ledelse i Politiområdet primo 2019.

Dog identificerede telecentret allerede i september 2018 på baggrund af en kredshenvendelse fejl og problemstillinger vedrørende uoverensstemmelse mellem modtaget rådata og konverteret data. Den daværende chef for telecentret var orienteret herom.

8.2. Sammenfatning af enheden for Tilsyn og Controllings observationer

ToC har for perioden januar 2012 til marts 2019 undersøgt telecentrets håndtering og behandling af teledata. Undersøgelsen har haft særligt fokus på proces- og arbejdsgange, kvalitetssikringsaktiviteter og kontroller, opsamling på identificerede fejl samt ledelsesmæssig orientering og håndtering af identificerede fejl. De væsentligste observationer og resultater er på baggrund af undersøgelsen følgende:

Telecentret har understøttet politikredsenes efterforskning med hurtig videreformidling af tilvejebragt teledata til den fortsatte efterforskning. Telecentret har i de sager, hvor politikredsene har indrapporteret problemstillinger i modtagne teledata, søgt at løse problemstillingerne i relation til den enkelte sag hurtigst muligt. Problemstillingerne er ofte løst som et enkeltstående teknisk og driftsmæssigt anliggende.

I undersøgelsesperioden har der ikke været skriftlige interne procedurer, skriftlige vejledninger eller retningslinjer til internt brug i telecentret i relation til håndtering af teledata. Ligeledes er der ikke udarbejdet nationale retningslinjer for kredsenes håndtering og kvalitetssikring af teledata, men Rigsadvokaturen har udarbejdet en vejledning om forberedelse og præsentation af teleoplysninger i retten.

Telecentrets kontroller af teledata har primært sigtet mod at levere data til brugerne i politikredsene hurtigst muligt snarere end at være ind- og uddatakontroller for at kvalitetssikre indholdet af modtaget og behandlet teledata.

I store dele af undersøgelsesperioden har der ikke været en struktureret opsamling, dokumentation og opfølgning på indmeldte fejl. Manglende systematik og dokumentation i den generelle fejlløsning har gjort det vanskeligt for telecentret at kategorisere de enkelte fejl og prioritere den efterfølgende fejlløsning samt at tilrettelægge informationen om fejl.

Tiltag for at informere brugere af teledata i kredsene om bl.a. konstaterede fejl og uhensigtsmæssigheder har fundet sted, men har ikke været tilstrækkeligt fyldestgørende og stringente. Undersøgelsen viser, at politikredsene ikke systematisk og fuldstændigt er blevet orienteret om de mulige fejl og mangler i data, som de bør være opmærksomme på ved brug af teledata.

De nu identificerede fejl viser, at de procedurer, metoder og systemer, der er anvendt i NC3 og politikredsene, samlet set ikke har været egnet til at sikre kvaliteten af teledata.

Der ses tilsyneladende ikke at have været det nødvendige ledelsesmæssige fokus på at sikre medarbejderne tilstrækkelige rammer og muligheder for at løse deres opgaver med den nødvendige kvalitet.

Undersøgelsen viser, at telecentret i september 2018 i samarbejde med NEC identificerede fejl og problemstillinger vedrørende uoverensstemmelser mellem modtaget rådata og konverterede data, der indikerede systematiske fejl i forbindelse med afsendelse af data til politikredsene.

Undersøgelsen tyder ikke på, at fejlen vedrørende uoverensstemmelser i antallet af aktiviteter mellem rådata og konverterede data har været ledelsesmæssigt behandlet uden for telecentret før november 2018. Undersøgelsen viser samtidig, at viden om, at der var tale om en systematisk fejl i forbindelse med konverteringen, først bliver kendt i øverste ledelse i Politiområdet primo 2019.

Undersøgelsen viser, at der løbende har været henvendelser om fejl og mangler ved data, og der er eksempler på henvendelser om fejl i både 2012 og 2015. Eksemplerne viser, at der i undersøgelsesperioden har været både et behov for og konkrete anledninger til ledelsesmæssigt også udenfor telecentret at sætte fokus på området.

Teledata er karakteriseret ved at være data, der er indsamlet til brug for teleudbydernes virksomhed, men som med fordel kan anvendes i politiets og anklagemyndighedens arbejde. Sammenfattende er det ToC's vurdering, at der i undersøgelsesperioden ikke er taget tilstrækkeligt højde for dette ved behandlingen af teledata. Der har således været utilstræk-

kelige processer, arbejdsgange og kvalitetssikringsaktiviteter i telecentret til at sikre kvaliteten i de leverede teledata, ligesom der har været mangelfuld kommunikation til kredsene og videre i straffesagskæden om kendte mangler i indholdet af data. Dette har, sammenholdt med kredsenes uens praksis for kvalitetskontrol af data og et tilsyneladende manglende ledelsesmæssigt fokus på området, medført, at der ikke altid er tilvejebragt den bedst mulige kvalitet af teledata.

Retsudvalget 2019-20
REU Alm.del - Bilag 7
Offentligt

Bilag B

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 1. oktober 2019
Dok.: 1228283

Orientering om udskydelse af ændring af logningsreglerne

1. Ved lov nr. 716 af 8. juni 2018 om ændring af retsplejeloven og visse andre love (ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2018/19.

Af de almindelige bemærkninger til lovforslag nr. L 218, der lå til grund for lovændringen, fremgår det bl.a. at det er afgørende, at udformningen af nye logningsregler sker på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser sker i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet og Politiets Efterretningstjeneste (PET) samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet og terrorisme. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder.

2. Det er afgørende for mig som justitsminister, at politiet og PET har de nødvendige redskaber til at kunne efterforske og retsforfølge alvorlig kriminalitet og terrorisme. Her udgør loggede oplysninger et centralt og effektivt redskab.

EU-Domstolen behandler i øjeblikket to sager fra henholdsvis Belgien og Frankrig, der kan give EU-Domstolen anledning til at genoverveje den retstilstand, som Tele2-dommen har medført.

De pågældende sager blev mundtligt forhandlet ved EU-Domstolen den 9.-10. september 2019, hvor en lang række medlemsstater, inklusiv Danmark, afgav indlæg med henblik på, at EU-Domstolen trækker nogle af indskrænk-

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

ningerne fra Tele2-dommen tilbage. EU-Domstolens afgørelse i sagerne fra Belgien og Frankrig forventes at blive afsagt omkring maj 2020.

Med henblik på at afvente EU-Domstolens kommende dom, hvor Domstolen forhåbentlig genovervejer den retstilstand, som Tele2-dommen har medført, vil jeg i december II fremsætte et lovforslag om udskydelse af revision af logningsreglerne til folketingsåret 2020-21.

3. Jeg skal for god ordens skyld oplyse, at de gældende logningsregler i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen fortsat opretholdes, indtil revisionen af logningsreglerne er gennemført.

Nick Hækkerup

/

Lene Steen

FOLKETINGET

Folketingstidende
Tillæg A

Bilag AQ
Kammeradvokaten

Lovforslag nr. **L 87** Folketinget 2019-20

Fremsat den 18. december 2019 af justitsministeren (Nick Hækkerup)

Forslag

til

Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige

(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016, lov nr. 673 af 8. juni 2017 og lov nr. 716 af 8. juni 2018, foretages følgende ændring:

1. I *§ 8* ændres »2018-19« til: »2020-21«.

§ 2

Loven træder i kraft den 1. april 2020.

Justitsmin., j.nr. 2019-187-0032

Bemærkninger til lovforslaget

Almindelige bemærkninger

1. Indledning

Den daværende justitsminister fremsatte den 24. april 2019 et lovforslag om udskydelse af revision af retsplejelovens § 786, stk. 4, der fastsætter en pligt for teleudbyderne til at registrere og opbevare (logge) oplysninger om tele- og internettrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven mv., som senest ændret ved lov nr. 716 af 8. juni 2018. Lovforslaget bortfaldt som følge af udskrivelsen af folketingsvalg den 7. maj 2019.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler. Logningsreglerne indebærer overordnet set, at en række oplysninger om tele- og internetkommunikation skal registreres og opbevares hos teleudbyderne, således at politiet, herunder Politiets Efterretningstjeneste (PET), til brug for efterforskning og retsforfølgning af strafbare forhold kan indhente nærmere specificerede oplysninger, som de har brug for i konkrete sager. Det er en betingelse for politiets indhentelse af oplysninger, at oplysningerne i hvert enkelt tilfælde indhentes i overensstemmelse med retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden og edition. Det forudsætter som udgangspunkt, at rettens kendelse opnås forud for indhentelsen. De almindelige regler i retsplejeloven om tvangsindgreb gælder også for PET, jf. PET-lovens § 6.

Ved lov nr. 716 af 8. juni 2018 om ændring af retsplejeloven og visse andre love (Ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2018-19.

Baggrunden for udskydelsen var, at det efter Justitsministeriets opfattelse var afgørende, at udformningen af nye logningsregler skete på et fuldt oplyst grundlag, og at udlægningen af EU-Domstolens dom af 21. december 2016 (Tele2-dommen) skete i fællesskab med de øvrige EU-lande og EU-Kommissionen. Justitsministeriet afventede derfor, at Kommissionen færdiggjorde arbejdet med fælles retningslinjer for, hvordan medlemsstaterne kan fastsætte nationale logningsregler i lyset af Tele2-dommen. Kommissionen havde ved fremsættelsen af forslaget til lov nr. 716 af 8. juni 2018 senest tilkendegivet, at retningslinjerne ville foreligge i løbet af 2018.

Kommissionen har endnu ikke udstedt retningslinjerne.

Der verserer for tiden et antal sager for EU-Domstolen, som kan få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler.

Danmark og 16 andre EU/EØS-medlemsstater afgav mundtligt indlæg i EU-Domstolens forenede sager nr. C-511/18 og C-512/18 samt C-520/18 i forbindelse med domsforhandlingen den 9.-10. september 2019. Der henvises til notat af 29. november 2018 om afgivelse af indlæg i sagerne. Notatet er sendt til Folketingets Retsudvalg (Alm. del – bilag 171). I overensstemmelse med notatet gjorde regeringen under sagerne gældende, at Domstolen bør genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen.

Det forventes, at EU-Domstolen vil afsige domme i sagerne omkring maj 2020.

Det er Justitsministeriets vurdering, at udformningen af de nye logningsregler bør ske på et fuldt oplyst grundlag, og at rækkevidden af Tele2-dommen skal fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder. Justitsministeriet følger derfor udviklingen i de øvrige medlemsstater tæt.

Som følge heraf og i lyset af, at EU-Domstolens kommende domme i de ovenfor omtalte logningssager vil kunne give svar på, hvordan logningsregler kan indrettes, foreslås det at udskyde revisionen af logningsreglerne til folketingsåret 2020-21.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og energi-, forsynings- og klimaministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke om selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at rettens kendelse opnås forud for udleveringen.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til L 217 som fremsat, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2009-10, A, L 180 som fremsat, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret 2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2011-12, A, L 53 som fremsat, side 4, og Retsudvalgets betænkning af 31. maj 2012, B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2012-2013, A, L 142 som fremsat, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L 142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2014-15 (1. samling), A, L 193 som fremsat, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om

nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17. Baggrunden herfor var, at et eksternt konsulentfirma havde foretaget beregninger vedrørende en række anbefalinger, som Rigspolitiet var fremkommet med til brug for revisionen, som pegede på, at omstillingsomkostninger for udbyderne ved at følge anbefalingerne var i omegnen af en milliard kr. Det oversteg efter Justitsministeriets opfattelse grænsen for det acceptable. Samtidig havde Justitsministeriet indledt en dialog med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen, og ministeriet fandt det hensigtsmæssigt at fortsætte denne dialog, før revisionen blev foretaget. Der henvises til lovens forarbejder (pkt. 2.2 i de almindelige bemærkninger, jf. Folketingstidende 2015-16, A, L 183 som fremsat, side 4).

Ved lov nr. 673 af 8. juni 2017 blev revisionen udskudt til folketingsåret 2017-18. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2016-17, A, L 191 som fremsat, side 6-7) navnlig, at Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.3 nedenfor, at et centralt element i den udredning var en dialog med de andre EU-lande, og at EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen.

Ved lov nr. 716 af 8. juni 2018 blev revisionen udskudt til folketingsåret 2018-19. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2017-18, A, L 218 som fremsat, side 5-6), at det efter Justitsministeriets opfattelse var afgørende, at udformningen af nye logningsregler skete på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser skete i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces var vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet, herunder PET, samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Endvidere ville en fælles tilgang i EU efter Justitsministeriets opfattelse være med til at sikre, at telebranchen ikke pålagdes unødige byrder.

Justitsministeren fremsatte den 24. april 2019 et lovforslag om udskydelse af revision af logningsreglerne til folketingsåret 2019-20. Lovforslaget bortfaldt som følge af udskrivelsen af folketingsvalg den 7. maj 2019.

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i § 2, nr. 1, i lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer om elektroniske kommunikationsnet og -tjenester (teleloven). Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommuni-

keret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.4. EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl. (om de britiske og svenske logningsregler)

I EU-Domstolens dom af 21. december 2016 i Tele2-sagen udtalte Domstolen bl.a., at artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet), sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i EU's charter om grundlæggende rettigheder (Chartret), skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation (præmis 112).

EU-Domstolen udtalte i den forbindelse, at en sådan national lovgivning, der navnlig ikke er begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, derfor overskrider det strengt nødvendige og ikke kan anses for at være begrundet i et demokratisk samfund, således som det er påkrævet i henhold til artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7 (ret til respekt for privatliv og familieliv), 8 (ret til beskyttelse af personoplysninger) og 11 (ret til ytrings- og informationsfrihed) (præmis 106 og 107).

Endvidere udtalte EU-Domstolen, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafikdata og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen (præmis 108).

EU-Domstolen udtalte, at en sådan national lovgivning for det første skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige (præmis 109).

Endvidere udtalte EU-Domstolen, at en national lovgivning, der med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet gør det muligt i forebyggende øjemed at lagre trafikdata og lokaliseringsdata, skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds (præmis 110).

For så vidt angår afgrænsningen af en sådan foranstaltning udtalte EU-Domstolen, at den nationale lovgivning skal være baseret på objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan endvidere sikres gennem et geografisk kriterium, når de kompetente nationa-

le myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået (præmis 111).

3. Justitsministeriets overvejelser og den foreslåede ordning

Ved lov nr. 716 af 8. juni 2018 om ændring af retsplejeloven og visse andre lov (Ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til folketingsåret 2018-19.

Baggrunden for udskydelsen var, at det efter Justitsministeriets opfattelse var afgørende, at udformningen af nye logningsregler skete på et fuldt oplyst grundlag, og at udlægningen af EU-Domstolens dom af 21. december 2016 (Tele2-dommen) skete i fællesskab med de øvrige EU-lande og EU-Kommissionen. Justitsministeriet afventede derfor, at Kommissionen færdiggjorde arbejdet med fælles retningslinjer for, hvordan medlemsstaterne kan fastsætte nationale logningsregler i lyset af Tele2-dommen. Kommissionen havde ved fremsættelsen af forslaget til lov nr. 716 af 8. juni 2018 senest tilkendegivet, at retningslinjerne ville foreligge i løbet af 2018.

Kommissionen har endnu ikke udstedt retningslinjerne.

Der verserer for tiden sager for EU-Domstolen, som kan få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler.

Danmark og 16 andre EU/EØS-medlemsstater afgav mundtligt indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18 samt C-520/18 i forbindelse med domsforhandlingen den 9.-10. september 2019. Der henvises til notat af den 29. november 2018 om afgivelse af indlæg i sagerne. Notatet er sendt til Retsudvalget (Alm. del – bilag 171). I overensstemmelse med notatet gjorde regeringen under sagerne gældende, at Domstolen bør genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen.

Det forventes, at EU-Domstolen vil afsige domme i sagerne omkring maj 2020.

Det er Justitsministeriet vurdering, at udformningen af de nye logningsregler bør ske på et fuldt oplyst grundlag, og at rækkevidden af Tele2-dommen skal fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces er vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen ikke pålægges unødige byrder. Justitsministeriet følger derfor udviklingen i de øvrige medlemsstater tæt.

Som følge heraf og i lyset af, at EU-Domstolens kommende domme i de ovenfor omtalte logningssager vil kunne give svar på, hvordan logningsregler kan indrettes, finder Justitsministeriet det derfor rigtigst at afvente EU-Domstolens domme, inden der tages stilling til den fremtidige indretning af de danske logningsregler.

Revisionen af logningsreglerne bør derfor efter Justitsministeriets opfattelse udskydes til folketingsåret 2020-21.

Der henvises til lovforslagets § 1, nr. 1.

Det bemærkes i den forbindelse, at efter EU-Domstolens praksis skal medlemsstaterne så hurtigt som muligt iværksætte foranstaltninger til opfyldelse af en dom. Hvor hurtigt det skal ske, afhænger af sagens konkrete omstændigheder.

Spørgsmålet om, hvordan logningsregler, der lever op til Tele2-dommen, kan indrettes, er kompliceret, og rækkevidden af dommen bør som nævnt ovenfor fastlægges i fællesskab med de øvrige EU-lande og Kommissionen. Der har således også siden foråret 2017 været løbende drøftelser i EU-regi om, hvordan medlemsstaterne kan indrette deres regler, så de er i overensstemmelse med dommen. Som følge heraf og i lyset af, at EU-Domstolens kommende domme i logningssagerne, der vil kunne give svar på, hvordan logningsreglerne kan indrettes, forventes omkring maj 2020, vurderer Justitsministeriet, at det vil være muligt at udskyde et lovforslag om revision af logningsreglerne.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget har ingen økonomiske konsekvenser eller implementeringskonsekvenser for stat, kommuner og regioner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget har ikke i sig selv EU-retlige aspekter. Det bemærkes dog, at det forventes, at der i lyset af EU-Domstolens dom i Tele2-sagen vil skulle foretages nogle tilpasninger af de danske logningsregler, jf. nærmere herom pkt. 2.4 og pkt. 3.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 8. november 2019 – 6. december 2019 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten ¸ Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Dansk Journalistforbund, Justitia, Rådet for Digital Sikkerhed, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, DI Digital, PROSA, SAMDATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget har ikke i sig selv EU-retlige aspekter. Der henvises til pkt. 8.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering/Overimplementering af EU-retlige minimumsforpligtelser	JA	NEJ X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 716 af 8. juni 2018, skal justitsministeren i folketingsåret 2018-19 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2020-21.

Der henvises til pkt. 3 i de almindelige bemærkninger i lovforslaget.

Til § 2

Det foreslås, at loven træder i kraft den 1. april 2020.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006 og senest ved lov nr. 716 af 8. juni 2018, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2018-19 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2018-19« til: »2020-21«.

EKSTRAKT – BIND III – BILAG

I sagen for

Østre Landsret, 16. afdeling

BS-36799/2018-OLR

Foreningen imod Ulovlig Logning
Birkegade 15, 5. tv.
2200 København N
advokat Julie Bak-Larsen i henhold til proceduretilladelse
(”Sagsøger”)

mod

Justitsminister Nick Hækkerup
Justitsministeriet
Slotholmsgade 10
1216 København K
advokat Rass Holdgaard
("Sagsøgte")

Sagen hovedforhandles den 5. maj 2021, kl. 9.30-15, og den 6. maj 2021, kl. 9.30-12.

INDHOLDSFORTEGNELSE

Europaudvalget 2019-20
EUU Alm.del - Bilag 409
Offentligt

Bilag C

Kammeradvokaten

JUSTITSMINISTERIET

Dato: 14. februar 2020
Kontor: Politikontoret
Sagsbeh: Rune Bæk Krogh
Sagsnr.: 2020-614-1243
Dok.: 1380873

Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i EU-Domstolens forenede sager C-793/19 og C-794/19, SpaceNet m.fl.

1. Indledning

Bundesverwaltungsgericht (forbundsforvaltningsdomstolen) i Tyskland har i to sager vedrørende den tyske lov om telekommunikation forelagt EU-Domstolen præjudicielle spørgsmål om de EU-retlige rammer for nationale bestemmelser, der forpligter udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester til at lagre størstedelen af relevant trafik- og lokaliseringsdata.

Spørgsmålene angår endnu en gang fortolkningen af artikel 15 i direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor samt artikel 7, 8, 11 og 52 i Den Europæiske Unions charter om grundlæggende rettigheder (Charteret). Der skal således tages stilling til, om de nævnte EU-bestemmelser er til hinder for en national lovgivning, der fastsætter en generel forpligtelse for teleudbydere til at lagre størstedelen af relevant trafik- og lokaliseringsdata for en periode på henholdsvis fire uger for lokaliseringsdata og ti uger for trafikdata, når lovgivningen har til formål bl.a. at sikre den personlige og nationale sikkerhed, og reglerne indeholder en effektiv beskyttelse af de lagrede data mod risici for misbrug samt mod enhver uberettiget adgang.

2. Sagernes faktiske omstændigheder

Sagsøgeren, SpaceNet AG, har i sag C-793/19 gjort gældende for den tyske forbundsdomstol, at den tyske lovgivning, der pålægger udbydere af offentligt tilgængelige elektroniske kommunikationstjenester at lagre størstedelen af relevant telekommunikationstrafikdata, er i strid med EU-retten.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

I sag C-794/19, som omhandler Telekom Deutschland GmbH, svarer de faktiske omstændigheder og begrundelsen for forelæggelsen i det væsentlige til sag C-793/19, og de præjudicielle spørgsmål er identiske.

Forbundsforvaltningsdomstolen konstaterede i forelæggelseskendelserne, at der er behov for, at EU-Domstolen præciserer, hvordan dommen i Tele2-sagen (sag C-203/15 og C-698/15) skal forstås. I dommen fastslog EU-Domstolen, at de svenske regler om logning – som i det væsentlige var sammenlignelig med de danske – var i strid med direktiv 2002/58, sammenholdt med de grundlæggende rettigheder i EU-chartret. EU-retten var således til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en pligt til generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

Sagsøgte, Tyskland, har heroverfor gjort gældende, at de tyske regler – uanset resultatet i Tele2-dommen – er i overensstemmelse med EU-retten.

Forbundsforvaltningsdomstolen anser det ikke for udelukket, at de tyske regler er i overensstemmelse med EU-retten. I den forbindelse har domstolen påpeget, at de tyske regler på området ikke foreskriver lagring af samtlige telekommunikationstrafikdata for alle abonnenter og registrerede brugere, idet eksempelvis kommunikationsindhold, besøgte hjemmesider, data fra e-mailtjenester og data, som er baseret på forbindelser til eller fra bestemte personer, som i henhold til tysk lovgivning er pålagt tavshedspligt, herunder advokater, læger eller journalister, er undtaget fra kravet om logning. Endvidere påpeger domstolen, at lagringsperioden under den tyske lovgivning på henholdsvis fire og ti uger er væsentlig kortere end i Tele2-sagen, hvor lagringsperiode var på seks måneder efter de svenske regler. Domstolen anfører ligeledes, at de tyske regler, som fastsætter pligt til generel lagring af trafikdata, ikke uden videre kan anses for uforenelig med Charteret henset til behovet for at etablere en balance mellem på den ene side medlemsstatens forpligtelse til at sikre den personlige og nationale sikkerhed og på den anden side overholdelsen af de grundlæggende rettigheder.

3. Den danske interesse i sagen

Det er regeringens opfattelse, at regeringen bør afgive indlæg i disse sager, idet sagerne vedrører EU-medlemsstaternes muligheder for at pålægge tele-

udbydere at gemme og opbevare oplysninger om tele- og internettrafik (logning) til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

De danske regler om logning skal som konsekvens af EU-Domstolens afgørelse i Tele2-sagen revideres.

Tele2-dommen efterlader imidlertid væsentlig fortolkningstvivl i forhold til, hvordan nationale bestemmelser om logning kan indrettes i overensstemmelse med EU-retten. Der har således siden foråret 2017 løbende været drøftelser i EU-regi om, hvordan medlemsstaterne kan indrette nationale logningsregler i lyset af dommen. Kommissionen tilkendegav, som følge af Tele2-dommen, at Kommissionen ville udarbejde retningslinjer til medlemsstaterne om indretning af logningsregler. Disse retningslinjer er endnu ikke udarbejdet.

Der verserer for tiden en række præjudicielle sager fra andre EU-medlemsstater for EU-Domstolen, som kan få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler.

Danmark og 16 andre EU/EØS-medlemsstater har afgivet indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18 om de franske logningsregler samt i sag C-520/18 om de belgiske logningsregler. I begge sager gjorde regeringen gældende, at Domstolen bør genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen.

Det forventes, at EU-Domstolen vil afsige domme i sagerne i løbet af sommerhalvåret 2020.

Derudover afgav regeringen den 15. oktober 2019 mundtligt indlæg i en præjudiciel sag vedrørende de estiske logningsregler (sag C-746/18, H.K.). På samme måde som i den franske og den belgiske sag blev der også i denne sag fra visse medlemsstater argumenteret for, at EU-Domstolen bør genoverveje retstilstanden, som Tele2-dommen har medført. Det bemærkes, at dommen i denne sag navnlig vil kunne få betydning for, hvordan retsplejelovens regler om adgang til oplysninger, som teleselskaberne skal opbevare til brug for efterforskning og retsforfølgning af strafbare forhold i medfør af logningsbekendtgørelsen, kan udformes.

De forelagte spørgsmål fra den tyske forbundsforvaltningsdomstol adresserer som nævnt også spørgsmål om fortolkningen af EU-Domstolens dom i

Tele2-sagen. Domstolens besvarelse af de forelagte præjudicielle spørgsmål må derfor antages at få stor betydning for vurderingen af, hvorledes de danske logningsregler kan indrettes i overensstemmelse med EU-retten og på en måde, hvor logning fortsat vil udgøre et effektivt efterforskningsredskab for politiet og politiets efterretningstjeneste.

Regeringens synspunkter i sagen

Det er overordnet regeringens opfattelse, at EU-Domstolen skal opfordres til at genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen. Der skal i den forbindelse henvises til, at loggede oplysninger udgør et centralt og effektivt redskab for politiet og politiets efterretningstjeneste, som i forhold til efterforskning og strafforfølgning af alvorlig kriminalitet og terror er af afgørende betydning.

Der skal efter regeringens opfattelse ligeledes argumenteres for, at EU-retten ikke er til hinder for en generel og udifferentieret logningsforpligtelse, hvis formål bl.a. er at sikre den personlige og nationale sikkerhed, som staten har en positiv forpligtelse til at sikre for alle borgere.

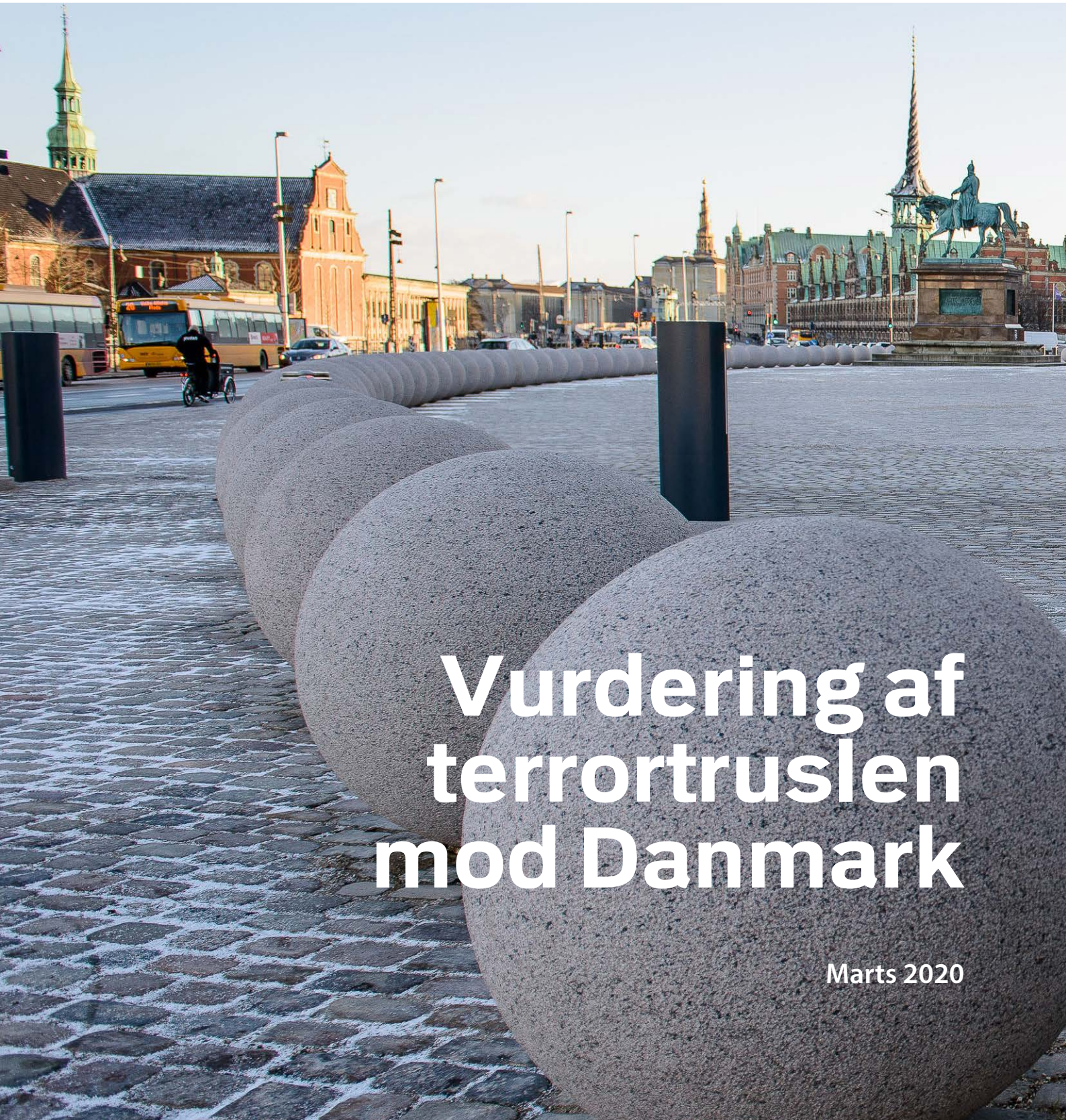
Det er i den sammenhæng afgørende, at der sikres en balance mellem på den ene side retshåndhævende myndigheders mulighed for at anvende centralt og effektivt redskaber til brug for efterforskning og strafforfølgning og på den anden side overholdelse af de grundlæggende rettigheder i Charteret.

PET

Center for Terroranalyse CTA

Bilag AD

Kammeradvokaten



Vurdering af terrortruslen mod Danmark

Marts 2020

Forord

Vurderingen af terrortruslen mod Danmark (VTD) udgør Center for Terroranalyses (CTA's) samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet.

Vurderingen bygger på et stort antal underliggende CTA-analyser, som for størstedelens vedkommende er klassificerede, og som strækker sig fra vurderinger af truslen mod konkrete personer, lokaliteter og begivenheder til bredere tendensanalyser og vurderinger af fænomener med betydning for terrortruslen mod Danmark og danske interesser i udlandet.

Vurderingen beskriver primært terrortruslen fra militant islamisme samt i mindre grad fra højre- og venstreekstremisme. Der peges dog også på en række andre trusler, der kan have betydning for den samlede vurdering af terrortruslen. Der er endvidere et separat afsnit om terrortruslen mod Grønland og Færøerne.

Nærværende vurdering er baseret på efterretninger, der er blevet behandlet før 1. marts 2020.

CTA er et fusionscenter, hvis medarbejdere stammer fra fem danske myndigheder (Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste, Udenrigsministeriet, Beredskabsstyrelsen og Rigspolitiets Nationale Efterforskningscenter).

Foto: *Scanpix*

INDHOLD

Forsidefoto: *Christiansborg Slotsplads, terrorsikring, Slots- og Kulturstyrelsen.*

UDVALGTE CENTRALE BEGREBER I VURDERING AF TERRORTRUSLEN MOD DANMARK

Begreber

Fremmedkriger: En privatperson, der er udrejst eller vendt tilbage fra et konfliktområde (Syrien/Irak, Libyen, Afghanistan, Yemen m.fl.), og hvis formål var at deltage i konflikten.

Hensigt: Vilje/intention om at bringe en given kapacitet i spil over for et givent mål eller en given målgruppe.

Kapacitet: Udtryk for de tilgængelige midler (personel, teknik, materiel osv.), holdt op imod evnen (uddannelse, færdigheder, logistik osv.) til at udnytte disse midler maksimalt i et muligt angreb.

Islamisme: Politisk ideologi med vision om et samfund baseret på islamiske værdier. En islamist er en person, der bekender sig til denne ideologi.

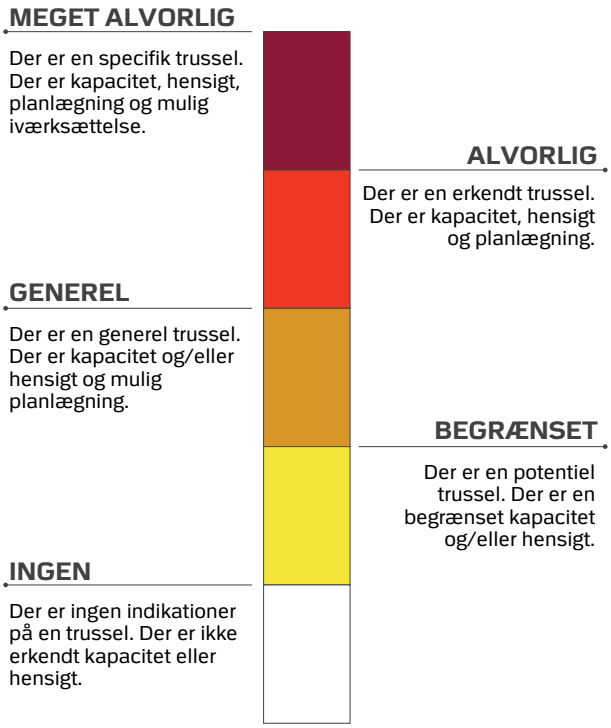
Militant islamisme: Fortolkning af islamistisk ideologi, der legitimerer anvendelse af vold for at opnå politiske, religiøse eller ideologiske mål.

Ekstremisme: Vilje til at anvende vold eller andre ulovlige handlinger for at ændre eksisterende samfundsforhold.

Radikalisering: Dynamisk proces, hvor en person i stigende grad accepterer anvendelse af vold til at opnå politiske, religiøse eller ideologiske mål.

Soloterrorist: En person, der angriber på egen hånd. Personen kan have haft kontakt til andre militante personer eller grupper.

Terrortrusselsniveauer



Typer af angreb

Inspireret: Gerningsmanden er inspireret af militant islamisme eller politisk ekstremisme og planlægger angreb på egen hånd.

Understøttet: Gerningsmanden er i kontakt med én eller flere personer, der opildner, vejleder eller på anden vis støtter angrebsplaner.

Dirigeret: Et angreb sanktioneres og/eller planlægges tæt på en terrorgruppes ledelse.

1. OVERORDNET VURDERING AF TERRORTRUSLEN MOD DANMARK

CTA vurderer, at terrortruslen mod Danmark fortsat er alvorlig. Det betyder i henhold til PET's definitioner, at der er en erkendt trussel, kapacitet, hensigt og planlægning[1].

Militante islamister udgør fortsat den væsentligste terrortrussel mod Danmark, og denne trussel er alvorlig (se afsnit 2). Truslen udgår først og fremmest fra sympatisører af gruppen, der kalder sig Islamisk Stat (IS). Det drejer sig primært om personer med tilknytning til visse islamistiske miljøer i Danmark, hvor der foregår aktiviteter, der kan have en radikaliserende indvirkning på de deltagende personer, og som kan føre til, at enkelte personer eller mindre grupper kan begå terrorhandlinger. Der kan også udgå en terrortrussel fra personer eller mindre grupper uden for miljøerne, som på anden vis har gennemgået et radikaliseringsforløb, eksempelvis via forskellige online-aktiviteter. Der kan endvidere udgå en terrortrussel fra personer, der er eller har været udrejst til konfliktzonen i Syrien/Irak, og fra radikaliserede indsatte i fængsler, når de løslades. Truslen udgår både fra personer i Danmark og personer fra andre lande, herunder Danmarks nabolande.

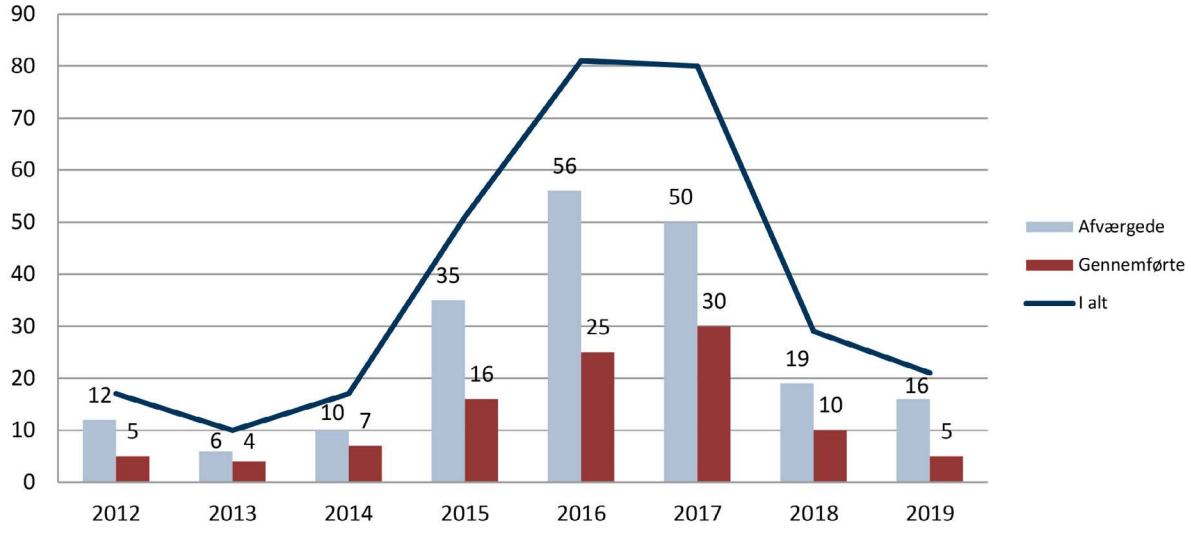
CTA vurderer imidlertid, at udviklingen i det globale trusselsbillede betyder, at terrortruslen mod Danmark fra IS er reduceret. Krigen i Syrien er gået ind i sit niende år, og IS har ikke opgivet sin kamp for at etablere et "kalifat". IS' tab af territorium i Syrien/Irak betyder dog, at gruppens evne til at gennemføre komplekse, dirigerede terrorangreb i Vesten, herunder i Danmark, i et stykke tid har været reduceret. Også IS' officielle propagandamaskine er svækket, og både kvantiteten og kvaliteten af propagandaen er faldet markant.

Al-Qaida har fortsat ambitioner om at ramme mål i Vesten, men organisationen råder ikke over de samme kapaciteter som tidligere.

Udviklingen i det globale trusselsbillede afspejler sig i CTA's angrebsstatistik for Vesten. Som figur 1 viser, har der siden efteråret 2017 været et markant fald i antallet af militant islamistiske terrorangreb i Vesten[2]. Der var i 2018 i gennemsnit 2,4 afværgede eller gennemførte terrorangreb pr. måned mod 6,7 pr. måned i 2017. Den faldende tendens fortsatte i 2019, hvor der i gennemsnit var 1,8 afværgede eller gennemførte angreb i Vesten pr. måned. Antallet af afværgede og gennemførte angreb nærmer sig nu niveauet for årene inden, at IS etablerede "kalifatet" i Syrien/Irak.

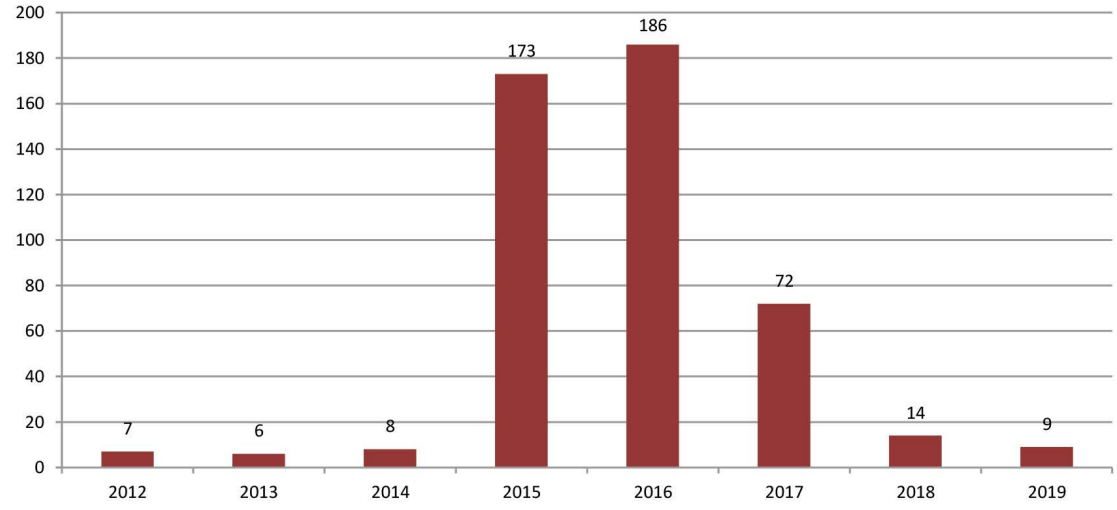
"CTA vurderer imidlertid, at udviklingen i det globale trusselsbillede betyder, at terrortruslen mod Danmark fra IS er reduceret."

1. Truslen mod Danmark kan fastholdes i "alvorlig" uden igangværende planlægning, da Danmark tidligere har været genstand for angrebsplanlægning, angrebsforsøg eller gennemførte angreb.
2. Det skal bemærkes, at opgørelser over antallet af afværgede og gennemførte terrorangreb kan variere afhængig af opgørelsesmetode og tilgængelige oplysninger.



Figur 1: Antal afværgede og gennemførte angreb i Vesten fra 2012 til 2019.

Figur 2 viser, at antallet af dødsofre for terrorangreb i Vesten også er faldet markant siden 2017 og nærmer sig niveauet inden IS' "kalifat". Det hænger bl.a. sammen med, at alle terrorangreb i 2018 og 2019 blev udført af soloterrorister, der var inspirerede – men ikke dirigerede eller understøttede – af militant islamistiske grupper, herunder IS.



Figur 2: Antal dræbte ved angreb i Vesten fra 2012 til 2019.

De fleste af de omkring 5.000 fremmedkrigere fra Europa, der siden 2012 tilsluttede sig IS eller andre militant islamistiske grupper i Syrien og Irak, er siden vendt tilbage til de lande, de udrejste fra, er omkommet eller taget til fange. De tilfangetagne udrejste er fortrinsvist tilbageholdt i lejre og fængsler i det nordøstlige Syrien. Det gælder bl.a. ca. halvdelen af de tilbageværende voksne udrejste fra Danmark med dansk statsborgerskab.

Trods den generelle forbedring i det globale trusselsbillede og den reducerede terrortrussel mod Danmark fra IS vurderer CTA imidlertid fortsat, at der er personer i Danmark og i udlandet, herunder i Danmarks nabolande, der har sympati for militant islamisme, og som kan udgøre en terrortrussel mod Danmark. Det illustreres bl.a. af den koordinerede anholdelsesaktion, som PET i samarbejde med relevante politikredse gennemførte den 11. december 2019, og som førte til varetægtsfængsling af syv personer for mistanke om overtrædelse af straffelovens § 114.

Der er herudover fortsat visse usikkerheder, som har en væsentlig betydning for vurderingen af terrortruslen mod Danmark. Det drejer sig primært om IS' strategiske hensigt efter gruppens tab af territorium i Syrien/Irak, herunder særligt gruppens hensigt om og kapacitet til at gennemføre dirigerede angreb i Vesten, eventuelt forankret i gruppens underafdelinger/"eksterne provinser". Hertil kommer en usikkerhed om, hvilken betydning opfattede krænkelser af islam har for terrortruslen i Danmark.

Militante islamister anser islam for at være under angreb fra Vesten, og Danmarks aktive deltagelse i militære operationer i bl.a. Mellemøsten og Afghanistan, herunder det danske bidrag til den militære operation mod IS i Syrien/Irak, gør, at militante islamister fortsat anser Danmark for at være et legitimt mål. Danmark har endvidere siden "Tegningesagen" haft et ry for at krænke islam, og selvom det er sjældent, at Danmark fremhæves konkret i den militant islamiske propaganda, kan Danmarks omdømme som "krænkernation" atter blusse op, hvis forhold eller handlinger i Danmark eller i udlandet, der opfattes som krænkende over for islam, spredes nationalt og/eller internationalt.

Truslen fra militante islamister er i de senere år blevet mere fragmenteret. Det er fortsat CTA's vurdering, at det mest sandsynlige militant islamistiske terrorangreb i Danmark er et angreb, der udføres efter kort planlægning af en soloterrorist eller en mindre gruppe, der er inspireret af militant islamistisk propaganda. Angreb, der gennemføres af en person uden forudgående kontakt med andre militante islamister eller militant islamistiske grupper, kan være vanskelige at afdække og afværge. Det gælder især, hvis angrebet gennemføres spontant.

De mest sandsynlige mål for et militant islamistisk terrorangreb i Danmark er et ubeskyttet civilt mål, såsom et offentligt befærdet sted eller et arrangement, hvor mange mennesker er samlet, eller "symbolmål", i første række personer, institutioner og begivenheder, der kan opfattes som islamkrænkende. Andre mulige mål er jødiske mål, politi og militær – særligt i forbindelse med bevogtningsopgaver – visse offentlige myndigheder samt udvalgte politikere. Militante islamister har fortsat fokus på at ramme transportinfrastrukturen, særligt international flytrafik. Den mest sandsynlige fremgangsmåde ved et militant islamistisk terrorangreb i Danmark er anvendelsen af lettilgængelige midler, hvorved hovedsageligt forstås knive,

slagvåben, ildspåsættelser eller køretøjer. Angreb med brug af skydevåben eller hjemmelavede bomber er også mulige.

Der er en terrortrussel fra militante islamister mod danske interesser i udlandet, først og fremmest i lande og regioner, hvor al-Qaida (AQ) og IS har underafdelinger, hvor de kan træne og planlægge angreb. I de seneste par år har militante islamistiske netværk uden direkte forbindelse til IS eller AQ imidlertid også andre steder udført angreb mod vestlige interesser i lande uden for Europa.

Terrortruslen mod danske interesser i udlandet retter sig både mod beskyttede mål, såsom diplomatiske repræsentationer, og mindre beskyttede mål, såsom virksomheder, NGO'er og turister. Truslen adskiller sig som udgangspunkt ikke fra truslen mod andre vestlige landes interesser, og som andre vesterlændinge kan danskere risikere at blive ofre for angreb, der målrettes vestlige eller lokale interesser. Det viser bl.a. drabet på en dansk turist i december 2018 i Marokko og angrebet i april 2019 i Sri Lanka, hvor tre danskere mistede livet. Danmark har imidlertid som nævnt fortsat et ry i militant islamistiske kredse for at krænke islam, og dette ry kan hurtigt blive bragt op internationalt, hvorved terrortruslen mod danske interesser i udlandet kan ændre sig i negativ retning. Danske diplomatiske repræsentationer og anden dansk tilstedeværelse i udlandet, herunder ansatte i danske virksomheder, vil i så fald kunne blive opfattet som symbolske mål, der giver mulighed for at ramme Danmark uden at foretage angreb i Danmark.

Der udgår også en terrortrussel fra henholdsvis højre- og venstreekstremister i Danmark.

Terrortruslen fra højreekstremister er efter CTA's vurdering øget og nu af en sådan karakter, at CTA hæver trusselsniveauet fra niveauet begrænset til niveauet generel (se afsnit 3). Det betyder i henhold til PET's definitioner, at der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.

Der har siden foråret 2019 været en række højreekstremistiske terrorangreb i Vesten udført af soloaktører, hvis radikaliseringsproces primært er foregået på online-fora. Blandt disse angreb var et omfattende angreb i marts 2019 i Christchurch, New Zealand, der bidrog til at inspirere til efterfølgende højreekstremistiske angreb udført af soloaktører i bl.a. USA, Norge og Tyskland. Det seneste angreb fandt sted den 19. februar 2020, hvor en person med højreekstremistiske sympatier dræbte ni personer på to lokaliteter i Hanau, Tyskland. De mange angreb viser bl.a., at virtuelle platforme og medier på internettet i stort omfang anvendes til at sprede højreekstremistisk propaganda og til radikalisering. Den internationale udvikling påvirker efter CTA's vurdering truslen fra højreekstremister i Danmark, og det er CTA's vurdering, at angrebene kan påvirke enkelte danske højreekstremister til at begå angreb i Danmark. Det er også CTA's vurdering, at danske højreekstremister i disse år etablerer flere kontakter til ligesindede i udlandet.

"Den internationale udvikling påvirker efter CTA's vurdering truslen fra højreekstremister i Danmark, og det er CTA's vurdering, at angrebene kan påvirke enkelte danske højreekstremister til at begå angreb i Danmark."

Det mest sandsynlige højreekstremistiske terrorangreb i Danmark er et angreb, der udføres af en soloterrorist eller en lille gruppe, der befinder sig i periferien af eller uden for et højreekstremistisk miljø. Det mest sandsynlige våben, der vil blive anvendt ved et højreekstremistisk terrorangreb i Danmark, er blank- eller stikvåben eller lette skydevåben, herunder særligt jagtrifler, haglgeværer og pistoler. Andre mulige våben inkluderer ildspåsættelse, hjemmelavede bomber og køretøjer.

Terrortruslen fra venstreekstremister er begrænset (se afsnit 4). Det betyder i henhold til PET's definitioner, at der er en potentiel trussel, men begrænset kapacitet og/eller hensigt. Truslen fra venstreekstremister har efter CTA's vurdering ikke udviklet sig nævneværdigt i de seneste år.

Der er herudover en række andre forhold, der kan have betydning for terrortruslen i Danmark (se afsnit 5). Politiske, etniske og religiøse konflikter i udlandet kan eksempelvis føre til konfrontation mellem personer eller grupper med tilknytning til de berørte grupper i Danmark. Dette kan udvikle sig til handlinger, der har karakter af terror. Herudover kan truende ytringer på bl.a. sociale medier påvirke visse psykisk uligevægtige eller meget påvirkelige personer til at begå ideologisk motiveret vold, der kan have karakter af terror.

PET iværksætter løbende operationer med henblik på at afdække og afværge mulige terrortrusler mod mål i Danmark, men terrorangreb kan finde sted uden forudgående efterretningsmæssige indikationer, også selvom gerningsmændene tidligere har været kendt for at nære sympati for militant islamisme eller politisk ekstremisme. En særlig bekymring knytter sig i den forbindelse til personer, der har gennemgået relativt kortvarige radikaliseringsforløb, og til personer, der ekskluderes fra eller afvises af miljøer, eksempelvis på grund af deres ekstreme opførsel eller holdninger.

2. TERRORTRUSLEN FRA MILITANT ISLAMISME

2.1. Udviklingen i det globale trusselsbillede[3]

Trods tabet af sin leder, Abu Bakr al-Baghdadi, udgør IS stadig en reel trussel mod Vesten, om end den er reduceret. IS forsøger fortsat aktivt at understøtte sympatisørers angrebsplanlægning, ligesom gruppens propaganda stadig opfordrer personer i Vesten til at begå terror. IS, relaterede grupper og sympatisører udgør derfor fortsat en terrortrussel i Danmark og mod danske interesser i udlandet.

IS' leder Abu Bakr al-Baghdadis død vil efter CTA's vurdering ikke på kort sigt påvirke terrortruslen mod Vesten og Danmark fra IS. Gruppen offentliggjorde fire dage efter al-Baghdadis død navnet på hans efterfølger – Abu Ibrahim al-Hashimi al-Qurashi.

I marts 2019 mistede IS kontrollen over sit sidste område i Syrien, men det betyder ikke, at gruppen er endeligt nedkæmpet. IS' erklærede mål er fortsat at etablere et "kalifat", men gruppens aktuelle fokus er at bekæmpe lokale sikkerhedsstyrker og genvinde styrke i Syrien og Irak. Kombinationen af den generelle ustabilitet i de to lande og IS' mangeårige erfaring med væbnet kamp gør, at det er usandsynligt, at gruppen vil blive nedkæmpet inden for de næste par år. Hertil kommer, at mange af de underliggende årsager, der muliggjorde, at IS kunne vinde fodfæste i Irak og Syrien, fortsat er til stede, og det betyder, at arabiske sunnimuslimer også fremover vil udgøre et rekrutteringspotentiale for gruppen. IS har siden 2014 udråbt flere såkaldte eksterne provinser i en række lande uden for Syrien og Irak. Disse provinser fungerer i praksis som IS' underafdelinger.

> *"I marts 2019 mistede IS kontrollen over sit sidste område i Syrien, men det betyder ikke, at gruppen er endeligt nedkæmpet."*

IS ser Vesten som sin fjende, og gruppen har fortsat en intention om at dirigere angreb i Vesten. IS' kapacitet til at foretage sådanne angreb er imidlertid reduceret. Netværk af IS-relaterede personer forsøger dog fortsat at yde bistand til og understøtte angreb mod mål i Europa. Personer med relation til IS fungerer bl.a. som facilitatorer og mentorer for sympatisører, der måtte ønske at gennemføre angreb i Vesten. IS forsøger også stadig at inspirere sympatisører til på egen hånd at gennemføre angreb i Vesten. Efter det højreekstremistiske terrorangreb i Christchurch, New Zealand, i marts 2019, opfordrede det officielle IS-medie al-Furqan eksempelvis til hævnangreb på højreekstremister. Efter al-Baghdadis død opfordrede IS i gruppens officielle tidsskrift al-Naba den 31. oktober 2019 til fortsat kamp mod Vesten.

3. For en uddybende gennemgang af forhold i det globale trusselsbillede af betydning for terrortruslen fra udlandet se *Efterretningsmæssig Risikovurdering 2019* fra Forsvarets Efterretningstjeneste på http://fe-ddis.dk.

I takt med, at IS har mistet territorium, er gruppens officielle propaganda dog blevet betydeligt svækket, da både kvantiteten og kvaliteten i de senere år er faldet markant. Gruppens propaganda er i dag primært målrettet publikum i Syrien og Irak samt gruppens eksterne provinser. Hvor propagandaen førhen fokuserede på opbygningen af et "kalifat", er fokus i dag først og fremmest på budskaber om militære aktiviteter og "sejre på kamppladsen". Der findes imidlertid fortsat en stor mængde meget velproduceret og ekstremt voldelig IS-propaganda online, der kan have betydning for radikalisering, udpegning af mål og bidrage med konkret vejledning ved angrebsplanlægning. Hertil kommer, at forskellige uofficielle pro-IS-medier i nogen grad har været i stand til at udfylde tomrummet efter nedgangen i den officielle IS-propaganda. Det er således sådanne pro-IS-grupper, der blandt andet står bag det arabisksprogede magasin "al-Anfal" og det engelsksprogede magasin "From Dabiq to Rome". Begge magasiner har dog en mindre udbredelse, og kvaliteten er markant ringere end de tidligere officielle IS-udgivelser.

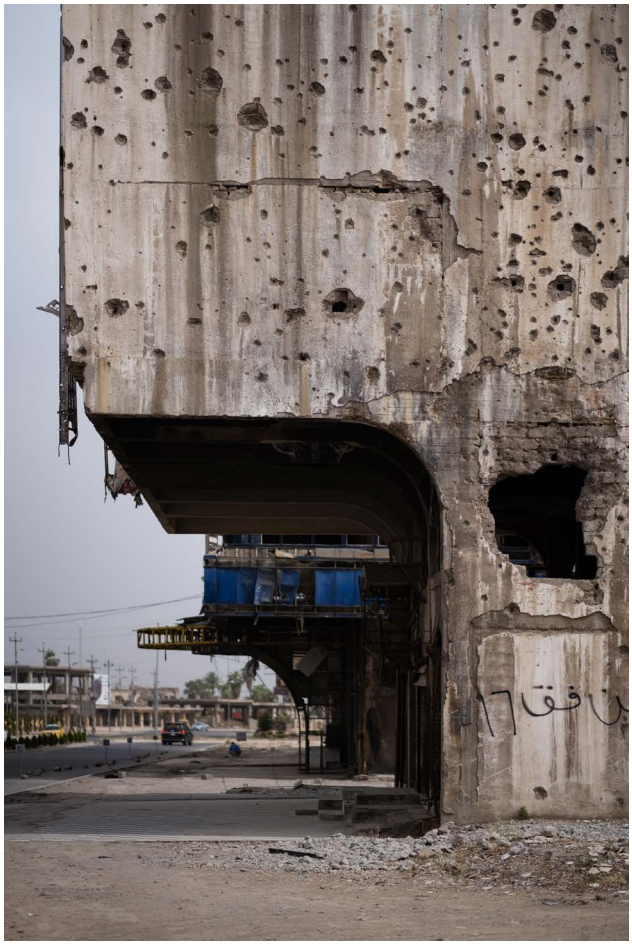


Foto: *Mosul, Irak, Unsplash.com*

Den 21. april 2019 fandt et stort terrorangreb sted i Sri Lanka rettet mod kirker, hoteller og et boligkompleks i og omkring hovedstaden Colombo og på Sri Lankas østkyst. Angrebet illustrerer endnu engang, at lokalt forankrede grupper uden direkte kontakt til IS' centrale ledelse kan begå terror på IS' vegne. Angrebet i Sri Lanka blev endvidere begået af personer, der ikke havde haft nævneværdig bevågenhed fra myndighedernes side.

Al-Qaida (AQ) anser islam for at være under angreb fra Vesten, såvel militært, økonomisk og socialt som kulturelt, og AQ og AQ-tilknyttede grupper har efter CTA's vurdering fortsat ambition om at udføre terrorangreb i Vesten og mod vestlige interesser i andre dele af verden. Al-Qaida på den Arabiske Halvø (AQAP) påtog sig i februar 2020 ansvaret for et angreb på en amerikansk flådebase. Det er første gang siden attentatet mod det franske satireblad Charlie Hebdo i 2015, at AQAP påtager sig ansvar for et angreb i Vesten. AQ er dog svækket og råder ikke længere over de samme kapaciteter som førhen. I de senere år har AQ-tilknyttede grupper primært angrebet lokale mål i lande i Afrika, Mellemøsten og Asien, hvor gruppen

har opbygget og konsolideret et internationalt netværk af underafdelinger, som fokuserer på lokale dagsordener inden for rammerne af en global vision. En af de væsentligste trusler mod Vesten fra AQ udgår fra Syrien, hvor AQ-tilknyttede grupper er til stede i det nordvestlige Syrien, særligt i Idlib-provinsen.

AQ's propaganda opfordrer jævnligt til angreb i Vesten, og det er oftest amerikanske og jødiske mål, der omtales. AQ har dog også fortsat fokus på konkrete sager om opfattede krænkelser af islam, og som noget nyt har AQ-relaterede grupper opfordret til angreb på højreekstremister som hævn for terrorangrebet i marts 2019 i Christchurch, New Zealand.

2.2. Truslen i Danmark fra militant islamisme – særlige fokusområder

Udviklingen i det globale trusselsbillede påvirker terrortruslen fra militant islamisme i Danmark. Det er CTA's vurdering, at der findes enkeltpersoner eller mindre grupper af personer med militant islamistiske sympatier i og uden for Danmark, som kan udgøre en terrortrussel mod Danmark. I det efterfølgende fremhæves en række områder, som ifølge CTA har særlig betydning for trusselsbilledet i Danmark.

Radikalisering i islamistiske miljøer i Danmark
Der findes i Danmark islamistiske miljøer, fysiske såvel som online, hvor der pågår aktiviteter af social og religiøs karakter, der kan have en radikaliserende indvirkning på de deltagende personer. Særligt mere lukkede gruppekonstellationer kan fungere som "ekkokamre", hvor deltagerne uimodsagt kan opbygge og bekræfte hinanden i et militant islamistisk verdenssyn, hvilket kan føre til, at enkeltpersoner eller en mindre gruppe af personer begår terrorhandlinger. Truslen kan både udgå fra kernemedlemmer og fra personer, der har haft mere kortvarig eller perifer tilknytning til de pågældende miljøer, samt personer, som af forskellige grunde er blevet ekskluderet eller afvist. Der kan også udgå en trussel fra enkeltpersoner eller små grupper, som ikke umiddelbart kan sættes i forbindelse med de øvrige miljøer i Danmark, men som på anden vis har gennemgået et radikaliseringsforløb, eksempelvis via forskellige onlineaktiviteter.

> *"Det er CTA's vurdering, at der findes enkeltpersoner eller mindre grupper af personer med militant islamistiske sympatier i og uden for Danmark, som kan udgøre en terrortrussel mod Danmark."*

De islamistiske miljøer, som CTA vurderer relevante i denne sammenhæng, er multietniske i deres sammensætning og hovedsageligt forankret fysisk i og omkring de større byer i Danmark. Aktiviteter på de sociale medier betyder dog, at berøringsfladen ofte er mere geografisk udbredt. Miljøerne varierer i størrelse og sammenhængskraft. Ofte er der et vist overlap mellem personkredsene i de forskellige miljøer, både historisk og aktuelt. Langt hovedparten af de personer, der er tilknyttet miljøerne, er unge mænd, men der findes også enkelte små religiøse kvindefællesskaber, hvor der kan foregå radikalisering. Ofte vil der være personlige og/eller religiøse forbindelser mellem de pågældende mænd og kvinder.

Det er CTA's vurdering, at opbakningen til IS og AQ fortsat er intakt i visse kredse, men at det ikke udtrykkes lige så åbent og eksplicit, som det tidligere har været tilfældet.

Et antal af de personer i Danmark, som efter CTA's vurdering sympatiserer med militant islamisme, har kontakter til ligesindede i udlandet. Kontakten er af meget forskelligartet karakter og omhandler alt fra gæsteprædikener, religiøse arrangementer og indsamling af penge til udveksling af propagandamateriale og angrebsmanualer i lukkede online-fora. Sidstnævnte er særligt bekymrende, da det kan tjene til gensidig inspiration og kapacitetsopbygning på tværs af landegrænser, ligesom der også kan være radikalisatorer online, der aktivt forsøger at tilskynde personer bosat i Danmark til at begå angreb.

Den 11. december 2019 gennemførte PET som nævnt i afsnit 1 i samarbejde med relevante politikredse en koordineret anholdelsesaktion rettet mod personer bosat flere steder i landet. I alt er syv personer blevet varetægtsfængslet sigtet for overtrædelse af straffelovens § 114. Sigtelserne er begrundet i mistanke om planlægning og forberedelse af militant islamistiske terrorangreb i Danmark eller Europa.

Udrejste og tilbagevendte fra Syrien/Irak

Det er CTA's vurdering, at personer, der er eller har været udrejst fra Danmark til konfliktzonen i Syrien/Irak, kan udgøre en trussel mod Danmark eller danske interesser i udlandet. Det gælder både mænd og kvinder, og uanset om personerne opholder sig i konfliktzonen, er returneret til Danmark eller opholder sig i et andet land i eller uden for Europa. Også personer udrejst fra andre lande end Danmark, herunder fra andre europæiske lande, kan udgøre en trussel mod Danmark og danske interesser i udlandet. Truslen fra andre landes udrejste udgår i første række – men ikke udelukkende – fra personer, der opholder sig i lande, der grænser op til Danmark.

Radikaliserede personer, der er eller har været udrejst til konfliktzoner som den i Syrien/Irak, adskiller sig efter CTA's vurdering på en række måder fra andre radikaliserede personer. Udrejse til en konfliktzone demonstrerer en stærk vilje til at handle, selvom det kan indebære livsfare og betydelige afsavn. Opholdet i en konfliktzone kan have ført til en øget brutalisering og voldsparathed hos den enkelte og have medført, at denne kan have tilegnet sig en øget kapacitet til at udføre angreb. Udrejste personer kan herudover have skabt forbindelse til andre personer, grupper og netværk med hensigt om og kapacitet til at begå terror i Vesten.

En persons udrejse til en konfliktzone for at støtte en militant islamistisk dagsorden betyder dog ikke nødvendigvis, at personen udgør en terrortrussel mod Danmark eller danske interesser i udlandet. Terrortruslen beror på en konkret vurdering af den enkeltes hensigt om og kapacitet til at angribe danske mål. Blandt relevante faktorer er den udrejste persons fortsatte sympati for militant islamisme og tilknytning til militant islamistiske grupper samt personens eventuelle våbentræning og deltagelse i kamphandlinger.

Den mulige trussel fra udrejste og hjemvendte personer er ikke begrænset til eventuel angrebsplanlægning, men vedrører også radikalisering af andre personer, propagandavirksomhed, logistisk støtte, terrorfinansiering eller anden terrorrelateret virksomhed.

PET vurderer, at der siden sommeren 2012 er mindst 159 personer, der er eller har været udrejst fra Danmark til Syrien/Irak for at tilslutte sig militant islamistiske grupper. Af disse er knap halvdelen på nuværende tidspunkt vendt tilbage til Danmark eller har taget ophold i primært andre europæiske lande. Omkring en tredjedel af det samlede antal udrejste er efter PET's oplysninger omkommet i konfliktzonen. 34 voksne personer udrejst fra Danmark opholder sig fortsat i Syrien/Irak, eller i omkringliggende lande. Lidt under halvdelen af dem er kvinder. Af de 34 voksne personer, der fortsat opholder sig i konfliktzonen, har ti alene haft opholdstilladelse i Danmark, og disse har alle fået deres opholdstilladelse inddraget. Herudover har tre personer fået frataget deres danske statsborgerskab administrativt. De resterende 21 voksne personer er danske statsborgere. Af disse 21 er 12 ifølge PET's oplysninger fængslet eller tilbageholdt, hovedsageligt i kurdiskkontrollerede lejre og fængsler i det nordøstlige Syrien, mens de resterende ni formodes fortsat at opholde sig på fri fod i konfliktzonen eller i omkringliggende lande.

Foto: *Al-Hawl, Scanpix*

Det er ifølge PET's oplysninger ikke lykkedes personer fra Danmark at udrejse til konfliktzonen i Syrien/Irak for at tilslutte sig militant islamistiske grupper siden 2016. Alle de tilbageværende 34 voksne udrejste fra Danmark har været i konfliktzonen i mere end tre år.

De tyrkiske myndigheder har siden indledningen af den tyrkiske militære intervention i det nordøstlige Syrien i oktober 2019 returneret et antal udrejste personer, der har været i tyrkisk varetægt, til de lande, hvorfra de i sin tid er udrejst. Dette gælder også en udrejst dansk statsborger, og det er muligt, at flere udrejste personer i tyrkisk varetægt i den kommende tid vil blive sendt retur til de lande, de er udrejst fra, herunder til Danmark. CTA vurderer på nuværende tidspunkt, at det er vanskeligt for de tilbageværende udrejste fra Danmark at vende tilbage til Danmark på egen hånd. Det skyldes bl.a., at det i praksis fortsat er svært at forlade konfliktzonen, og at mange af de tilbageværende som nævnt er tilbageholdt i lejre eller fængsler. Flere af de tilbageværende personer har endvidere som berørt tidligere mistet deres opholdsgrundlag i Danmark, og mange med dansk statsborgerskab har ikke længere deres pas. Nye udviklinger i konfliktzonen og/eller ændrede restriktioner på ind- og udrejse til og fra konfliktzonen vil dog kunne påvirke de tilbageværende udrejste personers muligheder for at indrejse i Danmark.

Størstedelen af de danske udrejste vil blive retsforfulgt, hvis de indrejser i Danmark.

Forholdene i de kurdiske lejre i det nordøstlige Syrien, hvor der bl.a. befinder sig personer udrejst fra Danmark, er vanskelige og kan efter CTA's vurdering øge radikaliseringen af de tilbageholdte personer, herunder tilbageholde udrejst fra Danmark. Det gælder især i al-Hawl-lejren, der primært huser kvinder og børn, hvor der befinder sig et stort antal radikaliserede kvinder med fortsat sympati for IS. Der har været flere eksempler på, at tilbageholdte kvinder har angrebet lejrpersonalet og udøvet social kontrol og selvjustits over for andre tilbageholdte kvinder. I september 2019 opfordrede IS' nu afdøde leder, Abu Bakr al-Baghdadi, i en officiel tale IS' medlemmer til at iværksætte angreb på fængsler og lejre for at befri IS-medlemmer. IS har tidligere haft succes med at organisere fangeflugter, og det er muligt, at sikkerheden omkring lejrene vil blive forringet yderligere fremover.

> *"Forholdene i de kurdiske lejre i det nordøstlige Syrien, hvor der bl.a. befinder sig personer udrejst fra Danmark, er vanskelige og kan efter CTA's vurdering øge radikaliseringen af de tilbageholdte personer, herunder tilbageholde udrejst fra Danmark."*

Der er flere af personerne udrejst fra Danmark, der medbragte børn til konfliktzonen, og nogle har fået børn dernede. Ifølge PET's oplysninger opholder der sig ca. 40 børn af danske statsborgere i konfliktzonen. PET har herudover oplysninger om, at ca. ti børn af personer, som tidligere har haft opholdstilladelse i Danmark, også opholder sig i konfliktzonen. Af de i alt ca. 50 børn af personer udrejst af Danmark opholder ca. 30 sig i det nordøstlige Syrien, primært i lejrene al-Roj og al-Hawl. De øvrige børn opholder sig ifølge PET's oplysninger bl.a. i det nordvestlige Syrien og i Tyrkiet. I 2019 blev to børn af personer udrejst fra Danmark evakueret fra Syrien med bistand fra danske myndigheder med henblik på efterfølgende indrejse i Danmark.

Det er efter CTA's vurdering usandsynligt, at der udgår en aktuel terrortrussel fra børn af personer udrejst fra Danmark til konfliktzonen. Det hænger først og fremmest sammen med børnenes nuværende lave alder. Det er CTA's generelle vurdering, at større børn, der vender hjem fra konfliktzonen eller fra lejre, kan udgøre en terrortrussel på grund af indoktrinering eller anden påvirkning i konfliktzonen. Det er i den forbindelse også CTA's vurdering, at risikoen for indoktrinering og påvirkning som udgangspunkt forøges, jo længere tid børnene opholder sig i et radikaliseret miljø, herunder i lejrene i det nordøstlige Syrien. Truslen fra udrejste fra Danmark, herunder fra udrejste børn, der kommer til Danmark, vil blandt andet kunne påvirkes af, hvorledes de modtages af de hjemlige myndigheder, herunder om de tilbydes støtte med henblik på eventuel afradikalisering og reintegration.

Radikaliserede løsladte fra fængslerne

CTA vurderer, at radikaliserede indsatte i fængslerne kan udgøre en terrortrussel, når de løslades. Truslen kan udgå fra personer, der er dømt for terrorrelaterede forbrydelser, samt fra andre voldsparate personer, der påbegynder eller fortsætter en radikaliseringsproces under afsoning. Radikaliserede, løsladte personer kan udgøre en terrortrussel allerede kort tid efter deres løsladelse. Herudover kan løsladte personer engagere sig i eksisterende islamistiske miljøer. PET har kendskab til enkelte tilfælde, hvor radikaliserede fanger i Danmark har haft kontakt til indsatte med relation til kriminelle miljøer, hvor der er adgang til våben.

Der er for tiden i mange europæiske lande et historisk højt antal indsatte, der er dømt i terrorrelaterede sager med relation til militant islamisme. Når disse personer løslades, kan de udgøre en terrortrussel i såvel afsoningslandet som i andre europæiske lande. Risikoen for, at personer, dømt for forbrydelser relateret til militant islamistisk terrorisme i andre europæiske lande, rejser til Danmark for at begå et terrorangreb efter løsladelse, afhænger efter CTA's vurdering i høj grad af, om personerne har personlige forbindelser til Danmark eller danske personer, eller om der er et særligt fokus på Danmark i militant islamistisk propaganda.

> *"Der er for tiden i mange europæiske lande et historisk højt antal indsatte, der er dømt i terrorrelaterede sager med relation til militant islamisme. Når disse personer løslades, kan de udgøre en terrortrussel i såvel afsoningslandet som i andre europæiske lande."*

CTA har kendskab til, at seks gerningsmænd i Europa siden 2015 har begået et terrorangreb under udgang eller inden for de første seks måneder efter deres løsladelse. En af disse gerningsmænd var danske Omar Abdel Hamid el-Hussein, der gennemførte et terrorangreb i København i februar 2015. CTA har kendskab til yderligere fire personer i Europa, der har begået et terrorangreb inden for det første år efter deres løsladelse. Senest begik en 20-årig mand den 2. februar 2020 et terrorangreb i London, Storbritannien, ca. en uge efter løsladelse fra afsoning af en terrorrelateret dom på tre år og fire måneder.

Den 1. marts 2020 var der i alt 23 personer i Danmark, der enten afsoner straf eller sidder varetægtsfængslet eller domsanbragt i en terrorrelateret sag med udspring i militant islamisme. To af personerne er dømt for at have planlagt at begå terrorangreb i Danmark. Der blev i 2018 og 2019 løsladt flere personer, der

har afsonet domme for at have begået eller planlagt at begå terrorangreb i Danmark. Det drejer sig om to personer fra "Vollsmose-sagen" (anholdt i september 2006), en person fra "Glasvej-sagen" (anholdt i september 2007), fire personer fra Sverige, der havde planlagt et angreb mod Jyllands-Posten i København (anholdt december 2010) og gerningsmanden bag et angreb mod Kurt Westergaard (anholdt i januar 2010). Det er sandsynligt, at nogle af de løsladte personer fortsat sympatiserer med militant islamisme og kan udgøre en terrortrussel efter deres løsladelse.

I 2019 blev tre personer løsladt efter endt afsoning af domme relateret til udrejse til en konfliktzone. Der er flere danske eksempler på, at personer, der har været dømt for andre terrorrelaterede forbrydelser end angrebsplanlægning, efterfølgende dømmes i lignende sager. Det drejer sig eksempelvis om sager vedrørende offentlig billigelse af terror, bombetrusler, terrorfinansiering og udrejse til en konfliktzone for at tilslutte sig militant islamistiske grupper.

Asylansøgere, flygtninge og migranter

CTA vurderer, at der kan udgå en terrortrussel fra personer, der sympatiserer med militant islamisme, blandt flygtninge og migranter, som ankommer til Europa og Danmark, samt fra asylansøgere, afviste asylansøgere og anerkendte flygtninge, der allerede opholder sig i Europa eller i Danmark. Også udlændinge på tålt ophold, der sympatiserer med militant islamisme, kan udgøre en trussel. Det er dog efter CTA's vurdering kun en meget lille andel af det antal personer, der ankommer til Europa og Danmark som flygtninge og migranter, der har sympati for militant islamisme, og som kan udgøre en terrortrussel.

Terrortruslen fra flygtninge og migranter, der søger mod Europa, udgår efter CTA's vurdering bl.a. fra personer, der er blevet udsendt af militant islamistiske grupper med henblik på at begå terrorangreb i Europa, herunder i Danmark. Det er fortsat muligt, at IS, og i mindre grad AQ, vil forsøge at udnytte flygtninge- og migrantruterne til dette formål. Eksempelvis blev to afrikanske asylansøgere i henholdsvis april og juni 2018 anholdt og sigtet af de italienske myndigheder for at planlægge terrorangreb i Europa. Begge personer havde forinden opholdt sig i IS-træningslejre i Libyen samt svoret troskab til gruppen. Personerne er siden blevet dømt i Italien. Medlemmer af IS har tidligere benyttet netværk af menneskesmuglere til at facilitere rejser til og fra konfliktzoner, herunder særligt Syrien. CTA vurderer, at IS forsat kan anvende sådanne netværk til at sende medlemmer af gruppen til Europa. CTA vurderer dog, at indrejse til Europa er vanskeliggjort af øgede sikkerhedsforanstaltninger, herunder øget kontrol af EU's eksterne grænser og et tæt politi- og efterretningssamarbejde.

I "Tændstiksagen" planlagde og forberedte to syriske flygtninge, bosat i henholdsvis Sverige og Tyskland, et terrorangreb i Danmark i slutningen af 2016. Angrebet skulle udføres ved brug af knive og en hjemmelavet bombe, bl.a. fremstillet ved hjælp af et meget stort antal tændstikker medbragt fra Tyskland. Angrebet skulle gennemføres i København mod et ukendt mål og på et ukendt tidspunkt. Angrebet blev ikke gennemført, fordi en af gerningsmændene blev nægtet indrejse i Danmark og derefter anholdt af det tyske politi. Den ene af de to personer blev i juli 2017 i Tyskland idømt seks et halvt års fængsel. Den anden blev i maj 2019 i Danmark idømt 12 års fængsel og udvist for bestandigt.

Tyrkiet har ved flere lejligheder truet med at frigive et stort antal flygtninge og har senest i slutningen af februar måned 2020 åbnet sine grænser mod Bulgarien og Grækenland for flygtninge, der vil forlade landet. Denne frigivelse har øget antallet af flygtninge, der forsøger at indrejse til Europa betragteligt, hvilket kan resultere i en markant overbelastning af særligt de syd- og mellemeuropæiske migrationsmyndigheders faciliteter og ressourcer. Også EU's sikkerhedsforanstaltninger, herunder kontrol af de eksterne grænser som eksempelvis patruljering i Middelhavet, vil blive sat under pres, hvilket kan føre til, at et større antal flygtninge, heriblandt radikaliserede personer eller personer, der er udsendt af militant islamistiske grupper, slipper uden om grænsekontrollen og når Europa som illegale indvandrere, uden at de europæiske myndigheder er bevidst om deres ankomst og/eller videre færden.

Asylansøgere, afviste asylansøgere og migranter kan efter CTA's vurdering være særligt sårbare over for radikalisering og påvirkning fra militant islamistiske dagsordener. Det gør sig især gældende for yngre personer, der rejser alene. Sårbarheden kan bl.a. skyldes frustration over egen situation, en følelse af eksklusion, fravær af familie samt psykisk ustabilitet.

Personer bosat i andre lande
CTA vurderer, at der kan udgå en terrortrussel mod Danmark fra enkeltpersoner og mindre grupper med militant islamistiske sympatier bosat i andre lande. Truslen kan bl.a. udgå fra tilbagevendte fremmedkrigere eller personer, der løslades efter endt afsoning af terrorrelaterede domme. Truslen udgår i første række fra personer bosat i lande, der grænser op til Danmark.

Der er efter CTA's vurdering en række faktorer, der kan have en særlig betydning for, at personer i andre lande, herunder i Danmarks nabolande, måtte have en hensigt om at angribe mål i Danmark: Danmarks internationale, militære engagementer, herunder Danmarks deltagelse i den internationale koalition mod IS i Syrien/Irak; aktuelle eller tidligere sager, hvor Danmark fremstilles som en "krænkernation"; forudgående kendskab til Danmark; bevidsthed om, at forberedelser af angreb i ét land rettet mod mål i et andet kan være særligt vanskelige for myndigheder at afdække og dermed også afværge; modvilje mod at angribe i eget land samt Danmarks geografiske nærhed.

> *"Truslen kan bl.a. udgå fra tilbagevendte fremmedkrigere eller personer, der løslades efter endt afsoning af terrorrelaterede domme."*

Der har i de seneste ti år været flere sager, hvor personer bosat i andre lande har udvist en intention om at angribe mål i Danmark. Det seneste eksempel er den allerede nævnte "Tændstiksag", hvor to syriske flygtninge, bosat i henholdsvis Sverige og Tyskland, i slutningen af 2016 planlagde og forberedte et angreb i Danmark.

2.3. Terrormål i Danmark for militante islamister

CTA vurderer, at de mest sandsynlige mål for et militant islamistisk terrorangreb i Danmark er et ubeskyttet civilt mål, såsom et offentligt befærdet sted eller et arrangement, hvor mange mennesker er samlet, eller

"symbolmål", i første række personer, institutioner og begivenheder, der kan opfattes som islamkrænkende. Andre mulige mål er jødiske mål, politi og militær – særligt i forbindelse med bevogtningsopgaver – visse offentlige myndigheder samt regeringsrepræsentanter. Militante islamister har fortsat fokus på at ramme transportinfrastrukturen, herunder særligt den internationale flytrafik og lufthavne.

Militante islamisters måludpegning følger ikke et ensartet og forudsigeligt forløb, og den kan ændre sig i løbet af en planlægningsfase. Måludpegningen kan påvirkes af opfordringer i militant islamistisk propaganda, aktuelle dagsordner, personlige netværk og præferencer samt angrebsplanlæggerens kapacitet. Herudover kan allerede gennemførte terrorangreb virke som inspiration – en såkaldt copycat-effekt. IS har siden midten af 2014 haft stor fokus på at ramme tilfældige civile i Vesten, og civile har i stigende grad været det primære mål for terrorangreb.

Transportsektoren, herunder civile personer, der opholder sig i et transportmiddel, har vist sig at være et attraktivt terrormål for militante islamister. I marts 2019 gennemførte en terrorist et angreb i en sporvogn i Nederlandene, hvor fire personer blev dræbt.

Som nævnt i afsnit 2.1. har AQ fortsat fokus på konkrete sager om opfattede krænkelser af islam i sin propaganda. Det har IS kun i meget begrænset omfang indtil videre haft. CTA vurderer dog, at militante islamister generelt anser opfattede krænkere af islam og islamkritiske arrangementer i Danmark for at være legitime mål. CTA vurderer yderligere, at nye sager med opfattede krænkelser, som får en væsentlig eksponering i nationale og internationale medier, kan skabe opmærksomhed på opfattede krænkere i Danmark. Der har ikke været gennemført angreb rettet specifikt mod krænkermål i Vesten siden terrorangrebet i København i februar 2015. Der har dog været gennemført angreb mod tilfældige civile, som var motiveret af krænkersager. I efteråret 2018 angreb en gerningsmand med kniv tilfældige personer i Amsterdam, Nederlandene, som reaktion på en "Tegn Profeten"-konkurrence arrangeret af den nederlandske politiker Geert Wilders.

Definitioner på måltyper

CTA vurderer, at der i den militant islamistiske angrebshistorik mod mål i Vesten kan skelnes mellem symbolmål og civile mål.

Symbolmål:

- Myndighedsmål: Nationale myndigheder, herunder ministerier, politi, militær og redningsberedskab samt repræsentanter for sådanne myndigheder. Myndighedsmål kan også omfatte diplomatiske repræsentationer.
- "Krænkermål": Grupper, personer, lokaliteter og arrangementer, der er udpeget i kraft af udtalelser, handlinger eller tematikker, som en gerningsmand opfatter som krænkende over for islam.
- Jødiske mål: Synagoger, jødiske tilholdssteder og institutioner, som f.eks. skoler samt andre mål, hvis tilknytning til jødedommen er nemt identificerbar. Jødiske mål omfatter tillige israelske interesser i Danmark, herunder diplomatiske repræsentationer, virksomheder og turister.
- Religiøse mål: Andre religiøse mål, herunder kristne symbolmål som kirker og kristne skoler, samt andre muslimske symbolmål, herunder shiamuslimske moskeer. Derudover omfatter andre religiøse symbolmål også andre trosretninger.

Civile mål:

- Tilfældige borgere uden særlig tilknytning til myndigheder, vestlig udenrigspolitik, religion eller kritik af islam.

Jødiske personer, begivenheder og lokaliteter har fortsat en fremtrædende plads i militant islamistisk propaganda, og militante islamister anser sådanne mål for at være legitime terrormål.

2.4. Fremgangsmåder ved militant islamistiske terrorangreb i Danmark

CTA vurderer, at terrorangreb med lettilgængelige midler er den mest sandsynlige militant islamistiske angrebsform i Danmark. Med lettilgængelige midler forstås hovedsageligt knive, slagvåben, ildspåsættelser og køretøjer. Angreb med brug af skydevåben eller hjemmelavede bomber er også mulige. Angreb med mere innovative midler såsom droner eller kemiske, biologiske og radiologiske midler omtales løbende i militant islamistisk propaganda, og risikoen for angreb med sådanne midler nævnes også lejlighedsvist i åbne medier. Det er imidlertid CTA's vurdering, at angreb med disse midler er langt mindre sandsynlige.

Militante islamisters valg af fremgangsmåde påvirkes af propagandaen og af ressourcer, evner, netværk, adgang til det påtænkte mål samt inspiration fra andre angreb. Kapaciteten hos militante islamister i Danmark kan øges gennem kontakt til ressourcepersoner, som deler instruktioner og giver specifik rådgivning om konkrete fremgangsmåder, eller ved rekruttering eller radikalisering af nøglepersoner, der har legitim adgang til faciliteter, ressourcer eller information. Sådanne "insidere" kan have forskellige funktioner og ansættelsesforhold, der kan gøre dem i stand til at gennemføre et terrorangreb, bidrage til gennemførelse af et terrorangreb eller på anden måde forvolde skade.

Foto: *København, Unsplash.com*

"Jødiske personer, begivenheder og lokaliteter har fortsat en fremtrædende plads i militant islamistisk propaganda, og militante islamister anser sådanne mål for at være legitime terrormål."

Terrorangreb med lettilgængelige midler bliver løbende fremhævet i militant islamistisk propaganda og kan gennemføres spontant eller efter kort planlægning. Især angrebene i 2016 og 2017 med køretøjer mod store menneskemængder i en række europæiske byer viser, at angreb med lettilgængelige midler kan have stor skadevirkning. Der er i Danmark personer med kapacitet til at anvende skydevåben til at gennemføre terrorangreb, men erhvervelsen af skydevåben er primært forbeholdt personer med lovlig adgang til våben eller med kriminelle kontakter.

Det er CTA's vurdering, at der i Danmark er personer, der har kapacitet til at fremstille og gennemføre angreb med mindre, hjemmelavede bomber. Der findes på internettet retvisende vejledninger og manualer til brug for fremstillingen af forskellige sprængstoffer og hjemmelavede bomber, der vil kunne benyttes af personer uden særlige forkundskaber. Effekten af de fremstillede bomber kan dog variere betydeligt. Der er en række barrierer i forhold til produktion af hjemmelavet sprængstof, herunder den generelle bevågenhed omkring salg af stoffer, som kan anvendes til fremstilling af bomber. Tilgængelighed af kommercielt sprængstof og andre kommercielle komponenter, som eksempelvis detonatorer, kan lette fremstillingen af mindre bomber. Der er enkelte kriminelle miljøer i Danmark, der har kontakter, som muliggør erhvervelsen af fabriksfremstillet sprængstof, herunder særligt dynamit, som med stor sandsynlighed stammer fra Sverige.

CTA vurderer, at personer, der har gennemgået våbentræning i en konfliktzone, såsom i Syrien/Irak, eller som har våbenkendskab fra f.eks. kriminelle miljøer, vil være i stand til at gennemføre angreb med særlig stor effekt samt serieangreb, hvor personer eller grupper foretager flere angreb i forlængelse af hinanden.

Der er i Danmark kapacitet til at anvende droner til rekognoscering, simple angreb eller til at skræmme, men militante islamisters kapacitet til at bruge droner til at forvolde betydelig skade er lav. Militante islamister har demonstreret en ikke ubetydelig evne til at operere og anvende droner til bl.a. angreb i og omkring konfliktzonen i Syrien/Irak, men den opbyggede kapacitet er endnu ikke set overført til Vesten. Militante islamisters udfordringer ved at anvende droner som angrebsvåben er efter CTA' vurdering fortsat meget store i forhold til den skade, som et sådant våben ville kunne udrette.

Den militant islamistiske propaganda har løbende fokus på anvendelsen af kemiske virkemidler, men CTA vurderer, at militante islamisters kapacitet til at gennemføre kemiske angreb med andet end uforarbejdede midler er lav. Den militant islamistiske propaganda fokuserer ligeledes løbende på biologiske virkemidler, men CTA vurderer, at militante islamisters kapacitet til at våbengøre biologiske virkemidler, såsom miltbrand, er meget lav. Der var i 2018 tre sager (i henholdsvis Storbritannien, Frankrig og Tyskland), hvor brug af toksinet ricin blev overvejet i forbindelse med militant islamistisk angrebsplanlægning. I ingen af sagerne resulterede overvejelserne i angreb. Ifølge CTA's oplysninger var der ikke i 2019 sager med validerede oplysninger om, at militante islamister har haft fokus på brug af ricin i forbindelse med angrebsplanlægning. Såvel kemiske som biologiske virkemidler har været benyttet i forbindelse med fremsendelse af såkaldte "pulverbreve", men der er kun meget få eksempler på vellykkede angreb med pulverbreve, og CTA vurderer, at langt størstedelen af brevene indeholdende et uidentificeret pulver primært har til formål at skræmme og chikanere modtageren.

CTA vurderer, at militante islamistister i Danmark har meget lav kapacitet til at gennemføre terrorangreb med radiologiske virkemidler og ingen kapacitet til at begå terror ved hjælp af nukleare midler.

Militante islamister har i få tilfælde vist interesse for at udføre cyberterror, men CTA vurderer, at militante islamisters kapacitet til at gennemføre cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk national infrastruktur eller lignende mål, er lav[4].

CTA følger løbende den teknologiske udvikling med henblik på at vurdere nye teknologiers indvirkning på terrortruslen i Danmark. Trods et muligt potentiale vurderer CTA, at ingen af de nye teknologier, såsom kunstig intelligens, 3D-printning og syntesebiologi[5], på nuværende tidspunkt er velegnede til brug i et terrorangreb.

2.5. Finansiering af militant islamistiske terrorgrupper i udlandet

Terrorfinansiering er med til at opretholde terrorgrupper og fremme deres virke. Tilførsel af finansielle ressourcer forbedrer terrorgruppers mulighed for at forberede og udføre konkrete operationer samt rekruttere og fastholde medlemmer.

CTA vurderer, at omfanget af terrorfinansiering i Danmark til militant islamistiske grupper i Syrien og Irak i de senere år er faldet. Det skyldes bl.a. indskrænkede muligheder for at overføre midler som følge af IS' tab af territorium i Syrien og et lavt antal tilbageværende danske fremmedkrigere i konfliktzonen. CTA vurderer dog, at intentionen blandt personer i Danmark om at finansiere militant islamistiske grupper i udlandet ikke er aftaget. Samtidig er viden om metoder til at anskaffe penge ved økonomisk kriminalitet og måder at overføre penge eller andre formuegoder til terrorgrupper blevet mere udbredt i specifikke sunni-islamistiske netværk i Danmark i de senere år.

Blandt militant islamistiske grupper er det først og fremmest grupper i Syrien og Irak, der nyder godt af terrorfinansiering fra personer i Danmark.

2.6. Terrortruslen fra militant islamisme mod danskere og danske interesser i udlandet

Terrortruslen fra militant islamisme mod danskere og danske interesser i udlandet kommer særligt til udtryk i lande og regioner, hvor AQ og IS har afdelinger, hvor de kan træne og planlægge angreb. I de seneste par år har militante islamistiske netværk uden direkte forbindelse til IS eller AQ imidlertid også andre steder udført angreb mod vestlige interesser i lande uden for Europa.

4. Se også CFCS´s vurdering af Cybertruslen mod Danmark.
5. Ved syntesebiologi designes og konstrueres nye biologiske systemer, som ikke findes i naturen.

Terrortruslen retter sig både mod beskyttede mål, såsom diplomatiske repræsentationer, og ubeskyttede mål, såsom virksomheder, NGO'er og turister. Truslen mod danske interesser adskiller sig som udgangspunkt ikke fra truslen mod andre vestlige landes interesser, og som andre vesterlændinge kan danskere risikere at blive ofre for angreb, der rettes mod vestlige interesser. Det viser bl.a. angrebet i Sri Lanka i 2019, der kostede tre danske statsborgere livet. Danskere i udlandet risikerer herudover at blive ofre for angreb, hvis de befinder sig i nærheden af lokale terrormål, såsom store menneskemængder, kirker eller særlige myndighedsbygninger.

"Tegningesagen" er ikke glemt i militant islamistiske kredse, og Danmarks ry som "krænkernation" kan hurtigt blive bragt op internationalt, hvorved terrortruslen mod danske interesser i udlandet i så fald vil kunne ændre sig i negativ retning. Danske diplomatiske repræsentationer og anden dansk tilstedeværelse i udlandet, herunder ansatte i danske virksomheder, vil kunne blive opfattet som symbolske mål, der giver mulighed for at ramme Danmark uden at foretage angreb i Danmark. Det er muligt, at danske diplomatiske repræsentationer kan blive mål for terrorangreb, hvis de opfattes som mindre sikrede end større vestlige landes repræsentationer.

Der udgår en alvorlig terrortrussel mod vestlige, herunder danske, interesser i en række lande i Nord-, Vest- og Østafrika. Der har været flere angreb og angrebsplaner, der viser, at særligt turistmål og lokaliteter, hvor vesterlændinge opholder sig, er prioriterede mål for militante islamister i regionen. I Østafrika gennemfører den Somalia-baserede gruppe al-Shabaab jævnligt angreb i Somalias hovedstad Mogadishu, ligesom gruppen har planlagt og gennemført angreb i Kenya, herunder i hovedstaden Nairobi. I Egypten har militante islamister i flere tilfælde angrebet udenlandske, herunder vestlige, mål.

Der har de seneste to år fundet angreb sted i Nord- og Vestafrika, hvor danske statsborgere er blevet angrebet. Det seneste angreb fandt sted i december 2018, hvor en dansk og en norsk turist blev dræbt af en gruppe IS-sympatisører i Marokko i et bjergområde tæt på Marrakesh. Gerningsmændene udsendte efter angrebet en video, hvor de udlagde drabene på de to kvinder som et hævnangreb for IS' tab af Hajin, der på daværende tidspunkt var en af IS' sidste byer i Syrien. CTA vurderer, at de to kvinder ikke blev udvalgt pga. deres nationalitet, men derimod pga. deres vestlige udseende.

Der udgår også en alvorlig terrortrussel mod vestlige, herunder danske, interesser i en række lande i Mellemøsten og Syd- og Sydøstasien, hvor både AQ og IS samt deres tilknyttede grupper er aktive. Det gælder især i Syrien og Irak samt i Afghanistan og Pakistan.

CTA vurderer, at truslen fra militant islamistiske bortførelser er størst i konfliktzoner og disses nærområder. Bortførelser indgår bl.a. som en del af militant islamistiske gruppers finansieringsgrundlag, og risikoen for bortførelser kan derfor stige, hvis militant islamistiske grupper har mistet andre finansieringskilder.

Det er muligt at holde sig orienteret om særlige landerisici i Udenrigsministeriets rejsevejledning på www.um.dk.

3. TERRORTRUSLEN FRA HØJREEKSTREMISME

CTA vurderer, at terrortruslen fra højreekstremister i Danmark er øget og nu er af en sådan karakter, at CTA hæver trusselsniveauet fra niveauet begrænset til niveauet generel.

Danske højreekstremister har en række politiske mål, hvoraf de primære er at bekæmpe udbredelsen af islam i Danmark, at begrænse indvandring og at konfrontere politiske modstandere, særligt venstreorienterede politikere og grupper. Et højreekstremistisk terrorangreb ville derfor primært rettes mod muslimer og moskeer, asylansøgere og asylcentre, jøder og synagoger samt personer af anden etnisk oprindelse, herunder lokaliteter hvor sådanne personer vurderes at samles. Øvrige mulige mål er politiske modstandere, især venstreekstremister, homoseksuelle samt myndigheder og udvalgte politikere, herunder særligt dem, der opfattes som ansvarlige for ikke-vestlig indvandring til Europa.

CTA vurderer, at det mest sandsynlige højreekstremistiske terrorangreb i Danmark er et angreb, der udføres af en soloterrorist eller en lille gruppe, der befinder sig i periferien af eller uden for et højreekstremistisk miljø. Det mest sandsynlige våben, der vil blive anvendt ved et højreekstremistisk terrorangreb i Danmark, er blank- eller stikvåben eller lette skydevåben, herunder særligt jagtrifler, haglgeværer og pistoler. Andre mulige våben inkluderer ildspåsættelse, hjemmelavede bomber og køretøjer.

Der var i 2015-2017 i flere europæiske lande talrige tilfælde af voldelige overfald på asylansøgere og migranter samt hærværk og brandstiftelse mod asylcentre i flere europæiske lande. Sådanne hændelser kan efter en konkret vurdering udgøre terror. Disse voldsepisoder var i høj grad ansporet af indrejsen på daværende tidspunkt af et stort antal asylansøgere til Europa. Også i Danmark har der været tilfælde af brandstiftelse mod asylcentre. I takt med faldet i indrejse af asylansøgere til Europa er antallet af sådanne angreb faldet betragteligt, og der har ikke været tilfælde af brandstiftelse i de seneste år i Danmark. CTA vurderer dog, at tilsvarende hændelser kan forekomme igen, særligt hvis der sker en stigning i antallet af asylansøgere i Danmark.

> *"CTA vurderer, at det mest sandsynlige højreekstremistiske terrorangreb i Danmark er et angreb, der udføres af en soloterrorist eller en lille gruppe, der befinder sig i periferien af eller uden for et højreekstremistisk miljø."*

Der har i de senere år været en række antisemitiske aktioner i Danmarks nabolande og senest også i Danmark. I november 2019 begik højreekstremister eksempelvis groft hærværk og gravskænding af jødiske symboler og grave.

Der har siden foråret 2019 været en række højreekstremistiske terrorangreb i Vesten udført af soloaktører, hvis radikaliseringsproces primært er foregået på online-fora[6]. Blandt angrebene var et omfattende angreb i marts 2019 i Christchurch, New Zealand, samt angreb i Poway og El Paso, USA, Bærum, Norge, og Halle,

6. Der var efter CTA's opgørelse i alt mindst 12 højreekstremistiske angreb i Vesten i 2019. Det skal understreges, at de vestlige lande har forskellige definitioner af højreekstremisme og varierende opgørelsesmetoder.

Tyskland. Det seneste angreb fandt sted den 19. februar 2020, hvor en person med højreekstremistiske sympatier dræbte ni personer på to lokaliteter i Hanau, Tyskland.

Det er CTA's vurdering, at angrebet i Christchurch var med til at inspirere de efterfølgende enkelt-mandsangreb. Gerningsmanden bag angrebet i Christchurch lagde umiddelbart inden angrebet et letforståeligt manifest ud på internettet, og han livestreamede dele af angrebet på Facebook. CTA vurderer, at højreekstremistiske angreb, såsom angrebet i Christchurch, eventuelt sammenholdt med en høj angrebsfrekvens, kan inspirere til yderligere højreekstremistiske angreb udført af solo-aktører. Højreekstremistiske enkelt-mandsangreb, der er inspireret af angrebene, kan også finde sted i Danmark. Også militant islamistiske angreb kan inspirere højreekstremister til at udføre terrorangreb.

Foto: *Unsplash.com*

De højreekstremistiske terrorangreb i 2019 og 2020 viser, at virtuelle platforme og medier på internettet i stort omfang anvendes til at sprede højreekstremistisk propaganda og til radikalisering. Deling af propaganda, herunder manifester eller breve i forbindelse med konkret udførsel af højreekstremistiske angreb, er en meget effektiv måde, hvorpå højreekstremister med en beskeden indsats kan få deres budskab spredt til et stort publikum. CTA vurderer derfor, at det er sandsynligt, at denne form for deling af højreekstremistisk propaganda vil fortsætte.

> *"De højreekstremistiske terrorangreb i 2019 og 2020 viser, at virtuelle platforme og medier på internettet i stort omfang anvendes til at sprede højreekstremistisk propaganda og til radikalisering."*

Danske højreekstremister opbygger efter CTA's vurdering i stigende grad relationer til ligesindede i udlandet, herunder på virtuelle platforme. Relationerne betyder bl.a., at danske højreekstremister hurtigere og mere effektivt kan tillære sig nye fremgangsmåder, koordinere internationalt og søge støtte fra ligesindede i udlandet.

4. TERRORTRUSLEN FRA VENSTREEKSTREMISME

CTA vurderer, at terrortruslen fra venstreekstremister i Danmark er begrænset. Den har ikke udviklet sig nævneværdigt i de seneste år.

Danske venstreekstremisters primære mål er at bekæmpe opfattet racisme og fascisme, særligt som det kommer til udtryk hos højreekstremistiske grupper. Truslen fra venstreekstremister retter sig derfor primært mod disse grupper samt mod enkeltpersoner med sympati for højreekstremisme og i mindre grad mod repræsentanter for højreorienterede politiske partier. Herudover kan der være en trussel rettet mod myndighederne, især politiet.

Det mest sandsynlige venstreekstremistiske terrorangreb i Danmark vil efter CTA's vurdering blive udført af personer, der har kontakt til eller er medlemmer af en venstreekstremistisk gruppe. Venstreekstremistiske terrorangreb kan ske i forbindelse med aktioner rettet mod højreekstremistiske begivenheder samt ved konfrontationer med myndighederne, særligt under venstreekstremistiske demonstrationer og aktioner.

Det mest sandsynlige våben ved et venstreekstremistisk terrorangreb i Danmark er slag- og blank-våben, molotovcocktails og fyrværkeri, herunder særligt kraftige kanonslag og krysantemumbomber. Et andet muligt våben er ildspåsættelse, herunder i forbindelse med demonstrationer og aktioner.

Højreekstremistiske angreb i Danmark kan inspirere personer med sympati for venstreekstremisme i Danmark til at begå angreb.

De venstreekstremistiske miljøer samarbejder med ligesindede organisationer og grupper i udlandet, og danske venstreekstremister deltager også i demonstrationer i udlandet. Det internationale samarbejde kan føre til en øget kapacitetsopbygning i form af både taktiske evner og voldsparathed i hjemlige venstreekstremistiske miljøer.

5. ANDRE TRUSLER, DER KAN HAVE KARAKTER AF TERROR

Politiske, etniske og religiøse konflikter i udlandet kan føre til reaktioner fra personer eller grupper med tilknytning til de berørte grupper i Danmark, der kan udvikle sig til handlinger, der har karakter af terror. De konkrete reaktioner, herunder voldelige protester, vil bl.a. kunne blive rettet mod diplomatiske repræsentationer i Danmark.

Voldelige aktioner motiveret af politiske enkeltsager kan efter en konkret juridisk vurdering have karakter af terror. Der er flere eksempler på enkeltsagsaktivisme, der har været motiveret af et ønske om at fremme sager, såsom dyrevelfærd eller miljøbeskyttelse. En nyere tendens er klimaaktivisme, der er drevet af et ønske om at skabe opmærksomhed omkring klimaet og/eller eventuelle klimaforbedrende initiativer. Klimaaktivisme kan både udøves af personer og/eller grupper, der er tilhængere af flere klimaforbedrende tiltag, og af personer og/eller grupper, der er modstandere heraf. I Danmark er klimaaktivisme indtil nu alene ført med ikke-voldelige midler, og CTA er ikke bekendt med, at enkeltsagsaktivisme, herunder klimaaktivisme, i Danmark har antaget karakter af terror.

Tilstedeværelsen af psykiske lidelser hos en gerningsmand kan gøre det vanskeligt for myndighederne at vurdere, hvorvidt personens voldelige handlinger udøves med forsæt om at begå terror. Der kan i visse situationer være grund til at rette særlig opmærksomhed mod personer med psykiske lidelser, der udviser tegn på radikalisering, og som tidligere har udvist voldelig adfærd eller foretaget impulsive handlinger.

En psykisk lidelse er ikke nødvendigvis udslagsgivende for en persons evne og vilje til at begå terror, men alene en af flere faktorer, der skal inddrages i en vurdering af den terrortrussel, der eventuelt udgår fra den pågældende person. CTA vurderer, at en persons mentale tilstand kan have stor betydning for dennes adfærd og motivation til at handle, herunder også i forbindelse med terror.

Sociale medier anvendes i stigende grad til at fremsætte truende ytringer, bl.a. imod offentlige personer, og til at sprede rygter og falske nyheder. Mens langt størstedelen af disse ytringer ikke fører til konkret angrebsplanlægning, vurderer CTA, at sådanne tilkendegivelser kan påvirke visse psykisk uligevægtige eller meget påvirkelige personer til at begå ideologisk motiveret vold, der kan have karakter af terror.

6. TERRORTRUSLEN MOD GRØNLAND OG FÆRØERNE

Vurderingen af terrortruslen mod Danmark er som udgangspunkt gældende for hele rigsfællesskabet, men der er en række særlige forhold, som gør sig gældende i Grønland og på Færøerne.

CTA vurderer, at der også er personer i Grønland og på Færøerne, der kan blive inspirerede af propaganda eller gennemførte terrorangreb i andre vestlige lande. Ud over personer med sympati for militant islamisme kan dette påvirke andre, f.eks. psykisk ustabile personer, til at begå en ideologisk motiveret voldshandling, der kan karakteriseres som terror. Sociale medier anvendes også i Grønland og på Færøerne til at fremsætte truende og fjendtlige bemærkninger. Hovedparten af disse ytringer fører sjældent til konkret angrebsplanlægning, men de kan påvirke visse psykisk uligevægtige eller meget påvirkelige personer til at begå ideologisk motiveret vold, der kan have karakter af terror.

CTA vurderer, at terrortruslen mod Grønland er begrænset. Det skyldes bl.a., at militant islamisme er mindre udbredt i Grønland end i Danmark. Militant islamistisk eller politisk ekstremistisk propaganda kan dog også påvirke personer i Grønland til at begå voldelige handlinger. Socialt marginaliserede og sårbare unge kan være særligt modtagelige over for radikalisering.

Den nemmere adgang til våben og sprængstoffer i Grønland sammenlignet med i det øvrige rigsfælleskab kan efter CTA's vurdering øge kapaciteten til at gennemføre terrorangreb med stor skadevoldende effekt.

CTA vurderer, at terrortruslen mod Færøerne er begrænset. Som på Grønland er militant islamisme generelt mindre udbredt på Færøerne end i Danmark.

Militant islamistisk eller politisk ekstremistisk propaganda kan påvirke personer på Færøerne eller tilrejsende til at begå voldelige handlinger, der kan karakteriseres som terror. Dette kan også være udløst af politiske enkeltsager som f.eks. dyrevelfærd.

Bilag 14

Retsudvalget 2019-20
REU Alm.del - Bilag 358
Offentligt

RIGSPOLITIET

POLITI

17. april 2020
J.nr.: 2020-033380

POLITIOMRÅDET

Redegørelse vedrørende politiets håndtering af signaleringsdata fra Telenor mv.

Indhold

1. Indledning

1.1. Justitsministeriets bestilling

Justitsministeriet har den 30. januar 2020 anmodet Rigspolitiet – efter behov med inddragelse af Rigsadvokaten – om at redegøre for politiets håndtering af en sag, hvor et teleselskab (Telenor) i forbindelse med kendelser om levering af signaleringsdata til politiet ved en fejl har videregivet oplysninger om SMS-indhold og B-numre.

Justitsministeriet har i den forbindelse anmodet myndighederne om at redegøre for, om politiet i andre tilfælde i forbindelse med kendelser om edition mere systematisk har modtaget oplysninger fra teleselskaber, som må anses for omfattet af reglerne om indgreb i meddelelseshemmeligheden.

1.2. Rigspolitiets og Rigsadvokatens konklusioner på baggrund af sagen

Sagen handler i sit udgangspunkt om, at en teleudbyder fejlagtigt har udleveret teleoplysninger til politiet, som ikke har været omfattet af de underliggende retskendelser. Oplysningerne har kun i begrænset omfang været læsbare for efterforskerne, og de har i vidt omfang været uden efterforskningsmæssig betydning.

Det er ikke ualmindeligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning, eller at oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. Det kendes således fra en række andre områder. Politiet har dog omvendt et ansvar for som myndighed at reagere, hvis politiet bliver opmærksom på, at der på mere systematisk vis fejlagtigt indgår oplysninger i politiets efterforskning. Dette ansvar skærpes endvidere, når der er tale om oplysninger, som politiet almindeligvis kun har adgang til med retskendelse.

I den konkrete sag reagerede politiet og anklagemyndigheden, da man blev opmærksom på problemet. I første omgang var fokus imidlertid primært på at udvikle

en operativ løsning, og der gik derfor for lang tid, før Rigspolitiet rettede henvendelse til Telenor om problemet.

Som led i arbejdet med denne redegørelse er det afdækket, at også andre teleudbydere har udleveret flere oplysninger, end hvad der var omfattet af de konkrete retskendelser.

Det rejser en række spørgsmål i forhold til både teleloven og lovgivningen om databeskyttelse, at der fra teleudbydernes side er udleveret teleoplysninger til politiet, som ikke har været omfattet af de indhentede retskendelser. Disse spørgsmål – og de retssikkerhedsmæssige aspekter der kan være forbundet hermed – henhører imidlertid under de relevante ressortmyndigheder. Derimod er der ikke grundlag for at antage, at fejlagtigt udleverede oplysninger konkrete har været anvendt i straffesager på en måde, der giver anledning til retssikkerhedsmæssige betænkeligheder.

Fremadrettet er det vigtigt i samarbejde med telebranchen at få sikret, at der ikke videregives oplysninger fra teleudbyderne til politiet, som ikke må udleveres på en kendelse om edition. Det er herudover vigtigt at være opmærksom på, at det uanset iværksættelse af relevante tiltag til imødegåelse af uberettiget og/eller fejlagtige videregivelser er vanskeligt helt at gardere sig mod, at der kan opstå fejl i fremtiden.

Der er bl.a. i forlængelse af teledatasagen og denne sag dog iværksat en række tiltag, som efter Rigspolitiets og Rigsadvokatens opfattelse vil medvirke til at minimere denne risiko.

2. Lokaliseringsoplysninger og signaleringsdata

Allerede registrerede oplysninger om lokaliseringen af en tændt mobiltelefon er oplysninger om, hvilke telemaster en mobiltelefon er registreret på i et bestemt tidsrum. Disse oplysninger omhandler:

- lokaliseringsoplysninger hidrørende fra aktiv brug af telefonen til eksempelvis tale, sms og mms, som skal logges af teleudbyderne.
- lokaliseringsoplysninger hidrørende fra en tændt telefon, der ikke er i aktiv brug, men som kommunikerer sin position til mobilnetværket. Disse *skal* ikke logges af teleudbyderne, men *må* godt opbevares – i en begrænset periode – med henblik på eksempelvis fejlretning.

Allerede registrerede lokaliseringsoplysninger logges ikke i et ensartet format hos de enkelte teleudbydere, ligesom indholdet og detaljeringsgraden af oplysningerne er forskellig fra udbyder til udbyder.

Hvis politiet anmoder om udlevering af signaleringsdata, vil datasættene efter omstændighederne i praksis indeholde såvel oplysninger, der hidrører fra aktiv brug af telefonen, som oplysninger, der er genereret ved, at en tændt telefon kommunikerer sin position til mobilnetværket, jf. ovenfor. Det skyldes, at teleudbyderne ved deres registrering af disse oplysninger ikke skelner mellem aktiv og passiv kommunikation.

I det følgende anvendes betegnelsen ”signaleringsdata” som en generel betegnelse for de data, der er udleveret fra teleselskaberne på editionskendelse om udlevering af signaleringsdata. Som redegjort for i det følgende må ”signaleringsdata” dog ikke indeholde modpartsnumre, når udlevering til politiet alene er hjemlet ved en kendelse om edition.

2.1. Politiets anvendelse af signaleringsdata

Signaleringsdata er et relativt nyt efterforskningsmiddel, som må forventes at få stigende anvendelse fremadrettet, også fordi alle fire teleselskaber nu kan levere disse data. Signaleringsdata vil ofte have væsentlig værdi for politiets efterforskning af alvorlige strafbare forhold såsom manddrab, voldtægt mv., herunder til hurtigt at målrette efterforskningen mod en afgrænset personkreds og udelukke andre

fra efterforskningen. Endvidere kan signaleringsdata anvendes til at følge en mistænkts færden i et relevant tidsrum. Den efterforskningsmæssige merværdi af signaleringsdata set i forhold til andre tilgængelige oplysninger ligger i, at disse data (også) opsamles, selv om en person ikke anvender sin telefon til at foretage eller modtage opkald.

For nuværende er signaleringsdata fra nogle af teleselskaberne ikke umiddelbart læsbart, når politiet modtager data, og brugen heraf forudsætter derfor i visse tilfælde, at data bearbejdes af medarbejdere med særlige kompetencer.

2.2. Politiets rekvisition af signaleringsdata

Politikredsene indhenter typisk signaleringsdata via Rigspolitiets Telecenter ved fremsendelse af en anmodning til telecenteret med afgrænsning af et område eller med oplysning om et fokusnummer samt med oplysning om den relevante tidsperiode for dataudtrækket. Telecentret bestiller herefter data fra teleoperatøren. Indhentelse af signaleringsdata er et straffeprocessuelt tvangsindgreb, der er omfattet af retsplejelovens kapitel 74 om edition, og sker på baggrund af rettens kendelse eller på øjemedet efterfulgt af rettens kendelse, hvis det af efterforskningsmæssige grunde har været nødvendigt at iværksætte indgrebet straks.

Når telecentret modtager data fra teleoperatøren, videresender telecentret disse til politikredsen.

Telecentret foretager ingen behandling af de modtagne data.

Politikredsene kan også bestille signaleringsdata direkte hos teleudbyderen. Leverancen af signaleringsdata sker da typisk via telecentret, men det forekommer også, at data sendes direkte fra udbyderen til den rekvirerende politikreds.

Politikredsene afregner særskilt over for teleoperatørerne for hver rekvisition.

Teleudbyderne leverer signaleringsdata i forskellige formater. Data kan være opdelt i flere forskellige filer, ligesom der er forskel på det data, der leveres fra de forskellige teleudbydere. Politikredsene vil derfor som nævnt have behov for at oversætte og/eller strukturere data, før de kan anvendes i efterforskningen.

3. Det retlige grundlag

3.1. Oplysninger omfattet af indgreb i meddelelseshemmeligheden

Indgreb i meddelelseshemmeligheden er reguleret i retsplejelovens kapitel 71. Telefonaflytning er i § 780, stk. 1, nr. 1, defineret som at politiet kan aflytte telefonsamtaler eller anden tilsvarende telekommunikation. Endvidere er teleoplysning i § 780, stk. 1, nr. 3, defineret som oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat. Telefonaflytning omhandler indholdet af kommunikationen, mens teleoplysning omhandler oplysninger om, hvilke telefoner der sættes i forbindelse med andre bestemte telefoner.

Endelig er udvidet teleoplysning – også kaldet mastesug – i § 780, stk. 1, nr. 4, defineret som oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område, der sættes i forbindelse med andre telefoner eller kommunikationsapparater.

Fælles for disse indgreb i meddelelseshemmeligheden er, at der som udgangspunkt gælder et kriminalitetskrav på fængsel i 6 år eller derover, ligesom der er skærpede krav til indhentelse af udvidede teleoplysninger. Oplysningerne kan således ikke indhentes på en editionskendelse, jf. nedenfor.

3.2. Signaleringsdata mv.

Retsplejeloven indeholder ikke bestemmelser, der definerer allerede registrerede lokaliseringsoplysninger (herunder signaleringsdata), eller bestemmelser, der sær-

ligt regulerer politiets adgang til at indhente allerede registrerede lokaliseringsoplysninger. Den retlige ramme for indhentelse af disse oplysninger er derfor udviklet gennem retspraksis.

Det følger af Højesterets kendelse gengivet i UfR 2009.2610 H, at allerede registrerede lokaliseringsoplysninger fra en tændt mobiltelefon kan indhentes med hjemmel i retsplejelovens regler om edition, jf. § 806, stk. 2, jf. § 804, stk. 1. Det er i den forbindelse uden betydning, om lokaliseringsoplysningerne er blevet registreret i forbindelse med aktiv brug af en telefon, eller om de er genereret ved, at en tændt telefon (automatisk) har kommunikeret sin position til mobilnetværket. Herudover fremgår det af Østre Landsrets kendelse gengivet i UfR 2017.1934 Ø, at allerede registrerede lokaliseringsoplysninger tillige kan indhentes for masteceller, der dækker en bestemt adresse, dvs. alle de telefoner, som har kommunikeret med en bestemt mast.

Indhentelse af allerede registrerede lokaliseringsoplysninger kan på baggrund af retspraksis ske som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, jf. retsplejelovens § 806, stk. 2, jf. § 804, stk. 1. Derfor kan allerede registrerede lokaliseringsoplysninger også indhentes til brug for sager, hvor strafferammen er under 6 års fængsel.

Allerede registrerede lokaliseringsoplysninger og signaleringsdata omfatter forskelligt indhold på tværs af teleselskaberne. Begreberne allerede registrerede lokaliseringsoplysninger og signaleringsdata kan derfor næppe forstås helt entydigt. Da indhentning af disse typer af oplysninger begge er omfattet af samme hjemmel, findes en indbyrdes afgrænsning også at være af mindre betydning ud fra et straffeprocessuelt perspektiv.

Derimod giver en kendelse om udlevering af allerede registrerede lokaliseringsoplysninger, herunder signaleringsdata, alene politiet adgang til at få udleveret oplysninger om en telefons placering, men ikke til oplysninger om, hvilke telefoner mv.

der har været sat i forbindelse med telefonen – dvs. modpartsnumre – eller indhold af kommunikationen. Sådanne oplysninger er omfattet af meddelelseshemmeligheden og kræver derfor kendelse efter retsplejelovens kapitel 71, jf. også retsplejelovens § 801, stk. 3.

3.3. Signaleringsdata mv., der fejlagtigt er fremsendt til politiet

3.3.1. Den retlige ramme for teleudbydernes udlevering

Det følger af telelovens § 7, stk. 1, at ejere af elektroniske kommunikationsnet og udbydere af elektroniske kommunikationsnet eller -tjenester og deres ansatte og tidligere ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af elektroniske kommunikationsnet eller -tjenester.

Bestemmelsen er strafbelagt, jf. telelovens § 81, stk. 1, nr. 1.

Det fremgår af de specielle bemærkninger til den daværende telekonkurrencelovs § 13[1], der efterfølgende er videreført i den gældende telelovs § 7, at telekonkurrencelovens § 13, stk. 1 og 2, rettede sig mod opretholdelsen af "fortroligheden med hensyn til den trafik, der foregår via de pågældende telenet og teletjenester"[2]. Herudover indeholder bemærkningerne ikke bidrag til fortolkningen af, hvad der er

[1] Forslag til lov om konkurrence- og forbrugerforhold på telemarkedet som fremsat den 30. marts 2000 af forskningsministeren, Folketingstidende 1999-00, Tillæg A, 6896ff, hvor det bl.a. anføres, at "*af den gældende bestemmelse i § 3, stk. 1, nr. 5, i lov om visse forhold på telekommunikationsområdet fremgår, at forskningsministeren kan fastsætte nærmere regler for udbud af telenet eller teletjenester, med sigte på at sikre hemmeligholdelse af telekommunikation. Med hjemmel heri er det i den gældende bekendtgørelse om udbud af telenet og teletjenester fastsat, at udbyderen af et telenet eller en teletjeneste og dennes ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller om indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af telenet eller teletjenester.* [……]. *Den foreslåede bestemmelse er en lovfæstet videreførelse af den ovenfor beskrevne regulering med enkelte justeringer.*

[2] Telekonkurrencelovens § 13, stk. 3, retter sig mod forpligtelsen til at træffe de nødvendige foranstaltninger med henblik på at sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelige for uvedkommende. Denne forpligtelse ses videreført i telelovens § 7, stk. 1, sidste pkt.

omfattet af betegnelsen ”oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf”.

Ud fra bestemmelsens ordlyd må den dog anses for at omfatte oplysninger, der afdækker om f.eks. en tjeneste har været ”brugt” af en slutbruger og dermed også den umiddelbare oplysning om, hvorvidt andre (i praksis en slutbruger) har etableret adgang til et net eller tjeneste. For så vidt angår fortolkningen af begrebet ”oplysninger om indholdet heraf” må bestemmelsen anses for at beskytte oplysninger, der afdækker det egentlige indhold, der har været kommunikeret som led i en slutbrugers anvendelse af et net eller en tjeneste.

Bestemmelsen i telelovens § 7 implementerer artikel 5 om kommunikationshemmelighed i direktivet om databeskyttelse inden for elektronisk kommunikation[3]. Efter denne bestemmelse kan medlemsstaterne tillade indskrænkninger i kommunikationshemmeligheden i overensstemmelse med direktivets artikel 15, stk. 1. Artikel 15, stk. 1, tillader bl.a. indskrænkninger, der er nødvendige, passende og forholdsmæssige i et demokratisk samfund af hensyn til forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager. Retsplejelovens bestemmelser om indgreb i meddelelseshemmeligheden og edition udgør sådanne indskrænkninger. Enhver behandling – og hermed også videregivelse – af personoplysninger skal dog finde sted i overensstemmelse med de generelle databeskyttelsesretlige principper fastsat i databeskyttelsesforordningens artikel 5.

Oplysninger, der må anses for omfattet af begreberne ”andres brug af elektroniske kommunikationsnet og –tjenester eller indholdet heraf”, er således som udgangspunkt tavshedsbelagte, hvilket skal ses i sammenhæng med retten til kommunikationshemmelighed.

[3] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

Afgørende for, om en videregivelse af oplysninger omfattet af telelovens § 7, stk. 1, sker i overensstemmelse med bestemmelsen, er, om videregivelsen i den konkrete situation må betragtes som *berettiget*. En videregivelse må eksempelvis betragtes som berettiget, når den sker på baggrund af en kendelse efter retsplejelovens regler[4], f.eks. en kendelse om indgreb i meddelelseshemmeligheden eller edition.

Kendelsen – og det regelgrundlag, den er afsagt efter – udgør derved en konkret angivelse af, hvad der efter telelovens § 7, stk. 1, kan anses som en berettiget videregivelse af oplysninger om andres brug af elektroniske kommunikationsnet- og tjenester eller indholdet heraf. Modsætningsvist følger det, at en videregivelse af oplysninger, der omfatter andre oplysninger end fastsat i den givne kendelse, vil være uberettiget – medmindre, der kan peges på et andet retligt grundlag, som gør videregivelsen berettiget.

Er grundlaget for en konkret videregivelse et pålæg om edition, så medfører dette– foruden at gøre den konkrete videregivelse berettiget – at adressaten undergives en aktiv og domstolsbestemt[5] handlepligt til at fremkomme med de oplysninger, som pålægget omhandler.

Som nævnt skal den dataansvarlige teleudbyder altid iagttage de almindelige principper for behandling af personoplysninger i databeskyttelsesordningens[6] artikel 5, stk. 1, litra a – f. Ét af disse er dataminimeringsprincippet, jf. artikel 5, stk. 1, litra c,[7] hvorefter personoplysninger skal begrænses til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

---

[4] Se i den forbindelse Lasse Lund Madsen, Edition som efterforskningsmiddel, U.2017B.205, afsnit 4, for så vidt angår kendelser om edition.
[5] Herved adskiller pålæg om edition sig fra reglerne om indgreb i meddelelseshemmeligheden, hvor teleudbyderne er undergivet en lovgiverbestemt forpligtelse til at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 786, stk. 1.
[6] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
[7] Jf. bl.a. Datatilsynets afgørelse offentliggjort 11. februar 2019 om en teleudbyders efterlevelse af databeskyttelsesforordningens artikel 5, stk. 1, litra c (j.nr. 2018-31-0070).

3.3.1.1. Underretning om brud på persondatasikkerheden

Teleudbyderes underretning ved brud på persondatasikkerheden er reguleret i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation.

I medfør af forordningens artikel 2, stk. 1, skal udbyderen således underrette den kompetente nationale myndighed om samtlige brud på persondatasikkerheden. Den kompetente nationale myndighed er i denne sammenhæng Erhvervsstyrelsen. Hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal udbyderen foruden den underretning, der er nævnt i artikel 2, også underrette abonnenten eller den fysiske person om bruddet, jf. artikel 3, stk. 1.

Ved brud på persondatasikkerheden forstås "et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester i Fællesskabet.", jf. artikel 2, litra i, i direktivet om databeskyttelse inden for elektronisk kommunikation.

3.3.2. Regulering i forhold til straffesagen

Som nævnt i afsnit 3.2. giver en kendelse om udlevering af allerede registrerede lokaliseringsoplysninger (herunder signaleringsdata) alene politiet adgang til at få udleveret oplysninger om en telefons placering, men ikke til oplysninger om, hvilke telefoner mv. der har været sat i forbindelse med telefonen – dvs. modpartsnumre, eller indhold af kommunikationen. Sådanne oplysninger er omfattet af meddelelseshemmeligheden og kræver derfor kendelse efter retsplejelovens kapitel 71.

Retsplejelovens regler om tvangsindgreb indeholder ikke bestemmelser, der særligt regulerer det tilfælde, hvor en teleudbyder videregiver flere oplysninger til politiet, end en kendelse om edition omfatter. Spørgsmålet er herefter, hvilken praksis der gælder i relation til straffesagen, hvis en teleudbyder alligevel videregiver oplysningerne til politiet.

Retsplejeloven indeholder ikke en generel regel om bevisførelsen inden for strafferetsplejen, men den materielle sandheds princip og princippet om den fri bevisbedømmelse, jf. retsplejelovens § 880, 2. pkt., spiller en central rolle ved behandlingen af straffesager. Herudover regulerer retsplejelovens § 789 såkaldte tilfældighedsfund ved indgreb i meddelelseshemmeligheden og § 800 tilfældighedsfund i forbindelse med politiets ransagning, ligesom § 791, stk. 3, regulerer destruktion af materiale fra indgreb i meddelelseshemmeligheden hidrørende fra den mistænktes forbindelse med personer, som efter reglerne i retsplejelovens § 170 er udelukket fra at afgive forklaring som vidne. Endelig er der i retspraksis taget konkret stilling til anvendelse af beviser, som er ulovligt tilvejebragt.

Det er ikke ualmindeligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning, eller at sådanne oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. I nogle tilfælde får politiet f.eks. i forbindelse med et tvangsindgreb kendskab til oplysninger om lovovertrædelser, der ikke dannede eller kunne danne baggrund for indgrebet. Det kan f.eks. være tilfældet, hvis politiet under en aflytning får kendskab til en lovovertrædelse, som ikke lever op til strafferammekravet i § 781. Disse såkaldte tilfældighedsfund er reguleret i retsplejelovens § 789 og § 800.

Tilfældighedsfund kan anvendes som led i politiets videre efterforskning af den pågældende lovovertrædelse, jf. retsplejelovens § 789, stk. 1. De kan imidlertid ikke anvendes som bevis i retten, medmindre retten tillader det, jf. retsplejelovens § 789, stk. 3, og § 800, stk. 2.

Ønsker anklagemyndigheden at anvende et tilfældighedsfund som bevis, medtages det i bevisfortegnelsen under udtrykkelig angivelse af, at der er tale om et tilfældighedsfund. Herefter har forsvareren mulighed for at begære spørgsmålet forelagt for retten til afgørelse efter princippet i § 841, stk. 1, inden hovedforhandlingen.

Er der udover tilfældighedsfundet tillige tilvejebragt beviser for den oprindeligt angivne kriminalitet, der dannede grundlag for indgrebet, vil det normalt være ubetænkeligt at tillade anvendelsen af tilfældighedsfund som bevis. Se f.eks. Michael Kistrup m.fl., Straffeprocessen, 3. udgave.

Selvom reglerne om tilfældighedsfund ikke finder direkte anvendelse på den foreliggende situation, hvor en teleudbyder udleverer flere oplysninger til politiet, end der er omfattet af de kendelser, anklagemyndigheden har indhentet på vegne af politiet, bør samme fremgangsmåde som udgangspunkt følges, herunder for at sikre fuld transparens for rettens aktører.

Anklagemyndigheden bør derfor – i det omfang oplysningerne er læsbare og indgået i sagen – sikre, at oplysningernes tilvejebringelse tydeligt fremgår af sagen. På den måde sikres det, at forsvareren har adgang til alt materiale af relevans for sagen, jf. retsplejelovens § 729 a, stk. 3, og at retten – ud fra principperne om den materielle sandhed og den fri bevisbedømmelse – har mulighed for at tage stilling til oplysningernes eventuelle bevismæssige betydning.

I det omfang oplysningerne indgår i sagen, er de omfattet af de almindelige regler for straffesagers behandling, herunder reglerne for arkivering, destruktion mv.

4. Det tidsmæssige forløb og underretning af berørte registrerede

4.1. Det tidsmæssige forløb

Sagen, der gav anledning til nærværende redegørelse, vedrører signaleringsdata, der er videregivet til politiet fra Telenor.

4.1.1. september 2018 – april 2019

Politiet har haft mulighed for at rekvirere signaleringsdata fra Telenor siden september 2018, hvor Københavns Politi første gang modtog signaleringsdata fra Telenor. Signaleringsdata blev leveret i binære PCAP datafiler. Det vil sige, at data var i binær kode, som ikke kunne læses, medmindre data blev oversat maskinelt, da binær kode alene består af 1-taller og 0' er

Ifølge de foreliggende oplysninger modtog Københavns Politi, Afdelingen for efterforskningsstøtte – i en anden sag end den ovennævnte – signaleringsdata fra Telenor medio november 2018. For at læse data blev disse gjort læsbare med hjælp af et open source værktøj. Dermed kunne data læses, men det var delt på mange forskellige filer, og det var ikke muligt at få et systematisk overblik over data i et samlet billede. I forbindelse med arbejdet med at udfinde de relevante data som målpersonens telefonnummer, tid og sted blev man i december 2018 opmærksom på, at der i datafilerne fandtes såkaldte modpartsnumre (hvilket omfatter – men ikke er tilsvarende med – såkaldte B-numre), som er telefonnumre, som de omhandlede telefoner har haft kontakt med, ligesom der i enkelte tilfælde også var SMS-indhold. Såvel Rigspolitiet som den lokale anklagemyndighed blev informeret om dette af medarbejdere i Afdelingen for efterforskningsstøtte i december 2018, og anklagemyndigheden i Københavns Politi gjorde opmærksom på, at politiet ikke måtte hverken tilgå eller anvende disse oplysninger i sagsbehandlingen.

Da data, selv om det blev gjort læsbart, var meget vanskelig at få overblik over og anvende i praksis, besluttede Københavns Politi at udvikle et værktøj, der kunne oversætte og strukturere data fra Telenor til et format, som kunne anvendes i efterforskningen. I løbet af de første måneder af 2019 arbejdede politikredsen på udviklingen af dette værktøj. Til brug for dette modtog Københavns Politi signaleringsdatasæt, som andre politikredse havde indhentet fra Telenor. Københavns Politi konstaterede i den forbindelse, at der ikke var SMS-indhold i alle de datasæt, som blev modtaget fra andre politikredse, idet SMS-indhold øjensynligt var isoleret til en bestemt protokol, som ikke altid blev udleveret som en del af datasættet.

Rigspolitiet kontaktede primo marts 2019 Rigsadvokaten om problemstillingen. Det blev i den forbindelse aftalt, at Rigspolitiet skulle rette henvendelse til Telenor og underrette dem om, at selskabet i nogle tilfælde havde fremsendt indholdsdata på baggrund af en editionskendelse, og samtidig anmode Telenor om, at dette ikke skete fremover.

I lyset af de oplysninger, som Rigspolitiet modtog fra Københavns Politi i forbindelse med deres arbejde med signaleringsdata fra Telenor, kontaktede Rigspolitiet den 27. marts 2019 Telenors politigruppe[8]. Telenor blev gjort bekendt med, at det leverede signaleringsdata indeholdt mere data end omfattet af editionskendelserne, herunder at der var konstateret indholdsdata i det modtagne materiale. Idet Københavns Politi havde konstateret, at der var forskelligt indhold i datasættene fra Telenor, blev det ved henvendelsen endvidere drøftet, hvordan disse datasæt blev genereret af Telenor.

Ud fra de oplysninger Telenor har afgivet, undersøgte selskabet i den forbindelse deres systemer, men fandt ingen tegn på, at disse indeholdt mere information, end politiet havde anmodet om. Telenor har efterfølgende oplyst, at selskabet meddelte dette til Rigspolitiet, ligesom selskabet anmodede om at modtage den information, som selskabet fejlagtigt skulle have sendt, men at selskabet ikke på daværende tidspunkt hørte mere fra politiet.

Rigspolitiet har ikke kunnet identificere nogen henvendelser fra Telenor, men kan ikke udelukke, at dette har fundet sted.

Oversættelsesværktøjet var færdigudviklet primo april 2019 og blev gjort tilgængeligt for alle politikredsene i den første version den 3. april 2019. I denne version

[8] "Politigruppe" anvendes som betegnelse for de medarbejdere, der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

blev eventuel SMS-indhold i datasættet fra Telenor ikke vist i de læsbare data. I en senere version af oversættelsesværktøjet, som blev udsendt den 3. juli 2019, blev også oplysninger om modpartsnumre frasorteret i de læsbare data.

Det bemærkes, at Rigspolitiet den 5. februar 2020 afholdt et ITV-møde med lederne af kredsenes it-efterforskere og NC3 forposter[9] med henblik på at afdække, hvordan kredsene har behandlet signaleringsdata fra Telenor. Politikredsene og efterforskningsfællesskaberne oplyste, at de, siden oversættelsesværktøjet udviklet af Københavns Politi blev gjort tilgængeligt for kredsene, har anvendt dette værktøj til oversættelse af signaleringsdata fra Telenor. Enkelte politikredse havde i tiden forud herfor i enkelte sager anvendt andre værktøjer til læsning af data, men ved anvendelse af disse værktøjer var det ikke muligt at få et systematisk overblik over data.

4.1.2. maj 2019 – juli 2019

Rigspolitiet konstaterede ultimo maj 2019, at signaleringsdata fra Telenor fortsat indeholdt modpartsnumre og i visse tilfælde endvidere SMS-indhold, hvorfor det på et møde den 28. maj 2019 mellem Rigspolitiet og Rigsadvokaten blev aftalt, i) at Telenor på direktionsniveau skulle orienteres om problemstillingen og med henblik på, at fejlen blev rettet, ii) at det skulle sikres, at værktøjet, som Københavns Politi havde, udviklet effektivt "spærrede" for de oplysninger, som ikke var omfattet af kendelsen, og iii) at indhentning af signaleringsdata fortsat burde ske i form af editionskendelse.

Samme dag rettede Rigspolitiet telefonisk henvendelse til Telenors juridiske direktør og oplyste, at signaleringsdata i visse tilfælde indeholdt oplysninger om b-numre og egentlig indholdsdata (SMS-indhold). Det blev i den forbindelse oplyst, at Rigspolitiet den 27. marts 2019 orienterede Telenors politigruppe om ovenstående og drøftede de mulige årsager hertil. Det blev ved henvendelsen understreget over for

[9] IT-ingeniører, der organisatorisk er tilknyttet National Cybercrime Center, men som er stationeret i hver politikreds

Telenor, at Rigspolitiet så med stor alvor på sagen, og at Rigspolitiet ønskede problemstillingen adresseret fra Telenors side. Det blev samtidig bemærket, at det var vigtigt for politiet, at Telenor vedblev med at kunne udlevere de oplysninger, som politiet i overensstemmelse med gældende ret anmoder om at modtage.

Rigspolitiet orienterede den 29. maj 2019 telefonisk Telenors politigruppe om henvendelsen til selskabets juridiske direktør. Repræsentanten fra Telenors politigruppe oplyste i den forbindelse, at man både i forbindelse med Rigspolitiets henvendelse den 27. marts 2019 og i forbindelse med Rigspolitiets henvendelse af 28. maj 2019 havde undersøgt signaleringsdata, som Telenor havde sendt til politiet. Man havde ved de undersøgelser ikke kunnet konstatere tilfælde, hvor indholdsdata (SMS-indhold) var fremsendt til politiet, hvorfor Telenor gerne modtog eksempler på dette.

Det blev endvidere oplyst, at Telenor efter fast praksis slettede de datasæt, der blev udleveret til politiet efter afsendelsen, og at Telenor derfor ikke efterfølgende var i stand til at fastlægge hvilke oplysninger, der var blevet udleveret.

Telenor anførte samme forhold i en e-mail af 29. maj 2019 til Rigspolitiet og anmodede om at modtage et eksempel på signaleringsdata, som Telenor havde fremsendt til politiet. Telenor oplyste endvidere, at selskabet – både ved Rigspolitiets henvendelse i marts 2019 og henvendelse den 28. maj – havde undersøgt deres systemer. Selskabet fandt dog ikke tegn på, at der i de fremsendte datasæt var oplysninger om indhold af kommunikation, ligesom Telenor ved forskellige test ikke kunne konstatere, at der fremgik indholdsoplysninger i deres system.

Rigspolitiet iværksatte på den baggrund fremsøgningen af et sæt signaleringsdata modtaget fra Telenor med henblik på at kunne fremsende det til selskabet. Den 6. juni 2019 fremsendte Rigspolitiet herefter et eksempel på SMS-indhold, som var leveret i signaleringsdata til Københavns Politi i maj 2019. Ved fremsendelsen be-

mærkede Rigspolitiet over for Telenor, at Københavns Politi havde oplyst, at modpartens nummer altid er synligt for kald og SMS uafhængigt af den benyttede protokol.

Rigspolitiet anmodede i den forbindelse ved e-mail af samme dato om at blive orienteret, såfremt Telenor måtte konkludere, at der forelå et eller flere brud på persondatasikkerheden, som Telenor efter gældende ret havde pligt til at indberette til den relevante tilsynsmyndighed.

Telenor svarede ved e-mail af 7. juni 2019, at selskabet måtte konstatere, at eksemplet indeholdt SMS-indhold, og at man nu havde fundet fejlen i systemet. Telenor anførte i den forbindelse, at man havde iværksat udbedring af fejlen hurtigst muligt, og at man ville indberette forholdet til Erhvervsstyrelsen som et brud på persondatasikkerheden.

Rigspolitiet lagde på denne baggrund til grund, at forholdet knyttet til såvel udlevering af SMS-indhold som modpartsnumre ville blive løst af Telenor. Som beskrevet nedenfor blev Rigspolitiet først efterfølgende bekendt med, at Telenor ikke på dette tidspunkt havde fundet grundlag for at adressere problemstillingen knyttet til udlevering af modpartsnumre.

Det bemærkes, at Rigspolitiet som led i den e-mail korrespondance, der beskrives nedenfor under afsnit 4.2, ved e-mail af 30. januar 2020 anførte, at Rigspolitiet havde konstateret, at Telenor på dette tidspunkt regelmæssigt fortsat fremsendte signaleringsdata til politiet, der indeholdt oplysninger om B-numre. Rigspolitiet opfordrede derfor på ny Telenor til at søge dette forhold afhjulpet snarest muligt.

I perioden ultimo maj til medio juni 2019 var der løbende dialog mellem Rigspolitiet og Rigsadvokaten for at få afklaret, om SMS-indhold og modpartsnumrene var tilgængelige for politikredsene og indgik i straffesagerne, og om der var behov for udfærdigelse af retningslinjer i den anledning.

Som led i disse drøftelser fremsendte Rigspolitiet den 12. juni 2019 et notat til Rigsadvokaten, der beskrev Rigspolitiets kommunikation med flere politikredse og efterforskningsfællesskaberne Særlig Efterforskning Vest og Særlig Efterforskning Øst. Af notatet fremgik det bl.a., at der den 3. april 2019 blev uploadet et konverteringsprogram på teledata ERFA netværket[10], hvorefter samtlige teledataanalytikere havde adgang til at konvertere signaleringsdata fra Telenor til et læsbart excel-format. Det uploadede konverteringsprogram eksponerede imidlertid ikke eventuelt SMS-indhold.

Den 17. juni 2019 oplyste Rigspolitiet over for Rigsadvokaten, at Telenor havde rettet deres procedurer/software til, så der fremadrettet ikke ville indgå indhold eller modpartsnumre i materiale, som er rekvireret på baggrund af editionskendelser om signaleringsdata. Da problemstillingen var historisk, og da man på daværende tidspunkt vurderede, at der var tale om relativt få sager, vurderede Rigsadvokaten, at der ikke var grundlag for at udstede generelle retningslinjer, men at legalitetssikringen burde foretages af de lokale anklagemyndigheder i de enkelte sager.

Fejlen vedrørende SMS-indhold blev ud fra de foreliggende oplysninger først endeligt udbedret fra Telenors side den 20. juni 2019, således at politiet ikke længere modtog oplysninger herom.

4.1.3. august 2019 – december 2019

Den 2. august 2019 konstaterede Rigspolitiet, at signaleringsdata fra Telenor fortsat indeholdt oplysninger om modpartsnumre. Telenors politigruppe blev orienteret herom den 6. august 2019, og der blev på ny taget telefonisk kontakt herom til Telenors juridiske direktør, der blev anmodet om at søge forholdet løst. Telenor bemærkede i den forbindelse, at man gerne så, at politiet præciserede editionskendelserne, så det var mere entydigt, hvilke oplysninger de omfattede. Hertil bemærkede

[10] En fælles informationsplatform for teledataeksperter og sagsbehandlere i politiet.

Rigspolitiet, at det ikke virkede som en egnet løsning, idet dette bl.a. forudsatte, at Rigspolitiet udtømmende skulle opregne hvilke datafelter en given teleudbyder skulle udtrække fra netop dennes system. Endvidere tilkendegav Rigspolitiet, at spørgsmålet om, hvilke oplysninger der er omfattet af en editionskendelse, skulle søges afklaret på baggrund af retsplejelovens bestemmelser.

Ved e-mail af 8. august 2019 forespurgte Telenor, om man fra politiets side kunne præcisere, hvilken information, politiet har brug for, når politiet anmoder om "signaleringsdata". Telenor anførte bl.a. følgende i e-mailen:

> *"Desuden vil* [Telenor] *bede politiet sørge for en præcisering i de kendelser, som Telenor modtager fremover, således at kendelserne lyder på netop den data, som I har behov for (og grundlag for at indhente)."*
>
> *Således har vi fra Telenors side ikke lige nu en holdbar løsning og ej heller en hurtig løsning på at udlevere den fulde mængde signaleringsdata uden oplysninger om den modtagende eller afsendende part – og ud fra et juridisk synspunkt mener vi også at vi udleverer det, som vi får kendelser på – nemlig (al vores) signaleringsdata."*

Ved samme e-mail tilkendegav Telenor, at selskabet forstod problemstillingen med hensyn til oplysninger om den part, som havde været sat i forbindelse med personens telefon (dvs. den modtagende eller afsendende part, som ikke selv nødvendigvis har befundet sig i det pågældende område). Telenor anførte i den forbindelse følgende:

> *"Vi er enige i, at udlevering af denne information alene kan udleveres efter reglerne i Retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, hvilket også forudsætter en kendelse, om end kravene til at få en sådan kendelse er anderledes."*

I forlængelse heraf anførte Telenor, at denne information om modtagende/afsendende part er en dybt integreret del af signaleringsdata, som Telenor anvender til fejlretning i netværket, og at en anonymisering eller sletning af disse oplysninger vil være en meget omfattende opgave, som enten vil kræve systemudvikling for at lave en teknisk løsning eller et stort antal mandetimer for at lave en manuel anonymisering/sletning.

Rigspolitiet orienterede den 16. august 2019 Rigsadvokaten om Telenors anmodning og gjorde i den forbindelse opmærksom på, at håndteringen af problemstillingen burde afklares sammen med Rigsadvokaten. Samme dag bekræftede Rigspolitiet over for Telenor modtagelsen af anmodningen og anførte i den forbindelse, at Rigspolitiet i samarbejde med Rigsadvokaten ville afklare, hvordan problemstillingen mest hensigtsmæssigt håndteres og vende tilbage, så snart det var muligt.

Rigspolitiet lagde på baggrund af korrespondancen med Telenor umiddelbart til grund, at Telenor havde vurderet spørgsmålet nærmere og fundet, at selskabets *udlevering* af oplysninger om modpartsnumre kunne finde sted efter de retlige rammer, som Telenor er underlagt, uanset om politiet havde adgang til at *indhente* disse, jf. også afsnit 4.1.4. nedenfor.

I perioden fra primo til ultimo august 2019 var der løbende dialog mellem Rigspolitiet og Rigsadvokaten, idet politikredsene fortsat modtog oplysninger om modpartsnumre ved indhentelse af signaleringsdata fra Telenor.

Som led i heri rettede Rigspolitiet den 27. august 2019 henvendelse til Rigsadvokaten med henblik på fornyede drøftelser af behovet for udfærdigelse af de påtænkte retningslinjer.

Rigsadvokaten og Rigspolitiet drøftede i dagene herefter håndteringen af Telenors henvendelse. Der var både politiets og anklagemyndighedens opfattelse, at Telenor

var forpligtet til at sikre korrekt efterlevelse af en retskendelse om "signaleringsdata" uden en nærmere specificering af dataindholdet i kendelsen, ligesom udbyderen var forpligtet til at sikre, at den udleverede signaleringsdata ikke indeholdt teleoplysninger, hvis indhentning kræver kendelse om indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71. Endelig var der enighed om, at der allerede i den eksisterende ordning er indbygget en proportionalitetsvurdering, som påses af domstolene.

Rigspolitiet oplyste samtidig, at da spørgsmålet om, hvad der udgør "signaleringsdata", bør ses som et spørgsmål, der berører alle de teleudbydere, der indsamler disse data, bør spørgsmålet med fordel drøftes med alle de relevante teleudbyderene i fællesskab. Rigspolitiet fandt på den baggrund – og da der var etableret en teknisk løsning, der udeholdt modpartsnumre fra sagsbehandlingen – at emnet burde sættes på dagsordenen for et kommende møde med repræsentanter fra telebranchen.

Spørgsmålet om fortolkning af begrebet "signaleringsdata" har efterfølgende været genstand for såvel korrespondance og telefoniske drøftelser mellem Rigspolitiet, Rigsadvokaten og enkelte teleudbydere, jf. for Telenors vedkommende det under afsnit 4.1.4. nævnte brev af 7. februar 2020 Emnet blev endvidere drøftet på mødet i den juridiske arbejdsgruppe under Rigspolitiets Telebrancheforum den 9. marts 2020.

4.1.4. januar 2020 – nu

På baggrund af medieomtale af sagen i januar måned 2020 rettede Erhvervsstyrelsen som kompetent tilsynsmyndighed på teleområdet henvendelse til Telenor og anmodede om en redegørelse om forholdene knyttet til Telenors videregivelse af b-numre[11] til politiet.

[11] "B-numre"-ses i denne sammenhæng at blive benyttet som en alternativ betegnelse for modpartsnumre, som er oplysninger, om hvilke telefoner eller andre tilsvarende kommunikationsapparater, som en bestemt telefon eller andet kommunikationsapparat har været sat i forbindelse med.

Til brug for Erhvervsstyrelsens oplysning af sagen anførte Telenor ved e-mail af 29. januar 2020, at selskabet ikke mente, at der var tale om brud på persondatasikkerheden, når Telenor havde overført information om B-nummer som del af signaleringsdata, og at Telenor således ikke mente uretmæssigt at have oversendt personoplysninger til Rigspolitiet.

Telenor anførte endvidere, at da man havde udleveret det, som kendelserne har lydt på indtil videre, har man ikke betragtet forholdet som et brud, og af denne årsag havde man ikke underrettet Erhvervsstyrelsen.

Telenor afgav den 4. februar 2020 en supplerende redegørelse til Erhvervsstyrelsen. Telenor har i den forbindelse anført, at der i den konkrete sag ikke var tale om et sikkerhedsbrud, idet det ikke var en utilsigtet hændelse, der havde ført til videregivelse af oplysninger. Endvidere har Telenor anført, at baggrunden for Telenors udlevering af data har været, at Telenor var blevet forelagt dommerkendelser om udlevering af signaleringsdata, og at Telenor derfor havde vurderet at være retligt forpligtet til at udlevere de pågældende oplysninger til politiet i overensstemmelse med ordlyden af kendelserne.

I den supplerende redegørelse har Telenor nærmere anført følgende:

> *"Efter en fornyet vurdering er Telenor imidlertid blevet opmærksom på, at der muligvis har været tale om en overfortolkning af forpligtelsen til at udlevere data fra vores side."*

Hvis det på dækningsområdet for en telemast bliver registreret, at en bestemt telefon har påbegyndt et opkald, vil denne telefon i forhold til den konkrete kommunikation være A-nummeret, mens den modtagende telefon vil være B-nummeret. B-nummeret vil i den konkrete kommunikation således være modpartsnummeret.

I forlængelse heraf har Telenor anført, at det er selskabets klare opfattelse, at Telenor har været i god tro omkring udleveringen af oplysningerne, som Telenor begyndte at udlevere i form af signaleringsdata i september 2018.

Samtidig har Telenor anført følgende:

> *"Henset til sagens udvikling og Telenors fornyede vurdering har vi imidlertid nu set os nødsaget til at begrænse de datasæt, som vi leverer til politiet efter editionskendelse."*

Ved e-mails af 31. januar 2020 og 6. februar 2020 anmodede Erhvervsstyrelsen om Rigspolitiets bemærkninger til de ovenfor omtalte redegørelser fra Telenor til Erhvervsstyrelsen omkring videregivelsen af modpartsnumre.

Telenor anmodede ved brev af 7. februar 2020 om, at politi og anklagemyndighed fremover undgik at benytte både begrebet "signaleringsdata" og begrebet "ikke-logningspligtige lokaliseringsdata", men i stedet benyttede begreberne – både ved hastesikring og edition – a) "oplysning om registrerede lokaliseringsdata for [fokusnummer] i [tidsrum]" og b) "registrerede lokaliseringsdata om, hvilke mobiltelefoner eller andre tilsvarende mobile kommunikationsapparater, der er registreret anvendt på mobilmaster, der dækker [fokusområde] i [tidsrum]".

Telenor angav i den forbindelse, at hvis andre begreber end ovennævnte a) og b) anvendtes, og disse begreber ikke var entydige, tog man forbehold for, at begæringen om udlevering af data måtte afvises. Disse forhold har efterfølgende indgået i den samlede dialog med telebranchen om afklaring af terminologien vedrørende signaleringsdata mv., jf. afsnit 6.4. nedenfor.

Som baggrund for anmodningen henviste Telenor til, at selskabet kun havde mulighed for at levere udtræk, som omfatter alle typer lokaliseringsdata, eller udtræk, som kun omfatter logningspligtige lokaliseringsdata. Endvidere henvistes der til, at

ingen af de hidtidige anvendte begreber efter Telenors opfattelse var entydige, hvorfor det for Telenor var uklart, hvad selskabet ved kendelsen eller anmodningen skulle hastesikre og/eller udlevere til politiet, og at selskabet derfor ikke var sikker på at have den nødvendige behandlingshjemmel til at hastesikre og/eller udlevere data til politiet.

Rigspolitiet afgav den 26. februar 2020 – efter høring af Rigsadvokaten – sine bemærkninger til Erhvervsstyrelsen.

Rigspolitiet anførte bl.a., at efter Rigspolitiets opfattelse skal spørgsmålet om hvilke oplysninger en teleudbyder er forpligtet til at – og dermed entydigt må – udlevere på baggrund af en kendelse, afgøres ud fra en fortolkning af ordlyden af den bestemmelse i retsplejeloven, der hjemler kendelsen og relevant retspraksis mv., og ikke ud fra overvejelser knyttet til, hvordan én eller flere teleudbydere vælger at definere begrebet signaleringsdata som led i udbyderens virksomhed.

På denne baggrund og på baggrund af den retspraksis, der også er gengivet ovenfor under afsnit 3.2., kunne Rigspolitiet tilslutte sig Telenors supplerende redegørelse af 4. februar 2020, hvor Telenor bl.a. anfører, at man i den foreliggende sag muligvis har overfortolket forpligtelsen til at udlevere data til politiet.

Endvidere anførte Rigspolitiet, at den enkelte teleudbyder må anses for at have en selvstændig forpligtelse til at sikre, at alene de oplysninger, der er omfattet af editionskendelse udleveres på baggrund af en sådan kendelse, men at det på den anden side påhviler anklagemyndigheden i relevant og passende omfang at vejlede teleudbyderen om indholdet af retsplejeloven og den pågældende kendelse.

Erhvervsstyrelsen har på nuværende tidspunkt endnu ikke truffet afgørelse om styrelsens vurdering af de forhold, der behandles i de ovennævnte redegørelser fra Telenor.

4.1.4.1. Status i forhold til modtagelse af signaleringsdata

Telenor begyndte i primo februar 2020 at fremsende signaleringsdata i et nyt format, som ikke indeholder oplysninger om modpartsnumre, og som ikke kræver anvendelse af oversættelsesværktøjet for at gøre data læsbart.

Rigspolitiet har indledt dialog med Telenor om det nærmere indhold af oplysninger i det nye format. Rigspolitiets vil endvidere indlede drøftelser med de øvrige teleudbydere om det fremtidige indhold og format for signaleringsoplysninger, der sikrer en korrekt overholdelse af editionspålæg vedrørende signaleringsdata.

Rigspolitiets Telecenter har i perioden fra den 24. september 2018 til den 28. januar 2020 registreret 262 bestillinger på signaleringsdata fra Telenor. Rekvisitionerne vedrører 96 unikke journalnumre. Telenor har i et brev af 4. februar 2020 til Erhvervsstyrelsen oplyst, at selskabet i perioden fra september 2018 til den 4. februar 2020 har udleveret 224 datasæt til signaleringsdata efter editionskendelse. Af disse 224 datasæt har der i 61% af tilfældene også foreligget en kendelse på indgreb i meddelelseshemmeligheden, hvorfor der har været udleveret 87 datasæt alene på baggrund af edition.[12]

Det fremgår af de journalnumre, som er angivet ved bestillingerne af signaleringsdata fra Telenor, at data overvejende har været rekvireret til brug for efterforskning af meget alvorlig kriminalitet som sprængninger, drab, drabsforsøg, brandstiftelse, kvalificeret vold, trusler på livet, besiddelse af skydevåben på offentligt sted, røveri og narkotikaforbrydelser. Det indebærer, at der i mange af sagerne ud over signaleringsdata også vil have været mulighed for at foretage indgreb i meddelelseshemmeligheden. Telenor har som nævnt oplyst, at der i 61% af tilfældene også har foreligget en kendelse på indgreb i meddelelseshemmeligheden. Det fremgår også af

[12] Forskellen i antallet af bestillinger og antallet af udleveringer kan bl.a. skyldes, at politikredsen anmoder om sikring af data, der ikke længere er tilgængeligt i Telenors system, eller at politikredsen, efter at have fremsendt en anmodning om hastesikring, alligevel ikke har brug for de sikrede data.

journalnumrene, at der har været indhentet signaleringsdata i sager vedrørende indbrud, tyveri og hærværk, men i et betydeligt mindre omfang.

Rigspolitiet er ikke bekendt med det præcise antal datasæt, hvori der er indgået oplysninger om SMS-indhold, idet det udarbejdede oversættelsesværktøj netop havde til formål at frasortere sådanne oplysninger. Det ville kræve, at politiet fremfandt alle rådatasæt modtaget fra Telenor før d. 20. juni 2019 og oversatte disse på en sådan måde, at oplysninger om SMS-indhold *ikke* blev frasorteret. Politiet ville derved gøre sig bekendt med oplysninger, som politiet ikke har hjemmel til at behandle på baggrund af en editionskendelse.

4.2. Underretning af de berørte

Som nævnt ovenfor anførte Telenor i e-mail af 7. juni 2019, at man ville indberette forholdet til Erhvervsstyrelsen som et brud på persondatasikkerheden.

Det fremgår af Telenors indberetning af 7. juni 2019 til Erhvervsstyrelsen, at der ikke ville ske underretning af de berørte personer, idet man ikke længere havde datasættene og ikke kunne identificere personerne. Telenor ses at have tilkendegivet i indberetningen, at det ville være umuligt eller uforholdsmæssigt vanskeligt at underrette de berørte personer.

De berørte personer forstås i denne sammenhæng som de abonnenter eller fysiske personer, hvis oplysninger har været omfattet af et brud på persondatasikkerheden, f.eks. de personer, hvis SMS'er uberettiget er blevet videregivet.

Det kan i den forbindelse oplyses, at Telenor i starten af juli 2019 rettede telefonisk henvendelse til Rigspolitiet vedrørende Erhvervsstyrelsens håndtering af den anmeldelse om et brud på persondatasikkerheden, som Telenor havde indgivet til styrelsen. Telenor forespurgte i den forbindelse om en underretning af de berørte registrerede måtte antages at have konsekvenser for politiets efterforskning. Rigspoliti et oplyste, at dette ikke er et forhold, der kan afklares generelt, men altid vil bero

på en konkret vurdering af, bl.a. hvor fremskreden en given efterforskning er og hvilken rolle den enkelte person, som Telenor ønsker at underrette, har i sagen. Det blev i den forbindelse bemærket, at denne afklaring alene kan foretages ved, at der rettes en anmodning herom til den enkelte politikreds, der forestår efterforskningen.

Efter de for Rigspolitiet foreliggende oplysninger har Telenor ikke rettet henvendelse til politikredsene.

Erhvervsstyrelsen har i et brev af 6. februar 2020 til bl.a. Telenor og Rigspolitiet oplyst, at Erhvervsstyrelsen, omkring tidspunktet for indberetningen, ikke mente, at der var grundlag for at pålægge Telenor at underrette de berørte abonnenter eller personer om bruddet. Samtidig anbefalede Erhvervsstyrelsen, at Telenor kontaktede Rigspolitiet for at drøfte spørgsmålet om underretning.

Telenor har i e-mail af 28. januar 2020 til Rigspolitiet anført, at Telenor ved telefonsamtalen i juli 2019 omtalt ovenfor havde fået forståelsen af, at en underretning af de berørte individer generelt ville kunne obstruere politiets efterforskning. Telenor anførte endvidere, at selskabet ikke havde modtaget dette på skrift fra Rigspolitiet, og Telenor forstod efter en telefonsamtale med Rigspolitiet den 27. januar 2020, at dette skyldes en manglende formel anmodning fra Telenors side.

Telenor fremsatte den 28. januar 2020 en formel anmodning om Rigspolitiets stillingtagen til, hvorvidt der kunne ske underretning af de berørte under hensyn til politiets efterforskning, og om politiets bistand med at identificere de berørte, i det omfang underretning kunne finde sted.

Rigspolitiet besvarede henvendelsen ved den e-mail af 30. januar 2020, der er omtalt ovenfor under afsnit 4.1.2. ovenfor, og anførte, at man gerne bistod med at identificere de berørte personer i det omfang, det var muligt, og at Rigspolitiet havde iværksat undersøgelser med henblik på afdække om, og i givet fald, hvordan man kunne bistå.

Samtidig anførte Rigspolitiet, at det – uanset udfaldet af undersøgelsen – altid ville bero på en konkret vurdering, om hensynet til efterforskning tilsiger, at underretning ikke finder sted, herunder at der skulle iværksættes en høring af den enkelte politikreds for at afdække dette i forhold til hver enkelt sag.

Rigspolitiet anførte endvidere, at i det omfang, Rigspolitiet kunne tilvejebringe de relevante oplysninger, ville Rigspolitiet dog ikke kunne foretage en gennemgang af oplysningerne med henblik på at identificere de berørte personer, idet dette ville indebære en behandling af oplysninger, der ikke tilkom Rigspolitiet at forestå. I stedet ville Rigspolitiet kunne tilbagesende det fulde datasæt til Telenor med henblik på, at Telenor selv foretog den fornødne fremsøgning, underretning mv.

4.2.1. Erhvervsstyrelsens vurdering af Telenors pligt til at underrette berørte personer

Ved det ovennævnte brev af 6. februar 2020 orienterede Erhvervsstyrelsen om, at styrelsen som uafhængig teletilsynsmyndighed havde foretaget en fornyet vurdering af spørgsmålet om underretning. Det bemærkes, at Erhvervsstyrelsens vurdering kun relaterer sig til eventuelt SMS-indhold i signaleringsdata.

Erhvervsstyrelsen fastholdt på baggrund af en konkret vurdering af de forhold, der er angivet i artikel 3 i Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 sin opfattelse af, at styrelsen i henhold til forordningen ikke havde belæg for at meddele Telenor en pligt til at underrette de berørte. Samtidig fastholdt styrelsen sin opfordring til, at Telenor drøftede spørgsmålet om underretning med Rigspolitiet, herunder om efterforskningsmæssige hensyn talte mod underretning, såfremt Telenor ønskede at underrette de pågældende personer.

Erhvervsstyrelsen lagde i den forbindelse bl.a. vægt på, at videregivelsen er sket til det danske politi, som er den rette modtager, og som myndighed er vant til at håndtere private, fortrolige og følsomme oplysninger, og at der absolut ikke foreligger

risiko for, at bruddet kan medføre identitetstyveri eller svig, fysisk skade, psykologisk forstyrrelse, tort eller skade af omdømme.

Rigspolitiet bemærker, at det er Erhvervsstyrelsen, der som uafhængig teletilsynsmyndighed foretager den endelige vurdering af, hvorvidt en teleudbyder har en underretningspligt, og at denne pligt alene påhviler teleudbyderen, der har videregivet oplysningerne.

Som nævnt anmodede Erhvervsstyrelsen om Rigspolitiets bemærkninger til de ovenfor omtalte redegørelser fra Telenor om videregivelsen af modpartsnumre. Telenor gentog ved sin supplerende redegørelse af 4. februar 2020, at man ikke betragter videregivelsen af modpartsnumre som et brud på persondatasikkerheden efter Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013.

I sine bemærkninger den 26. februar 2020 til Erhvervsstyrelsen, jf. ovenfor under afsnit 4.1.4., anførte Rigspolitiet bl.a., at man ikke finder anledning til at afgive bemærkninger til Telenors redegørelse vedrørende spørgsmålet om, hvorvidt der konkret foreligger et brud på persondatasikkerheden, der udløser indberetningspligt, da afgørelsen af dette forhold ses at henhøre under Erhvervsstyrelsens ansvarsområde.

Erhvervsstyrelsen ses som nævnt endnu ikke at have truffet afgørelse om, hvorvidt videregivelsen af modpartsnumre er at betragte som et indberetningspligtig brud på persondatasikkerheden, og i givet fald om der skal ske underretning af de berørte.

Det bemærkes afslutningsvis, at Rigspolitiet ikke har pålagt eller på anden måde instrueret Telenor om at undlade at orientere de berørte registrerede om, at deres oplysninger har indgået i et brud på persondatasikkerheden hos Telenor. Rigspolitiet har imidlertid efter telefonisk forespørgsel fra Telenor oplyst, at Rigspolitiet på daværende tidspunkt (sommeren 2019) ville undtage oplysninger om, hvilken teleudbyder, der var omfattet af sagen, idet det på det tidspunkt ikke var alle udbydere,

der indsamlede signaleringsdata. Identifikationen af, hvilke teleudbydere der på tidspunktet konkret indsamlede signaleringsdata – og dermed også kunne pålægges at udlevere disse oplysninger til politiet – kunne således afsløre konkrete forhold om politiets efterforskningsteknikker, jf. offentlighedslovens § 33, nr. 1. Dette hensyn til politiets efterforskning er ikke længere aktuelt.

5. Andre tilfælde, hvor politiet har modtaget for mange eller forkerte oplysninger mv.

5.1. Modtagelse af oplysninger uden relevans for efterforskningen

Politiets efterforskning – særligt i de indledende stadier af efterforskningen – er ofte kendetegnet ved en meget bred indsamling af oplysninger, herunder oplysninger der umiddelbart eller over tid viser sig ikke at have betydning for sagen.

Det gør sig blandt andet gældende ved ransagning af telefoner og computere, hvor politiet indledningsvist sikrer al data på enheden for efterfølgende at analysere og sortere i data, således at det alene er de for sagen relevante oplysninger, der inddrages. Det resterende – og i den forstand irrelevante – data, bliver ikke inddraget i sagen.

Et andet eksempel er politiets ransagninger i sager vedrørende grov økonomisk kriminalitet, hvor politiet ofte beslaglægger et stort antal dokumenter og andre effekter, der umiddelbart kan være relevante for sagen, idet det ikke er praktisk muligt at gennemgå alle dokumenter mv. på lokationen for en given ransagning.

Endvidere kan politiet i forbindelse med en anmeldelse fra en borger eller virksomhed modtage store mængder oplysninger fra anmelderen, der ved en nærmere gennemgang viser sig ikke at være relevante for en strafferetlig vurdering.

Endelig kan politiet i forbindelse med indhentning af videoovervågning fra eksempelvis en dagligvarebutik i forbindelse med et anmeldelse om røveri – på grund af systemets tekniske opbygning – modtage en større mængde videomateriale end det,

der tidsmæssigt er relevant i forhold til røveriet. Det vil i det tilfælde alene være en del af videoovervågningen, der inddrages i sagen.

Det er således almindeligt, at politiet med eller uden kendelse kommer i besiddelse af flere oplysninger, end der er relevant for den konkrete efterforskning. For visse data – herunder data fra teleudbyderne – gør der sig imidlertid det særlige forhold gældende, at teleudbyderne muligt bryder persondatasikkerheden, når der udleveres flere data, end der er omfattet af rettens kendelse.

5.2. Modtagelse af modpartsnumre

Rigspolitiet har ikke tidligere været bekendt med andre systematiske fejl i de modtagne signaleringsdata end de for mange udleverede oplysninger i signaleringsdata fra Telenor. I forlængelse af det ITV-møde, som Rigspolitiet afholdt den 5. februar 2020 med lederne af kredsens it-efterforskere og NC3 forposter, jf. afsnit 4.1.1, rettede en af NC3 forposterne imidlertid henvendelse til Rigspolitiet og henledte opmærksomheden på, at den pågældende ved anden lejlighed havde konstateret, at der også fandtes modpartsnumre i signaleringsdata modtaget fra Telia. En efterfølgende analyse af tre tilfældigt udvalgte datasæt fra Telia, indhentet på baggrund af editionskendelser, viste, at der i 2 ud af de 3 datasæt forekom modpartsnumre.

5.2.1. Rigspolitiets stikprøve

På den baggrund har Rigspolitiet iværksat en stikprøvevis analyse af såvel *signaleringsdata* som *logningspligtige lokaliseringsdata* fra alle teleselskaberne. Denne stikprøve omfattede dog ikke modtaget signaleringsdata fra TDC, idet der på tidspunktet for analysen ikke var modtaget signaleringsdata fra TDC.

Rigspolitiet har dog efterfølgende undersøgt det signaleringsdata, der er modtaget fra TDC, og har ikke fundet indholdsdata i form af SMS og modpartsnumre i de i alt 3 leverede datasæt.

Stikprøven vedrørende signaleringsdata omfatter 29 datasæt fra Hi3G og Telia fra 2018-2019. Analysen viser, at der fandtes modpartsoplysninger i 10 datasæt fra Telia i perioden efter den 29. januar 2019. Der er således konstateret, at Telia i en kortere periode systematisk har udleveret modpartsoplysninger. Der blev ikke fundet modpartsoplysninger i data fra Telia fra 2018 eller i datasæt fra Hi3G. Der blev ikke fundet SMS-indhold i nogen af stikprøverne. I stikprøven for Telia blev der dog fundet information om, hvor mange tegn, der er blevet sendt i de enkelte SMS-beskeder.

På baggrund af stikprøverne rettede Rigspolitiet den 8. februar 2020 henvendelse til Telia og oplyste, at politiet havde konstateret, at der i signaleringsdata modtaget fra Telia var fundet oplysninger om modpartsnumre. Oplysningerne var del af et større ustruktureret datasæt og vanskelige at udfinde uden en særlig indsats. Rigspolitiet opfordrede Telia til hurtigst muligt at analysere de signaleringsdatasæt, Telia havde leveret til politiet med henblik på at afhjælpe ovenstående gennem en frasortering af de data, der ikke måtte udleveres.

Telia oplyste den 10. februar 2020, at selskabet allerede havde et funktionelt filter, som frasorterede modpartsnumre i data inden fremsendelse af signaleringsdata til politiet. Da Telia sletter filerne efter afsendelse til politiet, anmodede Telia politiet om at fremsende nogle yderligere oplysninger, så Telia kunne identificere de to nævnte sager og dernæst gennemgå datasættet med henblik på at afdække, om der var sket fejl i udleveringen.

Telia har den 18. februar 2020 over for Rigspolitiet oplyst, at de siden den 8. februar 2020 ikke har leveret oplysninger om modpartsnumre i deres signaleringsdata.

I februar 2020 gjorde en politikreds Rigspolitiet opmærksom på, at Hi3G i flere tilfælde havde afvist at udlevere signaleringsdata, hvis der i kendelsen var angivet et andet tidsinterval end hele klokketimer.

Rigspolitiet iværksatte på den baggrund yderligere undersøgelser af signaleringsdata fra Hi3G. Disse indledende undersøgelser viste, at Hi3G formentlig udleverede signaleringsdata for hele klokketimer, selv om rekvisitionen alene vedrørte en kortere tidsperiode. Dette skyldes formentlig, at Hi3G ikke havde teknisk mulighed for at levere signaleringsdata inden for en kortere og mere præcis angivelse end én klokketime. Der var endvidere indikation på, at Hi3G i den forbindelse havde udleveret for meget data i forhold til det i kendelsen anførte tidsinterval. Dette er dog ikke muligt at konkludere med sikkerhed, da Hi3G alene registrerer aktiviteterne i blokke af en times varighed.

Rigsadvokaten er orienteret om denne tekniske indretning i Hi3G's system, og Rigsadvokaten udsendte den 9. marts 2020 en instruks til politikredsene i forhold til fremtidige anmodninger om udlevering af signaleringsdata fra Hi3G. Heraf fremgår bl.a., at der ved indhentning af kendelser om udlevering af signaliseringsdata fra Hi3G i medfør af retsplejelovens § 804, stk. 1, både skal fremgå, hvilken periode der er relevant for efterforskningen, og hvilken periode Hi3G vurderes i stand til at levere. Dermed kan begge oplysninger indgå i rettens vurdering af, om editionsbetingelserne er opfyldt. Samtidig henledte Rigsadvokaten opmærksomheden på, at fejlagtigt modtagne oplysninger som udgangspunkt skal håndteres efter principperne om tilfældighedsfund for at sikre fuld transparens for straffesagens aktører.

5.2.1.1. Stikprøve i logningspligtige lokaliseringsdata

For så vidt angår stikprøven i *logningspligtige lokaliseringsdata* (dvs. eksklusiv signaleringsdata) – i daglig tale omtalt som historiske masteoplysninger – omfattede denne i alt 131 datasæt fra alle teleudbyderne i perioden 2013-2020. Analysen viste, at der fandtes modpartsoplysninger i 11 datasæt fra HiG3. Stikprøven vedrørende Hi3G omfattede 42 datasæt fordelt på perioden 2013-2020. De 11 datasæt med modpartsoplysninger fordelte sig med 1-2 datasæt på alle årene undtagen 2013 og 2016.

Det er på baggrund af stikprøven ikke muligt at konkludere, at der skulle være tale om en systematisk fejl hos Hi3G. Rigspolitiet har underrettet Hi3G om resultatet af undersøgelsen.

Rigspolitiets har endvidere på anmodning fra Hi3G – og efter aftale med Rigsadvokaten – den 2. marts 2020 præciseret over for Hi3G, at indholdsoplysninger og modpartsoplysninger ikke må indgå i historiske masteoplysninger.

Der fandtes ikke modpartsoplysninger i stikprøverne vedrørende logningspligtige lokaliseringsdata fra de øvrige udbydere.

5.3. Uberettiget udlevering af andre oplysninger fra teleudbyderne

Som illustreret af de ovenstående eksempler vedrørende lokaliseringsdata, herunder signaleringsdata, forekommer der ved udlevering og modtagelse af data fra teleudbyderne såvel systematiske og mere enkeltstående fejl.

Som yderligere eksempel på mere enkeltstående fejl – der ikke vedrører allerede registrerede lokaliseringsdata – kan nævnes fire indberetninger fra TDC til Erhvervsstyrelsen. De tre indberetninger omfatter udlevering af data for længere tidsrum end, hvad der er anmodet om. Kendelserne lyder på bestemte tidspunkter, mens data udleveres for 2 minutters intervaller. Den fjerde indberetning omfatter udlevering af data for et forkert tidspunkt i forhold til det tidspunkt, som er angivet i kendelsen.

Det fremgår af de foreliggende oplysninger fra TDC, at der er tale om enkeltstående fejl.

Hvis sådanne fejl bliver opdaget umiddelbart – primært af teleudbyderen – bliver det efter politiets erfaring rettet ved fremsendelse af nye data. Teleudbyderen har i sådanne situationer anmodet om, at filerne med de forkerte data slettes med det samme, samt at fremsendelsen af data til rekvirenten stoppes. I de tilfælde, hvor

data allerede er fremsendt til rekvirenten, er det normal fremgangsmåde, at telecenteret kontakter rekvirenten og oplyser, at der er afsendt forkerte data, hvorfor datasættet skal slettes. Nyt data med korrekt indhold bliver eftersendt umiddelbart, og dermed inden sletning finder sted hos teleudbyderen.

6. Vurdering og fremadrettede overvejelser

Som redegørelsen viser, har teleudbydere i en række tilfælde fejlagtigt udleveret teleoplysninger til politiet, som politiet ikke har anmodet om, og som ikke har været omfattet af de retskendelser, der har været indhentet i sagen. Oplysningerne har kun i begrænset omfang været læsbare for efterforskerne, og de har i vidt omfang været uden efterforskningsmæssig betydning. Der kan dog i det fejlagtigt udleverede materiale have været oplysninger, som politiet har kunnet anvende i efterforskningen.

Der har hovedsageligt været tale om ikke-logningspligtige data, som teleudbyderne logger med henblik på fejlretning, og dialogen med teleudbyderne peger på, at det kan have spillet ind, at der blandt teleudbyderne har været usikkerhed om, hvilke oplysninger der er omfattet af begrebet "signaleringsdata", jf. afsnit 4.1.3. og 4.1.4. ovenfor.

Som beskrevet i afsnit 5.1. er det ikke usædvanligt, at politiet i forbindelse med en efterforskning kommer i besiddelse af "for mange" oplysninger. Det er heller ikke ukendt, at oplysninger kan indgå i en efterforskning ved en fejl eller tilfældighed. Blandt andet er bestemmelserne i retsplejeloven, som er beskrevet i afsnit 3.3.2., og fremgangsmåderne, herunder i telecentret, som beskrevet i afsnit 5.3., et udtryk for, at sådanne situationer jævnligt vil opstå og herefter skulle håndteres i forbindelse med sagens videre behandling.

Uanset at det ikke er usædvanligt, at politiet i forbindelse med efterforskning kan kommer i besiddelse af "for mange" oplysninger, har politiet et ansvar for som myndighed at reagere, hvis man bliver opmærksom på, at der på mere systematisk vis fejlagtigt indgår oplysninger i politiets efterforskning. Dette ansvar skærpes

endvidere, når der er tale om oplysninger, som politiet almindeligvis kun har adgang til med retskendelse.

6.1. Politiets og anklagemyndighedens håndtering af sagen

Som beskrevet i afsnit 4.1.1. blev Københavns Politi Afdelingen for efterforskningsstøtte, i første omgang opmærksom på problemstillingen vedrørende SMS-data og modpartsnumre indeholdt i binære PCAP datafiler med signaleringsdata fra Telenor ultimo 2018.

Anklagemyndigheden i Københavns Politi gjorde i den forbindelse opmærksom på, at politiet ikke måtte tilgå eller anvende disse oplysninger i sagsbehandlingen.

Københavns Politi iværksatte herefter et arbejde med at udvikle et oversættelsesværktøj, der kunne oversætte og strukturere data fra Telenor til et format, som kunne anvendes i efterforskningen. Rigspolitiet havde via National Efterforskningsafdeling indsigt i udviklingen af oversættelsesværktøjet og den bagvedliggende problemstilling, og søgte i samarbejde med Københavns Politi at afdække, hvorvidt der var tale om en systematisk fejl.

Selv om politiet og anklagemyndigheden reagerede med det samme – og fra starten var opmærksom på, at der var tale om oplysninger, som politiet ikke burde have modtaget – peger forløbet på, at fokus i den indledende fase i høj grad var på at udvikle en operativ løsning i form af et oversættelsesværktøj, som kunne gøre signaleringsdata fra Telenor egnet til brug for efterforskerne og samtidig fjerne SMS-indhold.

Det var først den 27. marts 2019, at Rigspolitiet tog kontakt til Telenors politigruppe og henledte opmærksomheden på, at signaleringsdata fra Telenor indeholdt oplysninger, som ikke var omfattet af de bagvedliggende retskendelser.

Rigspolitiet har ikke kunne fastslå, om der fra politiets side blev fulgt op på denne orientering før i slutningen af maj, hvor Rigspolitiet – efter dialog med Rigsadvokaten – tog kontakt til Telenors juridiske direktør og påpegede, at politiet fortsat modtog for meget data. Det førte til, at Telenor iværksatte en fejlretning af systemet.

Det må i lyset af ovenstående konstateres, at der samlet set gik for lang tid, før Rigspolitiet rettede henvendelse til Telenor og fejlretning blev iværksat, og at der fra Rigspolitiets side mere aktivt burde have været fulgt op i forhold til teleudbyderen for at sikre, at fejlen rent faktisk var rettet.

Tilsvarende burde der – uanset at det i den indledende fase ikke stod klart for politiet, at der var tale om et mere systematisk problem – på et tidligere tidspunkt være tilvejebragt et samlet overblik over problemstillingens omfang og karakter.

Det manglende overblik fik bl.a. betydning for anklagemyndighedens håndtering af sagen, idet Rigsadvokaten i sommeren 2019 fik indtryk af, at problemstillingen var løst og derfor ikke fandt behov for at udstede generelle retningslinjer på området, hvilket ellers havde været ønskeligt.

6.2. Særligt om redegørelsen om teledatasagen

Rigspolitiet og Rigsadvokaten afgav den 28. september 2019 en redegørelse om den såkaldte "teledatasag". Sagen handlede om systematiske fejl i telecentrets behandling af teledata, samt konstateringen af fejl i (ubearbejdet) teledata, med en deraf følgende frygt for, at teledata gennem en længere årrække havde været ufuldstændige, forvanskede, fejlbehæftede eller vildledende. Formålet med redegørelsen var at beskrive disse fejl og deres mulige konsekvenser for verserende og afsluttede straffesager.

Da problemstillingen om SMS-indhold og modpartsoplysninger i Telenors data ikke omhandlede fejl i teledata – og ikke rejste spørgsmål om mulige fejlagtige afgørelser i straffesager – var der ikke overvejelser om at omtale problemstillingen

nærmere i redegørelsen. Det fremgik dog af redegørelsen, at signaleringsdata kunne være ufuldstændige i lighed med fejlkonverteret data, jf. bl.a. punkt 2.3.1 og 6.2.4.4 i redegørelsen.

6.3. Retssikkerhedsmæssige overvejelser

Spørgsmålet om, hvorvidt teleudbyderne – ved at udlevere oplysninger til politiet som ikke har været omfattet af retskendelsen – har overtrådt teleloven og lovgivningen om databeskyttelse, og de retssikkerhedsmæssige aspekter, det i givet fald rejser, falder uden for denne redegørelse.

Som anført i afsnit 6.1. ovenfor burde der efter Rigspolitiets opfattelse tidligere have været rettet henvendelse fra Rigspolitiet til Telenor og være skabt overblik over problemstillingens omfang og karakter.

Uanset at forløbet således burde have være håndteret bedre, er der efter Rigspolitiet og Rigsadvokatens vurdering ikke grundlag for at antage, at fejlagtigt udleverede oplysninger konkret har været anvendt i straffesager på en måde, der giver anledning til retssikkerhedsmæssige betænkeligheder.

Som beskrevet i afsnit 6 har der været tale om oplysninger, som politiet ikke selv har anmodet om, og som i vidt omfang har været uden nogen efterforskningsmæssig relevans. Af samme grund vurderes sandsynligheden for, at oplysningerne senere er blevet anvendt som bevis i forbindelse med en straffesag ikke at være særlig stor.

Skulle der være forekommet tilfælde, hvor fejlagtigt udleveret oplysninger er indgået som et blandt flere beviser i en straffesag, vil der ikke tale om forkerte eller fejlbehæftede oplysninger. Der er vil derfor ikke være risiko for, at nogen er dømt eller frifundet på et forkert grundlag.

Det vil i givet fald være fremgået af sagen, hvorfra oplysningerne stammede, ligesom den relevante retskendelse vil være del af sagens materiale. Sagens aktører –

herunder forsvareren – vil derfor have haft mulighed for at rejse indsigelse mod, at oplysningerne blev anvendt i sagen. Det vil i sidst ende altid være rettens vurdering, i hvilket omfang oplysningerne ville kunne indgå og tillægges bevismæssig betydning i den konkrete sag, jf. afsnit 3.3.2. ovenfor om den frie bevisbedømmelse.

6.4. Fremadrettede initiativer

Fremadrettet er det først og fremmest vigtigt, at teleudbyderne sikrer, at der ikke videregives oplysninger fra teleudbyderne til politiet, som ikke må udleveres på en kendelse om edition.

I den forbindelse bemærkes, at der er indledt et samarbejde mellem Rigspolitiet, Rigsadvokaten og teleudbyderne med henblik på at understøtte dialogen om de praktiske, tekniske og juridiske aspekter af den daglige drift mv. samt informationsudveksling om fremtidige praktiske og tekniske tiltag.

Det er herudover vigtigt at være opmærksom på, at det uanset iværksættelse af relevante tiltag til imødegåelse af uberettigede og/eller fejlagtige videregivelser er vanskeligt helt at gardere sig mod, at tilsvarende situationer kan opstå i fremtiden, og at det således også fremover vil kunne forekomme, at politiet modtager oplysninger utilsigtet.

Der er i forlængelse af teledatasagen og denne sag dog iværksat en række tiltag, som efter Rigspolitiets og Rigsadvokatens opfattelse vil medvirke til at minimere denne risiko. Det drejer sig om:

- Et nyt uafhængigt tilsyn med brugen af tekniske efterforskningsmidler og beviser.

- Certificering og akkreditering af telecentrets kvalitetskontroller.

- Telecentret styrkes med flere og specialiserede kompetencer.

- Et nyt samarbejdsforum mellem politiet og telebranchen skal sikre en systematisk dialog såvel på direktørniveau som operationelt (juridisk og teknisk).

- Målrettet uddannelse og kompetenceudvikling for brugere af teledata, dvs. efterforskere, analytikere og anklagere.

- Nye retningslinjer for sletning og kontrol med at reglerne overholdes.

Rigspolitiet og Rigsadvokaten har derudover i forlængelse af teledatasagen udarbejdet nye retningslinjer og vejledninger om anvendelse og præsentation af teledata, så de afspejler de usikkerheder, der er nævnt i det uvildige notat, ligesom de indeholder nationale retningslinjer for politikredsenes håndtering og kvalitetssikring af teledata.

En forudsætning for, at lokaliseringsdata, herunder signaleringsdata også kan blive fuldt omfattet af de mange nye initiativer på området, er, at ansvaret for disse data bliver forankret i Telecentret. Hidtil har Telecentret ikke haft anden rolle i forhold til signaleringsdata end bestilling, modtagelse og videreformidling, og dette har ikke nødvendigvis omfattet alle leveringer. Der foregår ingen behandling af signaleringsdata i Telecentret, men centret skal fremadrettet have en mere retningssættende rolle i udvikling, brug, kvalitetskontrol og godkendelse af værktøjer, som politikredsene anvender til oversættelse, analyse og systematisering af data, ligesom indhentning af signaleringsdata bliver integreret i Telecentrets rekvisitionssystem. Telecentret kan i den sammenhæng have behov for at trække på kompetencer fra andre enheder i Rigspolitiet, herunder særligt Nationalt Cybercrime Center, men bør på sigt, i takt med at styrkelsen af Telecentret bliver udmøntet, selv opbygge de nødvendige kompetencer til opgaven.

Herudover er det i forbindelse med regeringens udspil om tryghed og sikkerhed den 10. oktober 2019 besluttet at lave et grundigt og omfattende arbejde med modernisering af retsplejelovens regler om tvangsindgreb. Arbejdet forankres i Strafferetsplejeudvalget, der skal komme med et bud på ny lovgivning. Det er Rigsadvokatens forventning, at resultatet af dette arbejde vil kunne lede til klarere regler og dermed mindre usikkerhed om indholdet af afsagte kendelser.

Det kan tilføjes, at der allerede nu i arbejdsforummet mellem politiet og telebranchen er iværksat et arbejde med afklare af terminologien vedrørende signaleringsdata mv. og på den baggrund opdatere Deloittes notat vedrørende anvendelse af historiske teledata i straffesager (den såkaldte "varedeklaration" som anvendes i straffesager).

Trusselsvurdering 2020:

Cybertruslen mod Danmark

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave juni 2020.

Cybertruslen mod Danmark

Denne vurdering informerer beslutningstagere i myndigheder og virksomheder samt offentligheden om cybertruslen mod Danmark. Viden om truslen kan bl.a. bruges til at prioritere tiltag for at forbedre cybersikkerheden og beredskabet hos den enkelte myndighed og virksomhed såvel som for Danmark som helhed.

Hovedvurdering

- Cybertruslen er en alvorlig trussel mod Danmark. Cyberangreb har især økonomiske og politiske konsekvenser.
- Hackere har forsøgt at udnytte COVID-19-pandemien til deres fordel. Det udgør et nyt element i det samlede trusselsbillede.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Truslen er rettet mod alle. Der er en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder.
- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder, der besidder en viden, som andre stater har interesse i.
- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater vil udføre destruktive cyberangreb mod Danmark. Virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, er mere udsatte for truslen
- Truslen fra cyberaktivisme er **LAV**. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, og cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder.
- Truslen fra cyberterror er **INGEN**. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt begrænset.
- Den teknologiske udvikling, herunder udviklingen af kunstig intelligens og kvanteteknologi, skaber både nye muligheder og udfordringer for cybersikkerheden.

Analyse

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgiver for femte gang den årlige vurdering af cybertruslen mod Danmark. Cyberangreb bruges af forskellige aktører og skal derfor opfylde forskellige formål.

Vurderingen af cybertruslen er som i tidligere år opdelt i trusler fra cyberangreb, der understøtter kriminalitet, spionage, aktivisme og terrorisme samt destruktive cyberangreb. Truslen fra destruktive cyberangreb har i år for første gang fået et trusselsniveau i erkendelsen af, at destruktive cyberangreb ikke kun er en angrebsmetode, men også kan være et selvstændigt formål.

Truslen fra cyberspionage og cyberkriminalitet er fortsat **MEGET HØJ**. Cybertruslen er derfor fortsat en alvorlig trussel mod Danmark, og det vil den blive ved med at være i fremtiden i takt med den fortsatte digitalisering og afhængighed af digitale tjenester.

CFCS har siden sidst ændret to af trusselsniveauerne. Cyberaktivisme er sat ned til **LAV** fra **MIDDEL**, og cyberterror er sat ned til **INGEN** fra **LAV**. Det sker som konsekvens af en faldende trussel fra begge typer cyberangreb, som beskrevet senere i vurderingen.

I 2020'erne kan nye teknologier såsom kvanteteknologi og kunstig intelligens skubbe udviklingen af cybertruslen og cybersikkerhed i nye retninger på både godt og ondt. Begge teknologier er fokus for dette års tendensanalyse sidst i vurderingen.

Cybertruslen under COVID-19-pandemien

Digitaliseringen har været med til at modvirke konsekvenserne af den sundhedsfaglige krise i forbindelse med COVID-19-pandemien. Behovet for at holde fysisk afstand er bl.a. blevet understøttet af større brug af hjemmearbejde, online møder, hjemmeskoling, sociale medier og ibrugtagningen af nye teknologier og platforme.

Ændringerne har samtidigt vist vores afhængighed af disse digitale løsninger, herunder af deres integritet, fortrolighed og tilgængelighed. Det har medført et øget fokus på cybersikkerheden hos mange myndigheder og virksomheder.

Der er altid hackere, der forsøger at udnytte aktuelle begivenheder, udviklinger eller vilkår til deres fordel. Det er også tilfældet med COVID-19-pandemien, som både fremmede stater og cyberkriminelle har udnyttet ved bl.a. at sende phishing-mails med COVID-19 som tema.

Udnyttelsen af COVID-19 udgør et nyt element i det samlede trusselsbillede, men udnyttelsen af pandemien har i sig selv ikke ændret den generelle trussel væsentligt. Udnyttelsen af COVID-19 har således primært påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger. Hovedparten af denne vurdering har derfor fokus på mange andre forhold af betydning for cybertruslen end COVID-19.

Myndigheder og virksomheder kan være mere sårbare under kriser som den igangværende COVID-19-pandemi. It-sikkerheden i mange myndigheders og

virksomheders netværk er under pres fra det ændrede brugsmønster i form af nye hjemmearbejdspladser, og fordi tilgængeligheden af systemerne prioriteres højt.

De ændrede arbejdsvilkår kan give hackere lettere adgang til organisationernes systemer og gøre det sværere at opdage hackerne. Selvom trusselbilledet grundlæggende er uændret, kan myndigheder og virksomheder derfor stå overfor et ændret risikobillede.

Hackere misbruger COVID-19 som tema
CFCS har viden om, at der under COVID-19-pandemien bliver sendt flere phishing-mails til danske myndigheder og virksomheder end normalt. Flere sikkerhedsfirmaer rapporterer også om en stigning i phishing i andre lande siden marts.

Mange af disse phishing-mails misbruger COVID-19 som tema for at øge sandsynligheden for, at modtageren læser mailen og klikker på links eller vedhæftede filer. Hackerne forsøger dermed at udnytte danskernes efterspørgsel på viden om COVID-19 og den nuværende sundhedskrise.

CFCS vurderer, at kriminelle fremadrettet også vil forsøge at udnytte statslige kompensationsordninger som tema i deres phishing-mails.

Under COVID-19-pandemien er der blevet oprettet en relativt stor mængde falske hjemmesider, som bl.a. udnyttes af hackere til at forsøge at franarre danske borgere deres NEMID-oplysninger og andre loginoplysninger. En del af hjemmesidernes domæner lægger sig tæt op ad legitime sundhedsmyndigheders hjemmesider og navne. CFCS samarbejder med andre partnere på at få nedtaget erkendte falske domæner.

Der er desuden set falske applikationer og malware rettet mod mobile enheder, som udnytter COVID-19 som tema. De falske apps kan eksempelvis stjæle informationer fra den mobile enhed.

CFCS vurderer, at hackere under COVID-19-pandemien forsøger at udnytte, at der er et øget behov for fjernadgange, VPN-løsninger samt samarbejds- og kommunikationsplatforme.

Cybertruslen ved overgangen til et nyt årti
Cybertruslen er ikke kun påvirket af aktuelle forhold som COVID-19 men er et resultat af den langsigtede udvikling af hvordan cyberangreb anvendes af såvel stater som ikke-statslige aktører. Med overgangen til et nyt årti er det oplagt at gøre status på udviklingen i cybertruslen i løbet af de seneste år.

Cyberangreb har fortsat hovedsaligt økonomiske og politiske konsekvenser. Der er endnu ikke tale om en generel trussel mod liv og helbred i modsætning til truslen fra eksempelvis krig og terrorisme. Enkeltstående eksempler på cyberangreb med fysisk skadevirkning og konsekvenser ved bl.a. ransomware-angreb mod hospitaler viser

dog, at cyberangreb også udgør en potentiel trussel mod liv og helbred. Med den fortsatte digitalisering af samfundsvigtige funktioner vil cyberangreb i stigende grad kunne få alvorlige konsekvenser i den fysiske verden.

Nogle stater, især Rusland og Kina, bruger cyberspionage meget aktivt og der er ingen tegn på, at truslen fra disse stater vil aftage. Der har i de seneste år været en stigning i antallet af lande, især i Asien, der bruger cyberspionage. Destruktive cyberangreb er med enkelte undtagelser forblevet et regionalt fænomen med særlig tilknytning til konflikten i Ukraine og rivaliseringen mellem Iran og Saudi Arabien. Angrebene kan imidlertid sprede sig og ramme Danmark, som det var tilfældet under NotPetya-angrebet i 2017.

Stigningen i brug af sociale medier og udfordringer forbundet med at vurdere, om information er sand eller falsk, har givet stater nye muligheder for at påvirke befolkninger. Hack og læk i forbindelse med det amerikanske præsidentvalg i 2016 var en ny og alvorlig anvendelse af cyberangreb til at understøtte en påvirkningsoperation, hvor cyberangreb bruges i forsøg på at påvirke den folkelige meningsdannelse i andre lande.

Kriminelle har fortsat digitaliseringen af den traditionelle berigelseskriminalitet. Teknologier som kryptovaluta og værktøjer til anonymisering har givet profitable rammer for et mere udviklet kriminelt miljø med bedre muligheder for samarbejde. Der er eksempler på, at cyberkriminelle indbyrdes bruger franchiseordninger og kundeservice.

Cyberaktivisme har i de seneste år været på retræte med undtagelse af steder præget af sociale og politiske uroligheder. Militante ekstremistiske grupper har været under massivt pres fra den internationale kontraterrorindsats, og det er ikke lykkedes militante ekstremister at udføre alvorlige cyberangreb med et terrorsigte.

Kendte cyberangreb i 2010'erne
Her er eksempler på kendte cyberangreb fra 2010'erne.

Stuxnet (2010) Iranske centrifuger til berigelse af uran blev i 2010 udsat for et destruktivt cyberangreb med malwaren Stuxnet, der medførte fysisk ødelæggelse af centrifugerne.

Saudi Aramco (2012) Det saudiske nationale olie- og gasselskab, Saudi Aramco, blev i 2012 udsat for et cyberangreb, der ødelagde en stor mængde data tilhørende selskabet.

Sony-hacket (2014) Hackere angreb i 2014 filmselskabet Sony Pictures Entertainment, hvor de ødelagde data og systemer og lækkede bl.a. e-mails og kopier af film, der endnu ikke var udkommet.

Strømafbrydelser i Ukraine (2015) I 2015 blev flere elselskaber i det vestlige Ukraine ramt af cyberangreb. Hackerne fik adgang til elselskabernes kontrolsystemer og lukkede for strømmen i op til 6 timer.

Demokraternes Nationale Komité (2016) Demokraternes Nationale Komité i USA blev i 2016 udsat for hack og læk af informationer, bl.a. e-mails, forud for det amerikanske præsidentvalg samme år.

Mirai (2016) Malwaren Mirai blev i 2016 brugt til at lave nogle af de største overbelastningsangreb (DDoS-angreb), der hidtil var set. Et angreb gjorde en række store internettjenester utilgængelige.

WannaCry (2017) WannaCry-ransomwaren begyndte at sprede sig automatisk til computere verden over i maj 2017. WannaCry var i stand til at kryptere filer på ofrets computer, slette originalerne og opkræve en løsesum for at dekryptere filerne igen. WannaCry ramte bl.a. hospitaler i Storbritannien.

NotPetya (2017) NotPetya-malwaren ramte i juni 2017 mange computere på verdensplan. NotPetya udgav sig for at være ransomware, men havde reelt en destruktiv karakter. NotPetya ramte bl.a. A.P. Møller-Mærsk, der har opgjort tabet til mellem 1,6 og 1,9 mia. kr.

OPCW (2018) Russiske efterretningsagenter blev i 2018 taget på fersk gerning af hollandske myndigheder i et forsøg på at skaffe sig adgang til organisationen for forbud mod kemiske våben OPCW's wifi-netværk.

Demant (2019) Den danske producent af bl.a. høreapparater, Demant, blev i 2019 udsat for et ransomware-angreb, der medførte, at virksomheden lukkede ned for it-systemer på tværs af virksomheden. Angrebet medførte et tab på op mod 650 mio. kr.

Georgien (2019) Den 28. oktober 2019 blev Georgien ramt at et omfattende cyberangreb, hvor tre TV-stationer fik afbrudt transmissionen og over 2.000 hjemmesider blev lukket ned af hackerne.

Cybersikkerhed er ved at blive institutionaliseret

Cybersikkerheden har også udviklet sig i det seneste årti. Cybersikkerhed er med den øgede opmærksomhed og regulering samt store cyberhændelser som NotPetya- og WannaCry-angrebene i 2017 flyttet fra it-afdelingerne til direktionsgangene i danske virksomheder og myndigheder. COVID-19-pandemien har som nævnt også øget fokus på cybersikkerheden i kølvandet på de pludseligt ændrede brugsmønstre af digitale tjenester og systemer.

I Danmark blev CFCS oprettet i 2012, og andre lande, herunder Storbritannien, Australien og Canada, har efterfølgende også oprettet nationale cybercentre med udgangspunkt i deres efterretningstjenester. Samfundsvigtige sektorer og virksomheder har opbygget funktioner, som kan højne cybersikkerheden, såsom decentrale cyber- og informationssikkerhedenheder (DCIS), computer emergency response teams (CERT) og operationscentre for cybersikkerhed (SOC).

Mellemstatslig normdannelse og forsøg på at fordømme og afskrække cyberangreb gennem bl.a. offentlige tilskrivninger af cyberangreb og stævninger af udenlandske hackere viser en villighed fra flere lande til at modvirke truslen. Det sker ikke kun ved

at opbygge et stærkt cyberforsvar, men også ved at lægge et pres på de lande, der udgør en cybertrussel.

Nogle lande er villige til at gå endnu længere for at modvirke truslen. Israels bombning af en bygning i 2019, der ifølge Israel husede hackere fra Hamas, er foreløbigt det mest vidtgående eksempel på det.

På trods af denne udvikling er viden om cybertruslen stadig ikke tilstrækkeligt udbredt. Det betyder bl.a., at hackerne fortsat kan misbruge gammelkendte sårbarheder, og at selv simple cyberangreb kan have alvorlige konsekvenser. Det betyder også, at mange cyberhændelser fortsat ikke bliver opdaget eller rapporteret til relevante myndigheder.

Mørketal og underrapportering er dermed fortsat en udfordring for vurderingen af cybertruslen mod Danmark.

CFCS anbefaler, at myndigheder og virksomheder løbende orienterer sig i vejledninger til, hvordan man kan øge cybersikkerheden. Vejledninger, trusselsvurderinger og undersøgelsesrapporter kan findes på CFCS' hjemmeside.

Cybersikkerhed kan føles fjernt, indtil ulykken indtræffer

"We do quite basic and simple things. We help accountants. We saw ourselves as quite distant from cybersecurity issues."

Citatet er fra Olesya Linnyk, som ledte virksomheden Linkos Group, der blev hacket og udnyttet til at starte det mest omfattende destruktive cyberangreb indtil nu, nemlig NotPetya-angrebet i 2017. Hackere misbrugte Linkos Groups software M.E.doc til at levere NotPetya-malwaren til Linkos Groups kunder, herunder A.P. Møller-Mærsk. Citatet fremgår i bogen 'Sandworm' af Andy Greenberg.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ.** Det betyder, at det er meget sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Cyberkriminalitet er i denne vurdering en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk berigelse.

Cyberkriminalitet udgør en vedvarende og aktiv trussel mod alle danske myndigheder, virksomheder og borgere.

Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang, bl.a. gennem phishing-angreb. Der findes dog også netværk med kapacitet til at udføre mere komplekse og tidskrævende cyberangreb, herunder målrettede ransomware-angreb.

Cyberangreb fra kriminelle grupper starter typisk, uden at aktøren på forhånd har udset sig et specifikt offer. De fleste cyberangreb starter som opportunistiske angreb, hvor eksempelvis phishing-mails bliver spredt til tusinder af ofre, eller hvor kriminelle misbruger it-systemer og enheder med kendte sårbarheder.

Cyberkriminelle udnytter også løbende nye sårbarheder. Der går ofte ikke mere end et par uger fra en teknisk sårbarhed bliver offentligt kendt, til den bliver brugt til at forsøge at hacke danske mål med.

Det høje angrebstempo stiller store krav til, at it-afdelingerne i danske myndigheder og virksomheder opdaterer systemer og programmer i tide eller får opsat kompenserende foranstaltninger i de tilfælde, hvor det ikke er muligt at lukke en sårbarhed.

Citrix sårbarhed efterlod mere end tusind danske enheder potentielt sårbare
Et eksempel på hvor hurtigt og let hackere kan tilegne sig adgang til tusindvis af servere udspillede sig i slutningen af 2019 og i starten af 2020, efter en sårbarhed i Citrix-udstyr blev offentliggjort.

De berørte Citrix-enheder anvendes bl.a. til at styre datatrafikken mellem internettet og hjemmearbejdspladser samt kommunikationen mellem webservere og interne it-systemer. Da sårbarheden blev offentliggjort, fandtes der ingen sikkerhedsopdatering, som kunne udbedre sårbarheden. Citrix anviste dog, hvordan indledende modforanstaltninger kunne implementeres.

To uger efter at sårbarheden blev offentlig kendt, blev de første beskrivelser af, hvordan sårbarheden kunne udnyttes, delt på internettet. Herefter var det let for hackere at bruge beskrivelserne som en opskrift på cyberangreb. Dagen efter at vejledningen blev

offentliggjort, registrerede et it-sikkerhedsfirma 290.000 angrebsforsøg og scanninger fra IP-adresser i 42 lande mod bare et enkelt Citrix-system.

I de følgende dage var der meldinger om, at forskellige hackere kæmpede om adgangen til de sårbare systemer. Nogle hackere smed endda de først ankomne hackere ud og lukkede ned for angrebsmuligheden. De ville have systemet for sig selv.

Det er sandsynligt, at hackerne brugte offentlige søgemaskiner såsom Shodan til at finde sårbare Citrix-enheder i verden, som de kunne forsøge at kompromittere. En søgning i Shodans database ved offentliggørelsen af sårbarheden viste over tusind potentielt sårbare enheder i Danmark.

CFCS er bekendt med flere danske organisationer, der i perioden er forsøgt kompromitteret. CFCS har udsendt varsler til identificerede sårbare myndigheder og virksomheder og løbende vejledt om modforanstaltninger. Antallet af sårbare enheder er i Danmark i dag under hundrede.

Truslen fra målrettede ransomware-angreb er stigende
Der er en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder.

I målrettede ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af offerets it-systemer ved hjælp af ransomware.

Siden slutningen af 2019 truer hackere, der har stået bag målrettede ransomware-angreb, nu også af og til med at lække følsomme data indsamlet fra det ramte system, hvis offeret ikke betaler løsesummen.

Målrettede ransomware-angreb har ramt danske virksomheder, og angreb sker nu relativt hyppigt. I efteråret 2019 har to danske virksomheder, Demant og GlobalConnect, eksempelvis været udsat for separate ransomware-angreb. Angrebet på Demant medførte iflg. virksomheden et tab på op mod 650 mio. kr. I februar 2020 blev den internationale servicevirksomhed ISS ramt af et ransomware-angreb, der også påvirkede den danske del af virksomheden. I april 2020 blev landbrugsvirksomheden Danish Agro og pumpeproducenten Desmi også ramt. I maj 2020 blev GlobalConnect igen kompromitteret. Angrebet ramte systemer tilhørende en række af GlobalConnects kunder, herunder medicin-indkøberen Amgros.

Der har i flere lande været sager, hvor målrettede ransomware-angreb medførte, at myndigheder og virksomheder i perioder ikke kunne udføre dele af deres arbejde. Lokale myndigheder, skoler, produktionsvirksomheder, hospitaler, it-firmaer, havne og rederier har bl.a. været ramt.

Målrettede cyberangreb som disse kan få alvorlige konsekvenser for samfundsvigtige funktioner. Det har f.eks. været tilfældet i forbindelse med ransomware-angreb mod

sundhedssektoren i bl.a. USA og Storbritannien, hvor nedetid i administrative systemer medførte, at patientaftaler måtte aflyses.

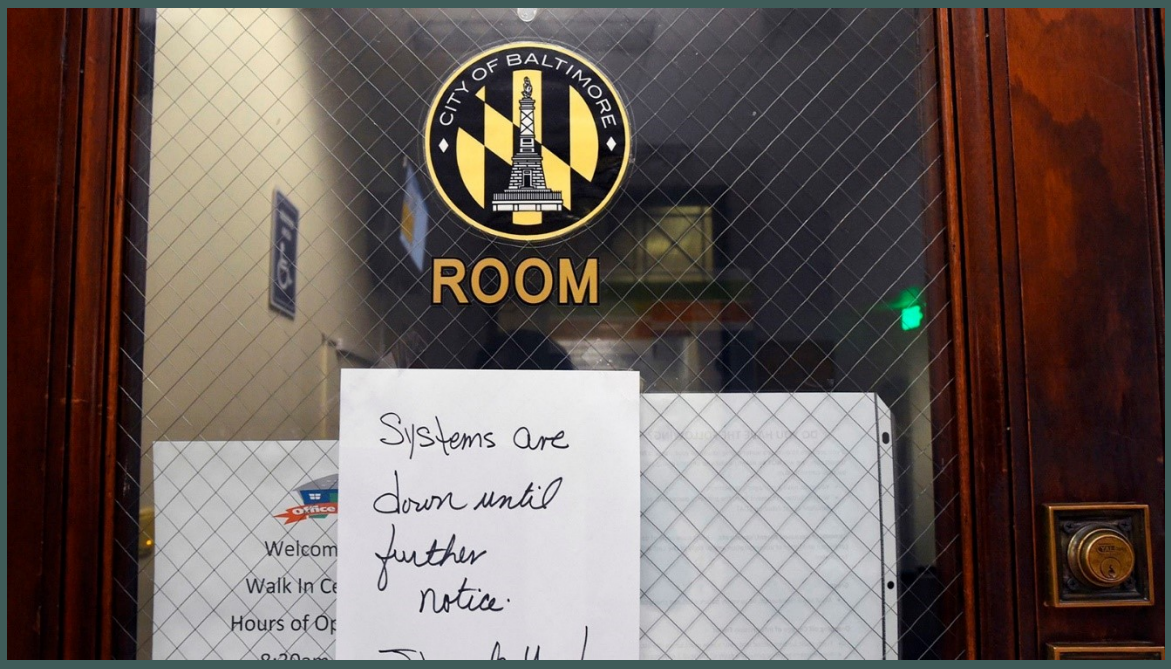
Et vellykket målrettet ransomware-angreb på leverandører af samfundsvigtige ydelser under en krise, som f.eks. mod sundhedssektoren i Danmark under COVID-19 krisen, vil kunne øge det pres, som sektoren allerede oplever pga. krisen.

Angrebet mod Amgros, der er leverandør til danske sygehusapoteker, er et eksempel på et ransomwareangreb mod sundhedssektoren i Danmark under krisen. Angrebet betød bl.a. at Amgros i nogle dage ikke kunne købe og sælge lægemidler via deres forretningssystem Naviline. Angrebet førte dog ikke til mangel på lægemidler på de offentlige hospitaler.

Lokale myndigheder i udlandet er blevet ramt flere gange
Lokale myndigheder i særligt USA har været hyppige mål for målrettede ransomware-angreb i de seneste år. Skoler og skoledistrikter har også været hyppige mål. I august 2019 har der eksempelvis været et målrettet angreb mod en it-leverandør, der lammede it-systemer hos 22 lokale myndigheder i Texas.

Nogle af myndighederne har også været udsat for afpresning med trusler om læk af dokumenter stjålet fra de ramte systemer i forbindelse med ransomware-angrebene. Det skete bl.a. for byen Pensacola, hvor afpresserne endte med at lække data på internettet i november 2019.

Angreb mod lokale myndigheder har ikke været afgrænset til USA.
I efteråret 2019 var der også en bølge af angreb på lokale myndigheder i Spanien.



Byen Baltimore i USA blev ramt af ransomware i 2019.
FOTO: Kenneth K. Lam/SIPA/Ritzau Scanpix

Digitale bankrøverier er rykket tættere på Danmark
Målrettede cyberangreb rettet mod finansielle virksomheder, såkaldte digitale bankrøverier, er i 2019 rykket indenfor Europas grænser. Der er en øget sandsynlighed for, at danske finansielle virksomheder kan blive udsat for denne type angreb.

I februar 2019 blev den maltesiske bank, Bank of Valletta, udsat for et digitalt bankrøveri. Hackerne forsøgte at stjæle 13 mio. Euro fra banken, hvilket svarede til omtrent 100 mio. kroner. Det lykkedes dog efterfølgende for banken at tilbageføre størstedelen af beløbet. Andre europæiske banker blev i samme periode sandsynligvis også udset som mål for digitale bankrøverier.

CFCS er bekendt med, at hackere, som sandsynligvis har kapacitet til at udføre digitale bankrøverier, er gået målrettet efter institutioner i den danske finanssektor i 2019, dog uden succes. Hackere har desuden udgivet sig for at være fra det danske finanstilsyn i phishing-mails, som blev sendt til banker i udlandet. Hackerne brugte navne på faktiske medarbejdere i Finanstilsynet.

Misbrug af finansielle myndigheders navne i phishing-angreb er sandsynligvis motiveret af, at det er almindeligt for finansielle institutioner at modtage forespørgsler fra myndigheder, som der skal reageres meget hurtigt på. Det kan øge sandsynligheden for, at modtageren reagerer på phishing-mailen ved eksempelvis at klikke på links eller åbne filer sendt af hackerne, under dække af en legitim henvendelse.

Simple angreb er en trussel mod alle
Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang i håbet om at få et afkast fra så mange som muligt. Disse angreb udgør en vedvarende trussel for virksomheder, myndigheder og borgere i Danmark.

Disse angreb sker ofte gennem phising-angreb rettet mod tusinder af modtagere. Der findes dog også mange andre metoder. Cyberkriminelle kan f.eks. inficere hjemmesider og derfra sprede malware til besøgende på hjemmesiderne eller stjæle information, som ofret indtaster, når de besøger hjemmesiderne.

Den spredte malware kan have forskellige formål, der understøtter cyberkriminalitet. Trojanere bruges eksempelvis til tyveri af personlige og finansielle oplysninger. Kryptominere misbruger inficerede computeres maskinkraft og strømforbrug til at genere kryptovaluta. Ransomware holder data og systemer på offerets computer som gidsel, da de krypteres og derved bliver utilgængelige for offeret.

Spredningen af malware gennem phishing udføres af kriminelle grupper og netværk, der samarbejder og udveksler tjenester og kapaciteter såsom malware og infrastruktur.

Kriminelle sælger adgange, der bliver brugt i målrettede angreb
Der er et samarbejde mellem de kriminelle, der udfører mere målrettede angreb, og de kriminelle, der rammer tusindvis af ofre gennem bl.a. phishing. Målrettede ransomware-angreb sker eksempelvis ofte opportunistisk efter en indledende

kompromittering af offeret med malware spredt gennem phishing. Videregivelse og salg af disse indledende kompromitteringer kaldes for access-as-a-service.

Massekompromitteringer gennem phishing udgør derfor ikke kun en trussel i sig selv, men understøtter også den stigende trussel fra målrettede cyberangreb udført af kriminelle.

Med stigende indtjeningsmuligheder ved bl.a. målrettede ransomwareangreb stiger indtjeningsmulighederne også for de kriminelle, der videresælger og faciliterer adgange til de målrettede angreb.

Disse indtjeningsmuligheder er muligvis årsagen til, at en af de mest udbredte malware på globalt plan, Emotet, siden 2017 ikke længere bruges som direkte indtjeningskilde for de kriminelle gennem tyveri af finansielle oplysninger. Emotet bliver nu hovedsageligt brugt som et værktøj, som andre kriminelle kan købe sig adgang til.

Statslige aktører kan også udnytte kriminelles adgange og tjenester i eksempelvis cyberspionage. Det kan både ske via køb af adgange eller via afpresning af hjemlige kriminelle netværk. Amerikanske myndigheder har i 2019 eksempelvis officielt beskyldt russiske myndigheder for at samarbejde med cyberkriminelle.

Flere statslige aktører benytter desuden malware og teknikker brugt af kriminelle. Det kan vanskeliggøre identifikationen af cyberspionage iblandt de mere hyppige kriminelle cyberangreb.

Amerikanske sanktioner mod netværk i Rusland
I december 2019 indførte amerikanske myndigheder i koordination med britiske myndigheder økonomiske sanktioner mod flere navngivne personer og virksomheder i Rusland, der menes at stå i ledtog med et cyberkriminelt netværk kaldet Evil Corp.

De amerikanske myndigheder beskylder samtidigt den russiske føderale sikkerhedstjeneste, FSB, for at samarbejde med netværket i spionageøjemed.

Netværket har ifølge sanktionerne stået bag spredningen af malwaren Dridex. Dridex, der i tidligere varianter blev kaldt Bugat og Cridex, er siden 2012 blevet spredt gennem massive spam-kampagner med et udbytte svarende til mere end en halv milliard danske kroner. Dridex har også været brugt til spredningen af ransomware.

Russiske myndigheder har officielt afvist anklagerne som propaganda. Amerikanske retsdokumenter viser dog, at russiske myndigheder har hjulpet med at identificere lederen af netværket, Maksim Yakubets.

Anklagerne blev gennemgået på en pressekonference i det amerikanske justitsministerium. FOTO: Samuel Corum/AFP/Ritzau Scanpix

Cyberspionage

Truslen fra cyberspionage er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Danmark er udsat for både politisk og kommercielt motiveret cyberspionage fra fremmede stater.

Det er en vedvarende trussel, der især er rettet mod danske myndigheder, som arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder, der besidder en viden, som andre stater har interesse i.

Leverandører og samarbejdspartnere til disse myndigheder og virksomheder kan også blive udsat for forsøg på cyberspionage med det formål at misbruge dem som trædesten i forsøg på at opnå adgang til myndighederne og virksomhederne.

Cyberspionage kan føre til pres på danske beslutningstagere
Truslen fra cyberspionage mod myndigheder er generelt et udtryk for aktuelle udenrigs- og sikkerhedspolitiske forhold.

Som FE beskriver i Efterretningsmæssig Risikovurdering fra 2019 er den verdensorden, der har dannet den overordnede ramme for håndteringen af Danmarks og Europas geopolitiske og sikkerhedsmæssige interesser de sidste mange årtier, under pres. Det ses eksempelvis ved, at USA's dominerende position i international politik bliver udfordret.

Cyberspionage bruges aktivt af flere lande, herunder Rusland og Kina, til at fremme nationale handlemuligheder og undgå strategiske overraskelser i et foranderligt udenrigspolitisk miljø. Flere offentligt kendte cyberangreb på europæiske udenrigsministerier de seneste år understreger, at truslen er højaktuel, og at viden om udenrigspolitiske beslutninger og dispositioner er en prioritet for flere landes cyberspioner.

CFCS ser kontinuerligt forsøg på cyberspionage mod danske myndigheder. Truslen er især rettet mod myndigheder og personer, der arbejder med sikkerheds- og udenrigspolitik, herunder Udenrigsministeriet og Forsvaret.

Danmark deltager i internationale fora, som fremmede stater har udvist en vedvarende interesse i at udføre cyberspionage imod. Der findes bl.a. eksempler på cyberspionage mod NATO, EU og OSCE.

Det er sandsynligt, at fremmede stater forsøger at bruge cyberspionage som et middel til at opnå viden om danske interesser, overvejelser og beslutninger i forbindelse med større internationale sager eller udenrigspolitiske forhandlinger. Denne viden kan staterne bl.a. udnytte til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres.

Særligt Rusland og Kina råder over meget væsentlige cyberkapaciteter og begge lande bruger deres kapaciteter aktivt på globalt plan. Det er sandsynligt, at bl.a. Iran også udfører cyberspionage og andre typer cyberangreb mod mål i og uden for deres nærområde.

Andre stater, der også har en cyberkapacitet, anvender hovedsageligt deres cyberkapaciteter i deres nærområder. Disse stater udgør en potentiel cybertrussel mod Danmark. De kan eksempelvis forsøge at udføre cyberspionage mod danske repræsentationer, dels for at få adgang til viden om dansk sikkerheds- og udenrigspolitik i regionen, og dels for at få adgang til viden om det land eller den region, repræsentationen ligger i.

Flere udenrigsministerier i Europa er blevet angrebet
Kort efter nytår offentliggjorde østrigske myndigheder, at landets udenrigsministerium var blevet udsat for et alvorligt cyberangreb. De østrigske myndigheder udelukker ikke, at en statslig aktør stod bag angrebet.

Et par måneder tidligere havde Tjekkiets efterretningstjeneste, BIS, beskyldt Ruslands føderale sikkerhedstjeneste, FSB, for at stå bag gentagne kompromitteringsforsøg mod det tjekkiske udenrigsministerium og det tjekkiske forsvarsministerium i 2018. Tjekkiske myndigheder har også udtalt offentligt, at Kina sandsynligvis også har stået bag et omfattende angreb på en "strategisk vigtig regeringsinstitution" i Tjekkiet i 2018.

Disse eksempler skriver sig ind i en lang række af cyberangreb mod europæiske udenrigsministerier. Over de seneste år har bl.a. Italien, Kroatien, Belgien og Tyskland offentliggjort, at deres udenrigsministerier har været udsat for cyberangreb.

CFCS har i to undersøgelsesrapporter beskrevet hvordan Udenrigsministeriet blev forsøgt kompromitteret i 2014 og 2015. Rapporterne er på CFCS's hjemmeside.

Cyberspionage kan skade dansk konkurrenceevne og økonomi
Stater bruger også cyberspionage med det formål at styrke den nationale udvikling og konkurrenceevne. Den form for cyberspionage retter sig især mod virksomheder og institutioner, der har en viden, som fremmede stater har interesse i.

Staterne kan bruge den stjålne information til at understøtte udviklingen af deres nationale sektorer, der kan springe flere led af deres innovations- og udviklingsproces over. Det er f.eks. sandsynligt, at udviklingen af motoren i det kinesiske passagerfly C919 bl.a. er sket på baggrund af målrettet statsstøttet cyberspionage mod flyproducenter og underleverandører i udlandet.

Forskning relateret til COVID-19 er også et eksempel på viden, der kan have værdi for fremmede stater. CFCS vurderer, uafhængigt af COVID-19-pandemien, at fremmede stater særligt har interesse i de dele af sundhedssektoren, der har adgang til forskningsdata eller intellektuel ejendom. Det er f.eks. virksomheder, universiteter og hospitaler, der beskæftiger sig med udvikling af bl.a. biokemi, biotek og lægemidler.

Det kan skade Danmarks konkurrenceevne og derved dansk økonomi, hvis danske virksomheder udsættes for cyberspionage, især inden for områder hvor danske virksomheder besidder en konkurrencestærk viden.

Grænsen mellem denne kommercielt motiverede og den sikkerhedspolitisk motiverede cyberspionage kan være overlappende. Der er flere eksempler på cyberspionage mod teknologier, som både kan bruges civilt og militært, eksempelvis inden for luftfart og rumfart. NASA offentliggjorde eksempelvis i 2019, at de havde været kompromitteret i ti måneder fra 2017 til 2018. Ifølge NASA lykkedes det bl.a. aktøren at stjæle information underlagt amerikansk våbeneksportkontrol.

Leverandører og samarbejdspartnere bruges som springbræt
Der er også en trussel mod leverandører og samarbejdspartnere til de ovennævnte typer myndigheder og virksomheder, som fremmede stater er interesserede i. I forsøget på at få adgang til disse myndigheder og virksomheder kan fremmede stater forsøge at bruge myndighedernes og virksomhedernes leverandører og samarbejdspartnere som et mellemliggende mål.

Her er der tale om en angrebsmetode, hvor hackere angriber en organisation for at bruge den som springbræt til at kompromittere de af organisationens kunder og samarbejdspartnere, der er interessante for den fremmede stat.

Målet med cyberspionage er derfor ikke nødvendigvis altid at skaffe konkret viden, men kan også være at skaffe en specifik adgang. Visse underleverandører eller samarbejdspartnere har måske ikke en viden, der er interessant for fremmede lande, men de kan til gengæld have en adgang eller troværdighed, hackerne kan udnytte til at kompromittere deres egentlige mål.

It-leverandører, eksempelvis hosting-udbydere og it-servicevirksomheder, kan have adgang til kundernes data eller it-systemer. Hackerne kan forsøge at kompromittere disse leverandører med det formål at tilgå disse data eller it-systemer via leverandøren. Kompromitterede software- og udstyrsleverandører kan også misbruges til at sprede malware, der kan bruges i cyberspionage, til deres kunder gennem eksempelvis inficerede systemopdateringer.

Fremmede stater kompromitterer også sårbare it-systemer i virksomheder og myndigheder på tværs af samfundet for at opbygge en it-infrastruktur, der kan misbruges i cyberangreb mod andre mål. Danske myndigheder og virksomheder kan derfor blive udsat for cyberangreb udført af fremmede lande uden at være i besiddelse af specifik viden eller adgang, som landene er interesserede i.

I 2015-2016 blev en række danske virksomheder og myndigheder eksempelvis systematisk angrebet som del af en angrebsbølge rettet mod sårbare JBoss-systemer, der bruges i en række it-løsninger. Angrebene ramte et bredt udsnit af mål, der ikke synes at have andet tilfælles end brugen af JBoss.

Cyberangreb mod norske Visma
Den norske softwareleverandør Visma offentliggjorde i februar 2019, at den var blevet kompromitteret. Ifølge åbne kilder var formålet at få adgang til Vismas kunders data.

Visma er en stor international leverandør, som blandt andet leverer cloud-software til virksomheders regnskab og forretning.

Selskabet har også afdelinger i Danmark og har blandt andet været leverandør til den danske Søfartsstyrelse. CFCS har ikke kendskab til, at Søfartsstyrelsen har været påvirket af angrebet, men angrebet viser den potentielle trussel fra angreb via leverandører.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Det skyldes, at det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at rette destruktive cyberangreb mod Danmark.

Flere stater har dog betydelige kapaciteter til at udføre destruktive cyberangreb, og de udvikler deres kapaciteter løbende. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

Hvad er destruktive cyberangreb?

CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er:

- død eller personskade
- betydelig skade på fysiske objekter
- ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Det er her vigtigt at bemærke, at CFCS' definition af destruktive cyberangreb dækker cyberangreb med meget forskellige konsekvenser, rangerende fra ødelæggelse af data til fysisk ødelæggelse og dødsfald. Langt de fleste af de destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data ved at slette eller kryptere dem uden mulighed for at genskabe dem.

Destruktive cyberangreb er selv inden for denne brede definition relativt sjældne. CFCS vurderer, at langt størstedelen af de destruktive cyberangreb, som CFCS har kendskab til, sandsynligvis har været udført af stater. Næsten alle disse angreb er udført i forbindelse med konflikter eller geopolitiske spændinger mellem stater. Det er mindre sandsynligt, at fremmede stater har intention om at ramme Danmark.

Det er dog muligt, at danske virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, kan blive udsat for følgevirkningerne af et destruktivt cyberangreb, sådan som det eksempelvis skete for A. P. Møller Mærsk ved NotPetya-angrebet i Ukraine i 2017. Indtil nu har de fleste angreb fundet sted i Ukraine og Saudi Arabien.

Danske virksomheder med aktiviteter i særligt Ukraine og Saudi Arabien kan i enkelte tilfælde også blive udset som direkte mål for destruktive cyberangreb. Det blev illustreret af angrebet, der slettede data hos den italienske virksomhed Saipem i 2018.

Saipem er underleverandør til den saudiske nationale olieproducent Saudi Aramco. Saudi Aramco har selv været udsat for destruktive cyberangreb både i 2012, 2016 og 2017.

Stater forsøger at afskrække brugen af destruktive cyberangreb
NATO har, bl.a. som reaktion på NotPetya-angrebet i 2017, slået fast i en fælles erklæring, at cyberangreb mod medlemslandene vil kunne udløse alliancens kollektive forsvarsforpligtigelser i rammen af Atlantpagtens artikel 5, den såkaldte musketer-ed.

Destruktive cyberangreb er indtil videre typisk ikke blevet mødt med militære modsvar. Dog bombede det israelske luftvåben i maj 2019 en bygning i Gaza, som ifølge Israel husede hackere fra Hamas. Der er flere eksempler på, at stater har reageret på destruktive cyberangreb med økonomiske sanktioner.

Stater kan have forskellige formål med destruktive cyberangreb
Stater kan forsøge at opnå forskellige resultater ved hjælp af destruktive cyberangreb. En stat kan ved hjælp af destruktive cyberangreb mod samfundsvigtige sektorer eksempelvis forsøge at sende et signal om, at den anden stat ikke er i stand til at beskytte sin befolkning.

Den angribende stat kan også bruge angrebene til at straffe eller til at signalere, at fremmede stater ikke må agere imod det angribende lands interesser. Destruktive cyberangreb rettet mod virksomheder med aktiviteter i en region præget af geopolitiske spændinger kan også have til hensigt at skræmme udenlandske virksomheder og investorer fra at gøre forretninger i det pågældende land.

Et destruktivt cyberangreb, der ødelægger kritisk infrastruktur eller militære kapaciteter, kan potentielt svække modstandere i tilfælde af en krise eller krig. Der er dog endnu ikke offentligt omtalte eksempler på destruktive cyberangreb, der har haft så vidtrækkende konsekvenser. Det eksempel, der kommer tættest på, er angrebet mod iranske centrifuger til berigelse af uran, der blev offentligt kendt i 2010. Det er også stadig det eneste kendte eksempel på et destruktivt cyberangreb, der har medført fysisk ødelæggelse i større skala.

I det årti, der er gået siden angrebet på de iranske atomcentrifuger, har både industrielle systemer og offensive cyberkapaciteter dog udviklet sig væsentligt, og det er sandsynligt, at der er flere lande, der har kapacitet til at lave lignende angreb.

Få destruktive cyberangreb uafhængigt af konflikter
Hackere benytter i få tilfælde også simple destruktive cyberangreb uafhængigt af politiske og militære konflikter.

Der er enkelte eksempler på, at hackere i forbindelse med digitale bankrøverier har slettet eller krypteret finansielle virksomheders data. Formålet har sandsynligvis været at slette deres spor eller forhindre virksomhederne i at reagere på tyveriet. Cyberkriminalitet kan altså potentielt ledsages af cyberangreb, der har en destruktiv effekt. Sletning eller kryptering af data i digitale bankrøverier er foreløbigt et relativt sjældent fænomen, men det kan have store konsekvenser for den enkelte berørte finansielle institution.

Der kan generelt ske fejl, når hackere manipulerer it-systemer. Det betyder, at andre typer cyberangreb også kan få en ødelæggende virkning, selvom det ikke var hackerens hensigt. Inden for søfart er der eksempler på cyberangreb, der har påvirket strømforsyning, navigationssystemer og positioneringssystemer. Konsekvenserne i sagerne, som CFCS har kendskab til, har ikke medført fysisk skade og ulykker, men det er muligt, at sådanne angreb kan få fysiske konsekvenser.

Cyberaktivisme

Truslen fra cyberaktivisme er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Truslen kommer særligt til udtryk i forbindelse med begivenheder eller enkeltsager, der tiltrækker cyberaktivisters opmærksomhed.

Det er også mindre sandsynligt, at Danmark vil blive ramt af faketivisme, hvor statsstøttede hackere udfører cyberangreb, mens de udgiver sig for at være cyberaktivister. Truslen fra faketivisme vil sandsynligvis stige i forbindelse med militære eller politiske konflikter med fremmede stater.

Fodboldhacker fælder Afrikas rigeste kvinde
Siden 2015 har den portugisiske hacker Rui Pinto hacket og lækket informationer om fodboldverdenen i kampagnen Football Leaks.

I 2018, da Pinto stjal dokumenter til understøttelse af Football Leaks, stødte han ifølge flere åbne kilder ved et tilfælde også på fortrolige dokumenter, der indeholdte inkriminerende informationer om Afrikas rigeste kvinde, Isabel dos Santos.

Pinto gav dokumenterne videre til en afrikansk whistleblowerorganisation, hvilket blev starten på Luanda Leaks. Luanda Leaks har medført, at dos Santos er blevet genstand for strafferetslig efterforskning i Angola, ligesom Portugal har indefrosset hendes bankkonti i landet.

Der er umiddelbart langt fra de europæiske fodboldbaner til de angolanske regeringskontorer, men der findes dog en tematisk fællesnævner. Football Leaks og Luanda Leaks indeholder begge anklager om bl.a. korruption og magtmisbrug. Sagen illustrerer, hvordan både aktivisternes fokus og tilfældigheder kan have betydning for, hvem der bliver ramt af cyberaktivisme.

Rui Pinto blev arresteret i Ungarn i 2019. FOTO: Ferenc Isza/AFP/Ritzau Scanpix

Begivenheder og tilfældigheder kan udløse cyberaktivisme
Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en sag. Cyberaktivister opnår dette mål med forskellige midler, og angrebsmetoderne varierer meget i kompleksitet – fra relativt simple DDoS-angreb til mere ressourcekrævende hack og læk af informationer fra myndigheder og virksomheder.

Det sidste cyberaktivistiske angreb i Danmark, der fik stor medieopmærksomhed, var et DDoS-angreb mod bl.a. Udlændinge- og Integrationsministeriet og Udenrigsministeriet i 2017. Angrebet var sandsynligvis en reaktion på en debat om Muhammed-tegningerne kort forinden. Angrebet understreger, at truslen er dynamisk, da angreb fra cyberaktivister ofte er en spontan reaktion på specifikke begivenheder.

DDoS-angreb er relativt nemme at udføre og forudsætter derfor typisk minimal planlægning og teknisk viden. Truslen fra sådanne simple angreb kan derfor stige pludseligt, hvis danske myndigheder eller virksomheder kommer i aktivisternes søgelys, som det eksempelvis skete i 2017. Hack og læk af eksempelvis personfølsomme oplysninger forudsætter til sammenligning længere planlægning og bedre tekniske færdigheder.

Cyberaktivistiske angreb dækker således over en mangfoldig gruppe af aktiviteter, der spænder fra opportunistiske angreb til mere organiserede kampagner. En fællesnævner på tværs af dette spektrum er dog, at mens angrebene ofte er en reaktion på specifikke begivenheder, så findes der en kontinuitet i de temaer, som de forskellige aktivister forfølger.

Stater bruger cyberaktivisme som dække for påvirkning
I nogle lande ledsager cyberaktivisme den traditionelle politiske aktivisme. Cyberaktivister har eksempelvis suppleret den seneste bølge af protester og civile uroligheder i Sydamerika og Catalonien med cyberangreb. Denne typer aktivisme sker typisk inden for rammerne af lokale konflikter og uroligheder.

Fremmede stater kan have interesse i at forstærke disse lokale konflikter og uroligheder ved selv at lave cyberangreb, der ligner cyberaktivisme. I populær tale kaldes dette for faketivisme.

Faketivisme repræsenterer typisk forsøg på at afspore og aflede den offentlige debat i de ramte samfund og kultivere en polarisering i samfundet. Det kan være vanskeligt at bevise, hvilke lande der står bag faketivismen. Staterne kan på den måde forsøge at unddrage sig et ansvar for påvirkningskampagner i andre lande.

Det er mindre sandsynligt, at Danmark vil blive ramt af faketivisme. Det er dog muligt, at truslen vil stige ved sager af særlig politisk, strategisk eller økonomisk karakter, som fremmede stater har en væsentlig interesse i at påvirke. Det er sandsynligt, at truslen vil stige ved en skærpet politisk eller militær konflikt mellem Danmark og fremmede stater.

Hackere plantede flere falske nyheder i Litauen
Den 19. juni 2019 dukkede en falsk nyhed op på flere litauiske internetmedier. I nyheden stod der, at NATO ved et uheld havde forurenet en flod i Litauen med radioaktive materialer under øvelsen "Iron Wolf". Det viste sig dog efterfølgende, at internetsiderne var blevet kompromitteret, og nyhederne var plantet af hackere.

Et par måneder senere i oktober 2019 gentog mønsteret sig. Et litauisk internetmedie kunne rapportere om amerikanske planer for at flytte atomvåben til Litauen, men igen viste det sig at være en falsk historie, der var blevet plantet, efter at mediet var blevet hacket.

I november 2019 udtalte det litauiske forsvar, at de mente, at hændelserne var en del af en større russisk påvirkningskampagne, hvis formål bl.a. var at skabe tvivl om NATO's tilstedeværelse i landet.

I april 2020 blev en fabrikeret e-mail, der udgav sig for at komme fra NATO's generalsekretær, sendt til bl.a. litauiske medier, med falske påstande om at NATO ville trække sig ud af landet.

Cyberterror

Truslen fra cyberterror er **INGEN**. Det betyder, at det er usandsynligt, at Danmark, herunder danske virksomheder og myndigheder, vil blive udsat for forsøg på cyberterror inden for de næste to år.

CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

Så alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

Der er endnu ingen terrorgrupper, som har udført cyberangreb, der lever op til CFCS's definition på cyberterror, mod hverken danske eller udenlandske mål. Der findes heller ingen hændelser, hvor terrorgrupper har taget ansvaret for at udføre cyberterror.

Manglende kapacitet ledsages af en meget begrænset hensigt
Der er kun få eksempler på, at militante ekstremister har opfordret til cyberterror. Militante ekstremister har heller ikke hævdet at stå bag nogle af de destruktive cyberangreb, som verden hidtil har set. Selvom det nogle gange er tilfældet, at terrorgrupper ikke offentligt påtager sig ansvaret for deres terrorhandlinger, vurderer CFCS, at et vellykket alvorligt cyberangreb ville være blevet fulgt op af propaganda for at understrege den nye trussel.

Den manglende hensigt skyldes sandsynligvis, at de etablerede terrorgrupper ikke anser cyberangreb som en realistisk og effektiv måde til at skabe den samme frygt og kaos, som konventionelle terrorangreb skaber.

Militante ekstremister står i stedet bag cyberaktivisme
Cyberangreb udført af militante ekstremistiske grupper har primært manifesteret sig som cyberaktivisme. Det fremgår af de opfordringer og vejledninger til cyberangreb, som militante ekstremister har udsendt. Angreb og ønsker om angreb har typisk drejet sig om defacement- og overbelastningsangreb på hjemmesider samt hack og læk af personoplysninger ledsaget af opfordringer til drab i form af såkaldte drabslister.

Hackerne bag disse cyberangreb har typisk udvist støtte til Islamisk Stat. Fire hackergrupper slog sig i 2016 sammen og dannede United Cyber Caliphate (UCC), sandsynligvis for at styrke deres kapacitet. Det militære pres på Islamisk Stat har medført, at hackergrupperne ikke har kunnet etablere sig som en fysisk samlet enhed, men stadig er overladt til at operere som løst forbundne enkeltpersoner.

Radikalisering og rekruttering kan øge truslen
Truslen fra cyberterror kan stige, hvis det lykkes militante ekstremister at radikalisere og rekruttere dygtige hackere eller insidere med adgang til kritiske it-systemer. Der er i udlandet eksempler på, at insidere i enkelte tilfælde har tilbudt deres it-ekspertise til militante ekstremister.

På mellemlangt sigt kan den øgede sammensmeltning af det fysiske og digitale domæne medføre en stigende risiko for, at et cyberangreb medfører skade på materiel eller mennesker. Det kan potentielt øge truslen fra cyberterror.

Fraværet af cyberterror betyder ikke, at internettet er uden betydning for terrortruslen. Militante ekstremister anvender krypterede chattjenester og lukkede internetfora til at rekruttere og radikalisere nye ekstremister på tværs af landegrænser. I de lukkede fora deles også opfordringer og vejledninger til udførelse af konventionelle terrorangreb samt råd om hvorledes mobil- og internetkommunikation kan skjules for myndighederne.

Kunstig intelligens og kvanteteknologi forandrer cybersikkerheden

En række teknologiske gennembrud har i de seneste år givet os et væld af nye digitale muligheder. Personlige assistenter er en del af manges hjem, vores ansigt kan bruges til autentifikation, og selvkørende biler testes allerede i flere storbyer.

Med hastige fremskridt følger dog også nye udfordringer, som vil forme vores digitale sikkerhed i de kommende år. Særligt har gennembrud indenfor kunstig intelligens og kvanteteknologi åbnet op for nye muligheder og udfordringer.

Kunstig intelligens: Automatisering af forsvar og angreb
Udviklingen inden for kunstig intelligens har givet langt bedre muligheder for at opdage cyberangreb end tidligere. Algoritmer, drevet af machine learning, danner i dag kerneforretningen for mange private cybersikkerhedsfirmaers it-sikkerhedsløsninger. Flere firmaer tilbyder aktiv monitorering af netværkstrafik, som løbende træner deres algoritmer til at identificere og standse ondsindet aktivitet i realtid. Særligt er der sket fremskridt inden for identificeringen af phishing-mails, hvor langt de fleste i dag bliver opdaget og frasorteret automatisk af machine learning algoritmer.

På den anden side har kunstig intelligens skabt en række nye udfordringer. Hackere er eksempelvis begyndt at udnytte samme algoritmer til automatisk at generere langt mere troværdige phishing-mails netop for at slippe forbi disse avancerede machine learning algoritmer. Det sker i stigende grad ved, at algoritmerne aktivt indarbejder informationer om deres mål fra sociale medier for at virke mere troværdige.

Kunstig intelligens
Teknologier, som efterligner menneskelig intelligens herunder sprog, syn, læring og evnen til at generalisere.

Machine Learning
IT-systemer, som behandler nye data på baggrund af maskinelle analyser af et tidligere datasæt (læring) frem for gennem eksplicit programmering (instrukser).

Kunstig intelligens giver også nye muligheder for at udføre langt mere målrettede hackerangreb. Under it-sikkerhedskonferencen Black Hat i 2018 demonstrerede IBM for eksempel, hvordan det er muligt at indlejre machine learning algoritmer i malware, som udnytter ansigts- og talegenkendelse til kun at frigive malwaren, hvis den genkender et specifikt ansigt eller en specifik stemme. Det åbner for særligt målrettede cyberangreb, der retter sig mod udvalgte enkeltpersoner eller grupper. Kunstig intelligens har med andre ord bl.a. gjort det muligt at misbruge vores biometriske data mod os selv. I takt med at kunstig intelligens tages i brug, også i systemer indenfor kritisk infrastruktur, er det derfor vigtigt, at cybersikkerhed tænkes ind i både udviklings- og anvendelsesfasen.

Cybersikkerhed efter kvantespringet
Udviklingen af kvanteteknologi vil også påvirke vores cybersikkerhed de kommende år. Forskere og virksomheder forsøger at overføre kvantefysiske fænomener til den digitale verden bl.a. med henblik på at udvikle universelle kvantecomputere og skabe kvantesikrede kommunikationskanaler.

Kvantecomputere bygger på såkaldte ”qubits”, som har langt flere frihedsgrader til at foretage beregninger relativt til klassiske computere. Faktisk fordobles computerkraften hos en kvantecomputer for hver qubit, der tilføjes. En kvantecomputers regnekraft vokser med andre ord dobbelteksponentielt, mens klassiske computere kun vokser eksponentielt. Det er en meget stor forskel, som sandsynligvis vil få betydelige konsekvenser i fremtiden.

Udviklingen af kvantecomputere udgør en potentiel trussel mod cybersikkerheden i Danmark, da kvantecomputernes øgede maskinkraft kan misbruges i cyberangreb. Udviklingen af kvantecomputere udfordrer især vores datasikkerhed på internettet. Kommunikation over internettet krypteres i øjeblikket med meget komplicerede beregninger, som beskytter vores data på en måde, som en klassisk computer skal bruge flere tusinde år på at bryde. I fremtiden kan kvantecomputere muligvis bryde disse krypteringer på få sekunder, og krypteret information, som vi i dag sender over internettet, kan således potentielt blive læsbar.

En af de mest udbredte krypteringsmetoder i dag hedder RSA. Ifølge det amerikanske forskningsinstitut National Institute of Standards and Technology (NIST) vil kvantecomputere sandsynligvis kunne bryde RSA om ti år. Derfor igangsatte NIST i 2017 en international konkurrence om udviklingen af en ny krypteringsmetode, som skal erstatte RSA og være såkaldt ”kvantesikret”. Udfordringen ligger nu i at udpege en erstatning og implementere denne, inden kvantecomputerne kan bryde RSA.

Selvom udviklingen i dag er i en tidlig fase, er de første prototyper på kvantecomputere allerede begyndt at levere resultater. Google byggede eksempelvis en kvantecomputer i 2019, som på lidt over 3 minutter løste et regnestykke, som en klassisk computer skulle bruge cirka 10.000 år på. Der er stadig betydelige udfordringer forbundet med kvantecomputere, men nogle sammenligner Googles bedrift med Wright-brødrenes første flyvning, der på trods af den begrænsede præstation åbnede døren til en ny fremtid.

Udviklingen af kvantesikret kommunikation præsenterer imidlertid en mulig løsning på nogle af udfordringerne. Ideen bag kvantesikret kommunikation bygger på muligheden for at dele ’nøgler’, som legitimt bruges til at afkode meddelelser af modtagere, på en ny og sikker måde baseret på kvantefysik. Det særlige er, at nøgleudvekslingen sker på en måde, hvor datasikkerheden ikke længere er afhængig af begrænset computerkraft, og at både afsenderen og modtageren altid vil kunne opdage, hvis nogen forsøger at opfange nøgleudvekslingen under forsendelsen.

Udviklingen af kvantesikker kommunikation er aktuelt længere fremme relativt til kvantecomputeren. Kina har på forsøgsbasis eksempelvis etableret en 2.000 km lang kommunikationslinje baseret på kvanteteknologi, som via fiberkabel forbinder Beijing,

Jinan, Hefei og Shanghai. I 2016 opsendte Kina desuden en satellit ved navn ”Micius”, som kan facilitere kvantekommunikation på tværs af landegrænser.

Implementering af kvantekommunikation i stor skala på internettet vil imidlertid kræve enorme omstruktureringer af internettets nuværende opbygning.

Medarbejder inspicerer IBM's kvantecomputer "Q". FOTO: Connie Zhou/Ritzau Scanpix

Kommercielle interesser driver udviklingen

Udviklingen af både kunstig intelligens og kvanteteknologi i den vestlige verden bliver primært drevet af store private teknologivirksomheder.

For virksomhederne understøtter teknologierne betydelige kommercielle interesser bl.a. i form af first-mover-fordele ved udviklingen af selvkørende biler, videreudvikling af digitale assistenter og yderligere optimering af machine learning algoritmer.

Der er en risiko for, at kommercielle interesser overskygger behovet for at imødegå de nævnte sikkerhedsmæssige udfordringer for fremtidens samfund.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og plan-lægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynligheder i analyser

Bilag 12

Anders Lønvig

Fra: Jens Fauring <jef@fiberby.dk>
Sendt: 3. august 2020 16:31
Til: ENS - Center for Telekommunikation
Cc: Anders Lønvig; Christian Rosenskjold
Emne: Høringssvar fra Fiberby - journalnummer 2020 - 6701

Til Energistyrelsen

I forbindelse med høring over udkast til forslag til lov om ændring af lov om elektroniske kommunikationsnet og -tjenester, § 13 har Fiberby følgende kommentarer

1. Er politiets mistanke om terroraktivitet en forudsætning for udlevering af en slutbrugers basale oplysninger?
   For at imødegå terrortrusler fik politiet i 2005 udvidede beføjelser i forbindelse med reglerne i Telelovens nuværende §13 til let, dvs. uden kendelse, at få adgang til basale oplysninger om en slutbrugers adgang til elektronisk kommunikation.
   Fiberby oplever, at krav fra politiet om udlevering af en slutbrugers basale oplysninger med en enkelt udtagelse stammer fra sager, der vedrører økonomiske forhold.
   Politiet udstrækker dermed sine beføjelser udover loven!

2. Hvilken effekt har reglerne om politiets beføjelser til let adgang til en slutbrugers basale oplysninger haft hidtil, fx de sidste 12 måneder?
   Fiberby har godt 20.000 aktive slutbrugere, hvoraf knap 350 har en eller flere faste ip-adresser, dvs. mindre end 2% af det samlede antal slutbrugere.
   Vi har ikke været opmærksom på, at udlevering af en slutbrugers basale oplysninger uden kendelse begrænser sig til slutbrugere, der har en fast ip-adresse.
   Fiberby tilbyder både faste ip-adresser, offentlig dynamiske ip-adresser og Carrier Grade NAT
   Derfor bør begrænsningen med faste ip-adresser præciseres – gerne i bemærkninger til loven. Alternativt bør reglerne vedr. dynamiske ip-adresser og Carrier Grade NAT præciseres

Vi ser frem til svar på vores spørgsmål.

Med venlig hilsen

Jens Fauring | 20 89 68 64 |
IT-chef

FIBERBY | Otto Busses Vej 5 bygn. 048 | 2450 København SV | 33 23 00 99 |

Klima-, Energi- og Forsyningsministeriet
Holmens Kanal 20
1060 København K

Sendt per email til **tele@ens.dk** med kopi til **anl@ens.dk** og **chro@ens.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 10. august 2020

Høringssvar vedr. ændring af § 13 i lov om elektroniske kommunikationsnet og –tjenester (J.nr. 2020-6701)

Med lovudkastet foreslås anvendelsesområdet for § 13 i lov om elektroniske kommunikationsnet og –tjenester (teleloven) udvidet til at omfatte mobiltelefoners IMEI nummer. Politiet vil efter lovforslaget uden retskendelse kunne få udleveret oplysninger om de mobiltelefonnumre og abonnementsoplysninger (navn og adresse), som et givent IMEI-nummer (International Mobile Equipment Identity) har været tilknyttet, fordi SIM-kortet for disse abonnementer har været anvendt i mobiltelefonen med det pågældende IMEI nummer.

IT-Politisk Forening vil anbefale at dette lovforslag ikke fremsættes. For det første kan et IMEI-nummer ikke med nogen teknisk eller juridisk rimelighed opfattes som en abonnementsoplysning inden for rammerne af telelovens § 13. **For det andet, og mere væsentligt, strider lovforslaget mod EU-retten**, idet IMEI-nummeret er trafikdata i forhold til e-databeskyttelses-direktivet, og telelovens § 13 indeholder ingen materielle og processuelle betingelser, som regulerer politiets adgang til oplysninger hos mobiludbyderen.

Disse bemærkninger uddybes i det følgende.

IMEI-nummeret er ikke en abonnementsoplysning i forhold til telelovens § 13

Det fremgår af de specielle bemærkninger til telelovens § 13, at bestemmelsen alene omfatter oplysninger om adresser og numre, som udbyderen af elektroniske kommunikationsnet og -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger. I forhold til telefonitjenester vil politiet med bestemmelsen kunne få oplyst abonnementsnavn og -adresse ud fra et telefonnummer og telefonnumre tilknyttet en bestemt person. Der er ikke krav om, at udbyderen registrerer flere oplysninger end hvad der følger af telelovens § 31, stk. 2 og 3 (afgivelse af ”118” nummeroplysningsdata). Det fremhæves endvidere i bemærkningerne, at der er tale om statiske oplysninger.

IMEI-nummeret er en unik ”identitet” for den mobiltelefon, som slutbrugeren vælger at benytte. Det er ikke en oplysning, som mobiludbyderen har tildelt slutbrugeren i en konkret tjeneste. Der er heller ikke tale om en statisk oplysning som de egentlige abonnementsoplysninger (mobilnummer, navn og adresse), idet slutbrugeren frit kan flytte sit SIM-kort til andre telefoner.

De personoplysninger, som politiet kan få udleveret ved forespørgsel på et IMEI-nummer, er i visse situationer mere omfattende og indgribende i retten til privatliv end hvis politiet beder om at få oplyst abonnementsnavn for et telefonnummer. Et telefonnummer er kun tilknyttet en enkelt abonnement, mens et IMEI-nummer vil være tilknyttet alle de abonnenter, som har brugt deres SIM-kort i den pågældende telefon.

Logningsbekendtgørelsens § 4, nr. 5 kræver, at mobiludbydere ved enhver kommunikation (opkald og SMS/MMS) registrerer både IMSI (International Mobile Subscriber Identity, dvs. oplysninger om abonnentens SIM-kort) og IMEI. Efter logningsbekendtgørelsen skal disse oplysninger gemmes i et år. Det kan endvidere ikke udelukkes, at koblingen mellem IMSI og IMEI kan blive gemt i længere tid end et år, hvis en udbyder vurderer at oplysningerne er nødvendige for debitering (jf. § 23, stk. 2 i udbudsbekendtgørelsen).

Telelovens § 13 kræver ikke at politiets forespørgsel er begrænset til en kort tidsperiode, og efter de specielle bemærkninger til ændringslovforslaget er der ikke nogen grænser for hvor mange personer, der kan udleveres abonnementsoplysninger om. En udlevering efter § 13 kan i princippet omfatte en række personer, der har indgået i et socialt fællesskab, hvor de på en eller anden måde har delt mobiltelefoner med hinanden. Det er langt mere indgribende i retten til privatliv og databeskyttelse end udlevering af abonnementsoplysninger om en enkelt person, som er det normale anvendelsesområde for §13.

Det gælder uanset, at der formelt ikke er tale om et indgreb i meddelelseshemmeligheden efter retsplejelovens kapitel 71, fordi forbindelsen mellem de pågældende personer (deres ”sociale graf”) ikke er direkte knyttet til en elektronisk kommunikation (som opkaldsoplysninger for en telefonsamtale eller SMS/MMS besked).

For at opsummere første del af høringssvaret kan IMEI-nummeret efter IT-Politisk Forenings opfattelse ikke med nogen rimelighed opfattes som en abonnementsoplysning inden for rammerne af telelovens § 13, fordi der ikke er tale om en statisk oplysning som udbyderen har tildelt slutbrugeren (abonnementsoplysning), og fordi udleveringen af oplysninger tilknyttet et IMEI-nummer kan afsløre private relationer mellem flere personer.

Forhold til EU-retten

I henhold til e-databeskyttelsesdirektivet 2002/58/EF er IMEI-nummeret trafikdata, jf. mere specifikt dette direktivs betragtning nr. 15 samt præmis 40-42 i EU-Domstolens dom i sag C-207/16 Ministerio Fiscal (”data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf”).

Det betyder, at udlevering af oplysninger til politiet via behandling af IMEI-nummer skal opfylde kravene i e-databeskyttelsesdirektivets artikel 15, stk. 1, idet EU-Domstolen har fastslået, at artikel 15, stk. 1 finder anvendelse på alle retsforskrifter, som giver politiet adgang til trafikdata (jf. præmis 35 i C-207/16 og den deri nævnte retspraksis).

I parentes skal det i øvrigt bemærkes, at anledningen til den præjudicielle forelæggelse i C-207/16 var en sag, hvor den spanske anklagemyndighed med en kendelse fra en forundersøgelsesdomstol ønskede adgang til abonnementsoplysninger om brugerne af de SIM-kort, som inden for en kort periode (12 dage) havde været anvendt i en bestemt stjålet telefon (identificeret ud fra dens IMEI-nummer). Altså en adgang som svarer til den foreslåede ændring af telelovens § 13, bortset fra begrænsningen på tidsperioden (12 dage) i den spanske sag, som ikke indgår som en del af telelovens § 13.

Lovgivning om kompetente myndigheders adgang til lagrede trafikdata (herunder IMEI-numre) skal opfylde et af målene i artikel 15, stk. 1. Derudover skal lovgivningen opstille materielle og processuelle betingelser for kompetente myndigheders adgang som begrænser adgangen til det strengt nødvendige, jf. præmis 118 i Tele2-sagen (forenede sager C-203/15 og C-698/15).

For at sikre fuld iagttagelse af disse betingelser skal kompetente myndigheders adgang til de lagrede data være undergivet en forudgående kontrol af en domstol (eller en uafhængig administrativ myndighed), undtagen i behørigt begrundede hastende tilfælde (præmis 120 i Tele2-sagen).

De berørte personer skal have underretning om kompetente myndigheders adgang, så snart underretningen ikke kan skade disse myndigheders efterforskning. Denne underretning er ifølge EU-Domstolen ”de facto nødvendig for at gøre det muligt for disse personer navnlig at udøve den adgang til retsmidler, som udtrykkeligt er fastsat i artikel 15, stk. 2, i direktiv 2002/58” (præmis 121 i Tele2-dommen).

Ifølge præmis 51 i C-207/16 vil adgang til lagrede IMEI-oplysninger udgøre et indgreb i den grundlæggende ret til privatliv og databeskyttelse, jf. artikel 7 og 8 i Charter om Grundlæggende Rettigheder, foruden de rettigheder som e-databeskyttelsesdirektivet sikrer. Det gælder uanset at adgang til oplysninger om SIM-kort, der har været anvendt sammen med IMEI-nummeret inden for en kort periode, ifølge præmis 59-61 i C-207/16 ikke vil kunne karakteriseres som et alvorligt indgreb.

Når indgrebet ikke er alvorligt, stiller EU-retten ikke krav om, at adgang til lagrede data skal være begrænset til sager om bekæmpelse af grov kriminalitet (jf. præmis 53-57 i C-207/16). De øvrige betingelser for adgang til lagrede data, som opstilles i Tele2-dommen som fortolkning af e-databeskyttelsesdirektivets artikel 15, stk. 1 i lyset af Charteret, herunder krav om forudgående domstolskontrol og underretning af de berørte personer, gælder imidlertid også for indgreb som ikke kan karakteriseres som alvorlige.

Præmis 51 i C-207/16 henviser endvidere til EU-Domstolens udtalelse 1/15 om EU-Canada PNR-aftalen, hvor der ved kompetente myndigheders adgang til lagrede data som udgør et indgreb i grundlæggende rettigheder mere generelt stilles krav om materielle og processuelle betingelser, samt forudgående kontrol heraf ved en domstol eller en uafhængig administrativ myndighed.

Af punkt 63-65 i generaladvokatens forslag til afgørelse i EU-sagen C-746/18 Prokuratuur (fremsat 21. januar 2020) fremgår det ligeledes meget klart, at forudgående kontrol ved en domstol eller en uafhængig administrativ myndighed (bortset fra behørigt begrundede hastende tilfælde) og efterfølgende underretning af de berørte personer (så snart det ikke kan skade efterforskningen) er to betingelser som altid skal være opfyldt, når kompetente myndigheder får adgang til lagrede oplysninger omfattet af e-databeskyttelsesdirektivet.

Telelovens § 13 lever ikke op til disse krav i EU-retten, idet politiet får en generel adgang til ”oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet og -tjenester”, endda uden at betingelserne for edition skal være opfyldt. Politiet kan potentielt benytte denne adgang til formål, der falder uden for e-databeskyttelsesdirektivets artikel 15, stk. 1. Der er under alle omstændigheder ingen materielle og processuelle betingelser støttet på objektive kriterier som sikrer, at adgangen begrænses til det strengt nødvendige. Der er desuden hverken uafhængig domstolskontrol eller efterfølgende underretning af de berørte personer, som e-databeskyttelsesdirektivet artikel 15, stk. 1 eksplicit kræver efter EU-Domstolens retspraksis.

Af ovennævnte grunde kan telelovens § 13 på grund af EU-

retten ikke udstrækkes til at omfatte behandling af oplysninger der udgør trafikdata, herunder IMEI-nummeret.

PROSA
Forbundet af It-professionelle

Association of IT Professionals
Vester Farimagsgade 37A
1606 København V

Søren Frichs Vej 38K
8230 Åbyhøj

Overgade 54
5000 Odense

prosa.dk
+45 33 36 4141

Klima-, Energi- og Forsyningsministeriet
tele@ens.dk
Cc: anl@ens.dk, chro@ens.dk
Journalnummer 2020 - 6701

København, 11. august 2020

Høringssvar til ændring af § 13 i lov om elektroniske kommunikationsnet og –tjenester om *Initiativer til styrkelse af cybersikkerheden (2018/006599)*

Klima-, Energi- og Forsyningsministeriet sendte den 28. maj 2020 udkast til forslag til ændring af lov om elektroniske kommunikationsnet og -tjenester og forskellige andre love i høring.

PROSA – Forbundet af It-professionelle vil gerne kommentere på høringen.

Retssikkerhed

Helt generet finder PROSA det problematisk, at man laver speciallovgivning, som omgår borgernes rettigehder. Dermed er man desværre med til at undergrave Grundloven.

I Danmark ønsker vi med rette at kunne kritisere lande, som arbitrært invaderer borgeres privatliv eller fængsler kritikere af styret. Den kritik bliver sværere og sværere at fremføre, når Danmark selv indfører lovgivning som er med til at undergrave vores egne borgeres retssikkerhed.

Vi skal holde fast i at være en retsstat, og derfor skal vi holde fast i, at man skal have en retskendelse for at overvåge borgerne – også selvom det blot er at indhente metadata om teletrafik.

PROSA kan godt se det nødvendige i, at man i enkelte tilfælde er nødt til at handle for at øjeblikket ikke forspildes, men så må der indhentse en retskendelse efterfølgende.

Bemærkningerne viser ikke behovet for ændringen

Et IMEI-nummer er koblet til den fysiske telefon og ikke telefonnummeret, hvorimod SIM-kortet er koblet til telefonnummeret.

Det er derfor ikke korrekt, hvis man vil lave en sammenligning mellem IMEI-numre og telefonbøger, hvor det er offentligt hvem, der har hvilket nummer. Vi har jo heller ikke et register over hvem, der ejer den fysiske telefon, der er koblet på fastnettet.

IMEI-nummeret er dermed en forøgelse af oplysninger om en borgers privatliv, som kun bør kunne indhentes gennem en retskendelse.

I bemærkningerne til udkastet fortæller man ikke, hvorfor den nuværende ordning med retskendelse er for langsom. Det rejser flg. spørgsmål:

- Hvor lang tid tager det i praksis at få en retskendelse, hvis det haster?
- Hvor ofte vil man anslå, at man vil benytte de nye beføjelser?

Forbundet af It-professionelle

- Hvorfor kunne man i disse tilfælde ikke indhente en retskendelse?

PROSA diskuterer gerne, om vi skal gøre det nemmere og hurtigere at indhente en retskendelse, men bemærkningerne kommer ikke ind på, hvorfor der skulle være behov for at sikre en lettere adgang til metadata om teletrafik, og bemærkningerne nævner slet ikke, hvorfor det skulle være nødvendigt ikke at indhente retskendelse.

PROSAs anbefaling

PROSA anbefaler derfor, at forslaget ændres, så det præciseres, at der altid skal indhentes en retskendelse, før politiet får adgang til en mobiltelefons IMEI-nummer. Herved opnås den ønskede præcisering af fortolkningen af bestemmelsen om udlevering af basale oplysninger på baggrund af en identifikation af slutbrugeren baseret på IMEI-nr.

Venlig hilsen

Niels Bertelsen

Formand

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Til Klima-, Energi og Forsyningsministeriet

Sendt pr. mail til: ENS - Center for Telekommunikation tele@ens.dk; Anders Lønvig anl@ens.dk; Christian Rosenskjold CHRO@ens.dk; Thomas Jønsson thojn@kefm.dk; Tore K. Christensen tkc@ens.dk

11. august 2020

Høring over udkast til forslag til ændring af Telelovens § 13

Teleindustrien (TI) vender hermed tilbage med høringssvar i anledning af tillægshøringen om udkast til ændring af Telelovens § 13 (jeres J.nr. 2020 -6701).

TI har følgende bemærkninger til lovudkastet:

A. TI har forståelse for, at IMEI-oplysning er et vigtigt efterforskningsmæssigt værktøj for politiet, og noterer sig regeringens ønske at skabe hjemmel til, at teleselskaberne på politiets begæring skal udlevere IMEI-oplysning uden rettens godkendelse.

B. TI finder imidlertid udkastet til ændring af telelovens § 13 og de tilhørende udkast til lovbemærkninger for uhensigtsmæssig. Lovudkastet skaber efter TI's opfattelse *ikke* den ønskede klare hjemmel til, at politiet får adgang til IMEI-oplysning uden rettens godkendelse. Udkastet til ændring af ordlyden af selve § 13 indebærer således ikke i sig selv en indholdsmæssig ændring af § 13, og udkastet til bemærkninger til lovforslaget er ikke retvisende i forhold til gældende praksis. Endvidere vil udkastet til lovforslagsbemærkninger kunne bidrage til uklarhed om bestemmelsens rækkevidde, jf. nærmere nedenfor i **Bilag A** om TI's konkrete bemærkninger til lovudkastet. Udkastet til lovforslagsbemærkningerne beskriver, hvordan bestemmelsen skal "fortolkes", hvilket er en usædvanlig lovmodel, idet lovgiver kan udstede præcise regler, hvorefter det er op til domstole m.fl. at fortolke eventuelle upræcise bestemmelser. TI må på den baggrund opfordre til en revurdering af den foreslåede lovmodel.

C. TI foreslår, at lovudkastet i stedet ændres til en særskilt og præcis regel, som giver politiet den ønskede adgang til IMEI-oplysning uden rettens godkendelse. Reglen kan fx formuleres på følgende måde:

> *"Udbydere af elektroniske kommunikationsnet og -tjenester til slutbrugere skal på politiets begæring udlevere registrerede oplysninger om, hvilke*

mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt (IMEI-oplysning)".

D. TI opfordrer til, at den nye regel om udlevering af IMEI-oplysning placeres i retsplejelovens kapitel 71 (og ikke i teleloven), idet IMEI-oplysninger er logningspligtige data – dvs. data, som teleselskaberne udelukkende registrerer som følge af kravet herom i logningsreglerne. Behandlingen af lovforslag om udlevering af loggede data bør efter TI's opfattelse ske i regi af Folketingets Retsudvalg (REU) – og ikke i regi af Folketingets Klima-, Energi- og Forsyningsudvalget (KEF). TI opfordrer til, at alle regler om udlevering af loggede teledata samles i retsplejelovens kapitel 71. I RPL kapitel 71 findes allerede både hjemmelsbestemmelsen om logning af teledata, herunder IMEI-oplysning, samt reglerne om udlevering af teledata ifm indgreb i meddelelseshemmeligheden og teleobservation (masteoplysninger). Det vil derfor være naturligt og samtidig skabe gennemsigtighed i reguleringen, hvis yderligere regler om udlevering af loggede teledata placeres i retsplejeloven.

E. TI opfordrer i øvrigt til, at udstedelse af regler om udlevering af IMEI-oplysning (som er loggede data) afventer den kommende revision af retsplejelovens regler om logning og udlevering af teledata, som forventes at skulle ske i efteråret 2020 efter EU-domstolens afsluttende behandling af de verserende sager om logning af teledata. TI finder det naturligt at udskyde udstedelsen af nye regler om IMEI-oplysning til den nært forestående revision af retsplejeloven – fremfor at udstede regler om udlevering af logningspligtige teledata via teleloven.

F. TI opfordrer konkret til, at det afklares om udkastet til ændring af telelovens § 13 ligger inden for rammerne af EU-retten. Ved at afvente EU-domstolens kommende afgørelse, kan det samtidig afklares, om det overhovedet er lovligt, at give politiet en generel direkte adgang til loggede teledata i form af IMEI-oplysninger. Den seneste EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) beskriver således, at artikel 15, stk. 1 i e-datadirektivet 2002/58/EF – som udgør den bagvedliggende EU-regel om logningsreglerne – er til hinder for national lovgivning, der giver politiet adgang til lagrede data "*uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …*".

G. TI bemærker i øvrigt, at det hidtil har været normal praksis, at teleselskabernes udlevering af teledata til politiet, herunder loggede data om IMEI-oplysning, er sket efter rettens kendelse og efter reglerne i retsplejeloven. Telebranchen vil naturligvis fortsat gerne bidrage til og understøtte politiets efterforskningsarbejde, og igennem mange år har der eksisteret et godt og konstruktivt samarbejde mellem politiet og teleselskaberne. Det er i den forbindelse TI's opfattelse, at der skal foreligge et klart hjemmelsgrundlag for teleselskabernes udlevering af teledata til politiet – enten i form af rettens kendelse eller i form af en klar lovhjemmel – og at det således skal være domstolene eller lovgiver og ikke teleselskaberne, der foretager vurderingen af, hvornår udlevering af teledata til politiet er berettiget.

Baggrund for TI's forslag og kritik:

1. TI har i februar 2020 opfordret til, at regler om udlevering af IMEI-oplysning fastsættes med hjemmel i Retsplejelovens kapitel 71. TI henviser til pkt. 4.4. i Teleindustriens notat om teledata (http://www.teleindu.dk/brancheholdninger/logning-og-teledata/), som er sendt til Justitsministeriet og Rigspolitiet med kopi til Energistyrelsen den 28. februar 2020.

2. TI finder det uhensigtsmæssigt, at udstede en lov, som ikke i sig selv indeholder en ny regel, men som blot indeholder bemærkninger, der beskriver, hvordan en gældende regel skal fortolkes. TI har i juni 2020 redegjort for, at den gældende regel i telelovens § 13 netop ikke vedrører loggede data i form af IMEI-oplysning, men derimod kun vedrører udlevering af de kundeoplysninger, som teleudbydere registrerer i kunde-/ordresystemer som led i den forretningsmæssige drift. TI henviser til TI's brev den 4. juni 2020 til Energistyrelsen i **bilag B** nedenfor, hvor TI bl.a. påpeger:
- at det fremgår af de gældende lovforslagsbemærkninger til TL § 13, at bestemmelsen kun vedrører statiske identifikationsoplysninger, som teleudbyderen har tildelt slutbrugeren som led i et abonnementsforhold, og som ikke findes i 118-databasen.
- at mobilselskaberne ikke tildeler mobilkunderne et IMEI-nummer, idet IMEI-nummeret er terminalens stelnummer, som hidrører fra terminalproducenten.
- at IMEI-nummeret ikke er statisk ift. slutbrugerens abonnement, idet slutbrugeren kan udskifte terminalen ved at sætte SIM-kortet over i en anden mobiltelefon. For et mobilabonnement er det SIM-kortet/IMSI og mobilnummeret, der statisk identificerer slutbrugerens adgang til tjenesten og registreres som kundedata – men derimod ikke terminalen/IMEI, som kunden kan udskifte.
- at formålet med den gældende § 13 er at forpligte teleudbyderne til at give politiet direkte adgang til kundedata om bredbåndsabonnementer (navn, adresse, fast IP-adresse og mail-adresse) – svarende til kundedata i form af nummeroplysningsdata/118-data for et telefoniabonnement (som politiet også har direkte adgang til uden kendelse, jf. telelovens § 31).
- at IMEI-nummer ikke er kundedata, men data som ikke findes i teleselskabernes kundedatabaser. Loggede data i form af IMEI-nummer registreres og opbevares i teleselskabernes "politisystemer" – og registreringen i 1 år sker udelukkende som følge af logningsreglerne.
- at det fremgår tydeligt af lovforslagsbemærkningerne til den gældende § 13 i teleloven, at loggede data, herunder IMEI-oplysning ikke er omfattet af reglen om politiets direkte adgang, idet udlevering af loggede data kræver kendelse: "Det skal bemærkes, at oplysninger, som udbyderne alene ligger inde med som følge af logningspligten, kun skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven".

TI bemærker supplerende, at baggrunden for den gældende regel i telelovens § 13 er "anbefaling 28" i Regeringens handlingsplan for terrorbekæmpelse, november 2005, som blev udmøntet antiterror-lovpakke II fremsat i foråret 2006, jf. lovforslag L219 til

ændring af teleloven fremsat 31. marts 2006. Baggrunden for anbefaling 28 om "pligt til at udlevere abonnementsoplysninger uden rettens kendelse" er beskrevet på følgende måde i lovforslagsbemærkningerne til det oprindelige lovforslag fra 2006 og den bagvedliggende rapport fra 'Den tværministerielle arbejdsgruppe om terrorbekæmpelse om terrorbekæmpelse', oktober 2005:

> "**Pligt til udlevering af abonnementsoplysninger uden rettens tilladelse**
> I forbindelse med efterforskning af alvorlig kriminalitet, herunder de i straffelovens kapitel 12 og 13 nævnte forbrydelser, vil der ofte være situationer, hvor politiet, herunder Politiets Efterretningstjeneste, vil have behov for oplysninger om en mistænkts adgang til kommunikation udover de oplysninger, der fremgår af 118-databasen. Det vil f.eks. kunne være oplysninger om en persons adgang til internettet, andre mobiltelefonnumre m.v.
>
> En umiddelbar adgang til ovenstående oplysninger vil sikre, at politiet straks i et efterforskningsforløb vil kunne blive bekendt med samtlige relevante oplysninger om en mistænkts eventuelle kommunikationsmuligheder.
>
> **28**. *Arbejdsgruppen anbefaler, at der pålægges udbydere af telenet- og teletjenester at udlevere abonnementsoplysninger uden rettens godkendelse."*

3. Politiet har aldrig før 2020 henvist til telelovens § 13 som hjemmel til udlevering af IMEI-oplysning. Det har således hidtil været forskelligt fra teleudbyder til teleudbyder om udlevering er sket efter editionskendelse eller efter interesseafvejning (såkaldt "frivillig udlevering"). Men i mere end 20 år har telelovens § 13 aldrig været anvendt som udleveringshjemmel i forhold til IMEI-oplysning. Først i februar 2020 er politiet begyndt at henvise til telelovens § 13 som udleveringshjemmel. Teleudbyderne har udtrykt bekymring vedrørende dette overfor Rigspolitiet.

4. TI beder om, at der i reglerne om udlevering af teledata sondres tydeligt mellem udlevering af data, som findes i teleudbydernes kunde-systemer uanset logningsreglerne (disse data kan udleveres iht. telelovens § 13) hhv. udlevering af loggede data (disse data bør udleveres efter reglerne i retsplejeloven). Hvis regeringen fastholder, at regler om udlevering af IMEI-oplysning skal udstedes med hjemmel i teleloven, uanset at der er tale om loggede data, anmoder TI om, at dette sker via særskilt hjemmel – fx i form af en ny § 13a. Idet IMEI-oplysning er data der behandles i forbindelse med udbud af elektronisk kommunikation, falder området under Erhvervsministeriets ressort, og TI foreslår derfor i øvrigt, at Erhvervsstyrelsen inddrages i det lovforberedende arbejde.

5. Lovudkastet synes at lægge op til, at den nye regel kun skal omfatte udlevering af 'IMEI -> navn/nummer' men ikke 'navn/nummer -> IMEI'. Idet begge disse ydelser er

basereret på og muliggøres af teleudbydernes lovpligtige logning af hvilket IMEI-nummer, der anvendes til en kommunikation, bemærker TI, at det vil være ulogisk og forvirrende, hvis ikke begge disse bliver omfattet af den nye regel. TI bemærker endvidere, at 'IMEI -> navn/nummer' typisk omfatter flere kunder, idet en mobiltelefon kan udskiftes og overdrages til andre slutbrugere. Omvendt omfatter oplysning om 'navn/nummer -> IMEI' altid kun én slutbruger. 'IMEI -> navn/nummer' er således en mere indgribende ydelse end 'navn/nummer -> IMEI', hvilket understreger det ulogiske i kun at indføre en lempet udleveringshjemmel for den mest indgribende ydelse.

I **Bilag A** findes TI's konkrete bemærkninger til lovudkastet, hvortil der henvises.

Med venlig hilsen

Jakob Willer, direktør, Teleindustrien

Bilag A. TI's konkrete bemærkninger til lovudkastet:

Simpel regel
Lovforslagets bemærkninger indeholder 2½ sides tekst, som kan medføre ny fortolkningstvivl. Hvis regeringen fastholder at gennemføre reglen om udlevering af IMEI-oplysning med den foreslåede ændring til telelovens § 13, anbefaler TI derfor, at alle bemærkninger til lovudkastet slettes, bortset fra 1. afsnit under "almindelige bemærkninger", og erstattes af følgende simple tilføjelse til lovforslagsbemærkningerne:

> *"Formålet med tilføjelsen til bestemmelsen er at forpligte udbydere af elektroniske kommunikationsnet og -tjenester til slutbrugere til – på politiet begæring – at udlevere registrerede oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt (IMEI-oplysning)".*

Hvis de 2½ sides lovforslagsbemærkninger fastholdes har TI følgende bemærkninger:

"Basale oplysninger"
På side 1 og 2 i udkastet til lovbemærkninger omtales flere steder, at teleudbyderne skal udlevere "*basale oplysninger*". Det er ganske uklart, hvad der menes med dette nye begreb. For at undgå ny begrebsforvirring, anmoder TI om, at begrebet ændres til enten "kundedata" (i modsætning til trafikdata) eller "abonnementsoplysninger", som nævnt i den bagvedliggende "anbefaling 28", som er citeret i det oprindelige lovforslag L219 fra 2006 som nævnt ovenfor.

Det bemærkes desuden, at IMEI-oplysning (enten 'abonnement til IMEI-nummer' eller 'IMEI-nummer til abonnenter') på ingen måde kan anses for at være en "basal oplysning", idet IMEI-nummeret ikke indgår i de registreringer af kundedata/abonnementsoplysninger, som teleudbyderne selv har et forretningsmæssigt behov for at registrere. IMEI-nummer og sammenhængen mellem IMEI-nummer og abonnenter registreres kun som følge af logningskravet.

"Identifikation af slutbrugeren baseret på IMEI-nr."
På side 1 i udkastet til lovbemærkninger omtales *"identifikation af slutbrugeren baseret på IMEI-nr."*. TI bemærker hertil, at det ikke er muligt entydigt at identificere en slutbruger på baggrund af et IMEI-nummer. Søgning på, hvem der i en given periode har brugt et IMEI-nummer (en mobiltelefon) kan således omfatte flere slutbrugere, idet en mobiltelefon kan udskiftes og overdrages til andre slutbrugere.

"Betydning og rækkevidden af telelovens § 13".
På side 1 i udkastet til lovbemærkninger er anført: *"Henset til den centrale betydning indhentningen af oplysninger efter telelovens § 13 har antaget i praksis, aktualiserer denne tvivl et behov for mere klart at fastlægge bestemmelsens rækkevidde med henblik på at sikre teleudbyderne og politiet entydige retlige rammer for det daglige samarbejde"*.

TI bemærker hertil, at telelovens § 13 efter TI's opfattelse ikke hidtil har haft en central betydning. Den gældende bestemmelse har således været brugt til udlevering uden kendelse af kundeoplysning om kunden bag en fast IP-adresse eller en mail-adresse (eller omvendt). Faste IP-adresser anvendes kun af et fåtal af kunder, og bestemmelsen har derfor i den sammenhæng kun være anvendt sjældent.

Udlevering af andre oplysninger
På side 1 i udkastet til lovbemærkninger er anført: "*Oplysninger om hvem den givne slutbruger har kommunikeret med er ikke omfattet, da sådanne oplysninger, er omfattet af meddelelseshemmeligheden. Adgang til sådanne oplysninger kræver, at politiet indhenter retskendelse efter retsplejelovens kapitel 71*".

TI anmoder om, at teksten enten slettes eller at det tilføjes at "masteoplysninger" og "oplysning om dynamiske IP-adresser" heller ikke er omfattet.

'Navn til IP-nummer' og 'IP-nummer til navn'
På side 1 og side 2 i udkastet til lovbemærkninger er anført:

"*Det fremgår af lovbemærkningerne til telelovens § 13, jf. Folketingstidende 2010-11, A, L 59 som fremsat, side 49, at der både er tale om, at navn til et bestemt nummer oplyses, og omvendt at nummer til et bestemt navn oplyses*".
og
"Det fremgår af lovbemærkningerne, jf. Folketingstidende 2010-11, A, L 59 som fremsat, side 49, at § 13 medfører, at navn til et bestemt nummer oplyses, og omvendt at nummer til et bestemt navn oplyses."

TI bemærker, at de citerede tekster fra de oprindelige lovforslag efter deres sammenhæng i de oprindelige lovforslag vedrører "IP-nummer" (fast IP-adresse) og ikke bare "nummer". Teksten om, at bestemmelsen omfatter både '(IP-)nummer til navn' og 'navn til (IP-)nummer' er i øvrigt indsat efter forslag fra TI i høringen i 2006 over udkast til det oprindelige lovforslag. Med henblik på at undgå ny fortolkningstvivl anmoder TI om, at gengivelsen af de gældende lovforslagsbemærkninger enten udgår eller citeres i deres helhed. Hvis den delvise omtale af de eksisterende lovforslagsbemærkninger fastholdes i lovudkastet anmoder TI om, at det præciseres, at der menes "IP-nummer" (fast IP-adresse).

Typer af oplysninger omfattet af § 13
På side 1-2 i udkastet til lovbemærkninger er anført:

"*Der fremgår yderligere [af lovbemærkningerne til den gældende § 13], at der som følge af den almindelige teknologiske udvikling vil kunne opstå nye typer af oplysninger, der kan betegnes som oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, og som kan tjene til at identificere en bestemt slutbruger.*

Det fremgår desuden, at oplysninger, som udbyderne alene ligger inde med som følge af logningspligten, kun skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven. …
For så vidt angår spørgsmålet om udlevering på baggrund af IMEI-nr. er der i telelovens § 13 eller bemærkningerne hertil, jf. Folketingstidende 2010-11, A, L 59 som fremsat, side 49, ikke taget udtrykkelig stilling til, om politiet kan forlange oplysninger udleveret på baggrund af et IMEI-nr. Retstilstanden beror derfor på en fortolkning af bestemmelsen, der hermed foreslås præciseret"

TI bemærker hertil, at IMEI-oplysning har været en ydelse, som teleudbyderne har leveret til politiet i mere end 20 år – og længe inden udstedelsen af telelovens § 13 i 2006. Hvis IMEI-oplysning havde været omfattet af den gældende § 13, ville ydelsen naturligvis have været nævnt i lovforslagsbemærkninger til bestemmelsen.

TI bemærker endvidere, at oplysninger om hvilke abonnementer, der har brugt et IMEI-nummer/terminal hhv. hvilke IMEI-numre/terminaler, der har været brugt af et mobilabonnement er loggede oplysninger, som teleudbyderne alene registrerer som følge af kravet herom i logningsbekendtgørelsen. IMEI-oplysning er derfor efter TI's opfattelse ikke omfattet af de gældende regler, og det er efter TI's opfattelse misvisende at skrive i lovudkastet, at retstilstanden beror på en fortolkning af bestemmelsen. Hvis lovgiver ønsker at forpligte teleudbyderne til at udlevere IMEI-oplysning uden kendelse, bør dette ske via en ny præcis regel om udlevering af sådanne logningspligtige oplysninger.

TI finder det generelt unødvendigt at gengive lovbemærkningerne til det oprindelige lovforslag. Hvis gengivelsen bibeholdes, opfordrer TI til, at følgende afsnit fra de oprindelige lovbemærkninger også gengives: "*Udbyderne forpligtes ikke til at registrere og gemme oplysninger, ud over hvad der allerede følger af den foreslåede § 31, stk. 2 og 3, om afgivelse af nummeroplysningsdata, men forpligtes alene til at udlevere oplysninger, som udbyderen i øvrigt måtte være i umiddelbar besiddelse af om en slutbrugers adgang til kommunikationsnet og -tjenester*". Som det fremgår af citatet, er IMEI-oplysning ikke omfattet af den gældende § 13, idet teleudbyderne kun registrerer IMEI-oplysning som følge af reglerne i logningsreglerne, og således netop ikke er i umiddelbar besiddelse af IMEI-oplysninger.

Masteoplysninger og lokaliseringsdata
På side 2 i udkastet til lovbemærkninger er anført: *"For så vidt angår udlevering af oplysninger knyttet til et IMEI-nummer – i lighed med basale oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester, bemærkes det, at denne type oplysninger ikke nyder særlig beskyttelse efter retsplejelovens bestemmelser. Udlevering af oplysninger om f.eks. hvilke telefonnumre, der har været tilknyttet det pågældende IMEI-nr., uden ledsagende oplysninger om f.eks. indholdet af kommunikation eller lokaliseringsoplysninger kan således ikke antages kun at kunne ske efter reglerne i retsplejeloven om indgreb i meddelelseshemmeligheden eller edition. Oplysninger med tilknytning til et IMEI-nr. eller om aktivitet på et telenet*

med tilknytning til et IMEI-nr., kan således ikke antages alene at kunne udleveres efter retskendelse, men må anses for omfattet af telelovens § 13".

En tilsvarende tekst findes på side 3 i lovbemærkningerne.

TI bemærker hertil, at udlevering af masteoplysninger og lokaliseringsdata heller ikke nyder særlig beskyttelse efter reglerne i retsplejelovens kapitel 71 – og i lighed med IMEI-oplysning udleveres masteoplysninger og lokaliseringsdata i dag til politiet efter editionskendelse. Rækkevidden af lovudkastet er generelt upræcist, og det fremstår uklart om formålet med lovændringen også er, at andre typer af oplysninger end IMEI-oplysning, skal udleveres til politiet uden kendelse. TI opfordrer derfor igen til, at regler om udlevering af IMEI-oplysning udstedes med en klar og direkte lovhjemmel.

TI bemærker endvidere, at det synes uklart, hvad der menes med sætningen "*Oplysninger med tilknytning til et IMEI-nr. eller om aktivitet på et telenet med tilknytning til et IMEI-nr. …"*. Samme ordlyd har været drøftet mellem telebranchen og Rigspolitiet på møderne i Rigspolitiets Brancheforum, og TI har også i den sammenhæng gjort opmærksom på, at telebranchen ikke forstår, hvad der menes. TI anmoder om, at teksten udgår eller omskrives.

TI finder det uhensigtsmæssigt, at der i bemærkningerne til lovudkastet anvendes begreber som "kan således ikke antages" og "må anses for omfattet af telelovens § 13". Lovgivers rolle er at udstede regler, og ikke via bemærkninger til lovforslag at bidrage til en diskussion om, hvad der "kan antages", og hvad der "må anses".

TI er ikke enig i det afslutningsvist anførte i det citerede afsnit om, at IMEI-nr. "må anses for omfattet af telelovens § 13". Hvis lovgiver ønsker at fastsætte regler om, at teleudbyderne uden kendelse skal udleverede loggede oplysninger om sammenhængen mellem IMEI-nummer og abonnementer (IMEI-oplysninger), opfordrer TI igen til, at der fastsættes en præcis regel herom.

Udlevering af logningspligtige data

På side 3 i udkastet til lovbemærkninger er anført: "*Med henblik på at adressere den tvivl om bestemmelsens rækkevidde, der er opstået i praksis, tilsigtes det med den foreslåede bestemmelse at præcisere, at det forhold, at en given oplysning om en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester samtidig måtte være omfattet af den registrerings- og opbevaringspligt, som følger af logningsbekendtgørelsen, ikke medfører, at oplysningen er undtaget fra den udleveringspligt, der følger af §13".*

TI bemærker, at det anførte er i direkte modstrid med lovbemærkningerne til den gældende § 13, hvor følgende fremgår: *"Det skal bemærkes, at oplysninger, som udbyderne alene ligger inde med som følge af logningspligten, kun skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven*".

Frivillig udlevering af oplysninger om teknisk udstyr og købssted for SIM-kort
På side 3 i udkastet til lovbemærkninger er anført: *"Samtidig vil oplysninger, der ikke vedrører andres brug af nettet eller tjenesten eller indholdet heraf, jf. telelovens § 7 – f.eks. om teknisk udstyr, hvor et SIM-kort er købt mv. – fortsat kunne udleveres frivilligt af teleudbyderen i overensstemmelse med de generelle databeskyttelsesretlige regler*".

TI er ikke enig i, at de nævnte oplysninger om teknisk udstyr og købssted for SIM-kort kan udleveres til politiet uden editionskendelse. TI finder det i øvrigt besynderligt, hvis lovbemærkningerne til telelovens § 13 forholder sig til fortolkningen af de generelle databeskyttelsesregler. For at undgå ny begrebsforvirring og fortolkningstvivl opfordrer TI til, at ovennævnte passus udgår af lovforslaget.

BILAG B: TI's brev til ENS 4. juni 2020 om IMEI-oplysning og Teleloven pgr 13

Til Energistyrelsen

Att.: Signe Schmidt og Tore Christensen

c.c.: Rigspolitiet

Sendt pr. mail til ens@ens.dk

4. juni 2020

IMEI-oplysning og Teleloven pgr 13

Teleindustrien (TI) takker for drøftelsen med Energistyrelsen den 28. maj 2020 og den efterfølgende mail, hvor Energistyrelsen bl.a. foreslår en præcisering i Teleloven om hjemmel til udlevering af loggede oplysninger om IMEI-nummer.

TI deltager gerne i det foreslåede møde mandag den 8. juni 2020, kl. 12. TI vil sørge for at indkalde repræsentanter for de fire mobilselskaber.

Som oplæg til mødet ønsker TI med dette notat at skitsere Teleindustriens vurdering af hjemmelsgrundlaget for teleselskabernes udlevering til politiet af loggede oplysninger om IMEI-nummer (IMEI-oplysning) – herunder Teleindustriens vurdering af om den gældende regel i telelovens § 13 indeholder hjemmel til udlevering af IMEI-oplysning. Som det fremgår nedenfor, er TI ikke enig i Rigspolitiets notat den 14. maj 2020 fortolkning af telelovens 13.

Teleindustrien hilser Energistyrelsen forslag om lovhjemmel til udlevering af IMEI-oplysning velkommen. Som det fremgår nedenfor – og i TI's notat om teledata fremsendt til Justitsministeriet den 28. februar 2020 – finder TI dog, at lovhjemmel om teleselskabernes udlevering af IMEI-oplysning til politiet mest naturligt hører hjemme i Retsplejelovens kapitel 71, således at regler om logning af teledata og regler om udlevering af teledata til politiet fortsat reguleres samlet. TI finder det således ikke hensigtsmæssigt at lade teleloven regulere udlevering af loggede data til politiet. Idet IMEI-oplysning er loggede data anbefaler Teleindustrien endvidere, at fastsættelsen af regler om udlevering af IMEI-oplysning afventer EU-domstolens kommende afgørelse, jf. nærmere herom nedenfor.

Hvad er IMEI-oplysning

IMEI-oplysning er defineret i samarbejds- og ydelsesaftalerne mellem Rigspolitiet og teleudbyderne som ”Oplysning af, hvilke telefonnumre, der har været anvendt i en terminal, eller oplysning om, hvilke terminaler, der har været anvendt ifm et bestemt telefonnummer”.

TI har noteret det anførte i Energistyrelsens mail den 29. maj 2020 om, at Rigspolitiet overfor Energistyrelsen har anført, ”*at IMEI-nummeret … i høj grad er statisk, idet det er fast tilknyttet en bestemt telefon*”.

TI anerkender, at IMEI-oplysning er et vigtigt efterforskningsmæssigt værktøj for politiet. Men TI gør for god ordens skyld opmærksom på, at IMEI-nummeret *ikke* er en statisk registrering i forhold til mobilselskabernes abonnenter. IMEI-nummer er således en mobilterminals unikke ”stelnummer” (International Equipment Identity) og er *ikke* fast knyttet til en slutbrugers abonnement, ligesom IMEI-nummer ikke indgår i de abonnementsoplysninger, som er fast registreret i teleselskabernes kunde-/ordresystemer.

IMEI-oplysning er derimod data, som findes i mobilselskabernes netværkselementer, hvor IMEI-nummer kan opsamles enten via teleselskabernes probesystemer (til brug for fejlretning) eller i CDR-data (call data records), hvorfra data kan opsamles og registreres i mobilselskabernes ”politisystemer” med henblik på opfyldelse af logningsbekendtgørelsens krav om opsamling og registrering af IMEI-nummer i 1 år.

I forhold til reglerne om logning og udlevering af loggede data til politiet, kan ”IMEI-oplysning” (mobilnummer->IMEI’er) bedst sammenlignes med ”masteoplysning”, om hvilke masterceller et mobilabonnement har været registreret på. Tilsvarende kan IMEI-oplysning om hvilke abonnementer/SIM, der har været anvendt i en bestemt terminal (IMEI->mobilnumre) bedst sammenlignes med oplysning om hvilke terminaler, der har været anvendt på en mastecelle (udvidet masteoplysning). Både masteoplysning og IMEI-oplysning er således ikke-statiske oplysninger, der udelukkende registreres i 1 år for at opfylde logningskravet i logningsbekendtgørelsen, og både for masteoplysning og IMEI-oplysning gælder, at sammenhængen mellem telefonnummeret og de loggede data (både nummer>IMEI og IMEI>numre) kun kan udledes som følge af logningskravet.

TI's forslag til definition af nyt tvangsindgreb: IMEI-oplysning

TI henviser til Teleindustriens notat om teledata (http://www.teleindu.dk/brancheholdninger/logning-og-teledata/), som er sendt til Justitsministeriet og Rigspolitiet med kopi til Energistyrelsen den 28. februar 2020.

Følgende fremgår af notatets pkt. 4.4.:

"TI foreslår, at der fastsættes regler i RPL kap 71 om et nyt tvangsindgreb, 'IMEI-oplysning', som giver politiet adgang til oplysninger om, hvilke mobilterminaler der har været anvendt til et bestemt telefonnummer og omvendt.

Registreringen af data om IMEI-nummer i 1 år sker udelukkende for at opfylde kravet i logningsbekendtgørelsen, idet teleselskaberne selv kun har brug for at registrere data om IMEI-nummer i en ganske kort periode til brug for fejlretning.

Ved en IMEI-oplysning oplyser teleselskabet til politiet, hvilke mobilterminaler, der har været anvendt til et bestemt telefonnummer (fokusnummeret) – og desuden om de identificerede mobiltelefoner omvendt har været anvendt sammen med andre telefonnumre og sim-kort end fokusnummeret. Oplysninger om, hvem der har været kommunikeret med, er ikke omfattet af IMEI-oplysning og kræver særskilt kendelse om teleoplysning, jf. RPL § 780, stk. 1, nr. 3.

Teleselskabernes udlevering af oplysninger til politiet om IMEI-numre og IMSI-numre er hidtil sket efter reglerne om edition. Der er således ikke fastsat regler i retsplejelovens kap 71, der definerer et tvangsindgreb ift. udlevering af oplysninger om IMEI-nummer mv. til politiet – på trods af, at der i medfør af retsplejelovens kapitel 71 (§ 786, stk. 4) er fastsat regler om logning af IMEI-nummer.
…
Det er TI's opfattelse, at der altid som minimum skal foreligge en editionskendelse, når der udleveres teledata til politiet, da det som nævnt i pkt. 4 i dette notat, er TI's opfattelse, at der bør defineres tvangsindgreb for enhver form for udlevering af trafik- og lokaliseringsdata til politiet.

Set i lyset af EU-domstolens afgørelse i EU-dom om logning fra 2016 (C-203-15, Tele2-Watson) finder TI det desuden uafklaret, om udlevering af loggede data om IMEI-nummer fortsat kan ske efter reglerne om edition uden samtidig stillingtagen til graden af den kriminalitet, der efterforskes. Det fremgår således af EU-dommen fra 2016, at artikel 15, stk. 1 i e-datadirektivet (2002/58/EF) er til hinder for national lovgivning, der giver politiet adgang til lagrede data "uden i forbindelse med bekæmpelse af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet …".

På den baggrund, foreslår TI konkret, at nyt tvangsindgreb – som fx kan benævnes 'IMEI-oplysning' eller 'terminal-oplysning' – defineres på følgende måde med direkte

lovhjemmel i RPL kapitel 71 – f.eks. i tilknytning til reglerne i § 780 om indgreb i meddelelseshemmeligheden:

> *[NY § i RPL kap 71]:*
> *Politiet kan fra udbydere af elektroniske kommunikationsnet og -tjenester indhente oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt (IMEI-oplysning), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen. "*

Telelovens § 13

Teleindustrien har gennemgået telelovens § 13 og lovforslagsbemærkningerne hertil (se bilag nedenfor), og det er TI's vurdering, at IMEI-oplysning ikke er omfattet af bestemmelsen.

Teleindustriens vurdering er baseret på, at det fremgår af lovforslagsbemærkningerne til TL § 13, at bestemmelsen kun vedrører statiske identifikationsoplysninger, om adresser eller numre, som teleudbyderen har tildelt slutbrugeren som led i en konkret tjeneste, og som ikke findes i 118-databasen.

Teleindustrien forstår herefter TL § 13 sådan, at bestemmelsen vedrører udlevering til politiet – uden kendelse – af oplysning om numre mv., som teleudbyderen tildeler kunden som led i et abonnementsforhold. Mobilselskaberne tildeler imidlertid ikke mobilkunderne et IMEI-nummer som et led i mobilselskabernes udbud af mobiltjenester. IMEI-nummeret er således blot terminalens stelnummer, som hidrører fra terminalproducenten.

IMEI-nummeret er desuden ikke statisk, idet slutbrugeren kan udskifte terminalen ved at sætte SIM-kortet over i en anden mobiltelefon. For et mobilabonnement er det SIM-kortet/IMSI og mobilnummeret, der identificerer slutbrugerens adgang til mobiltjenesten – men derimod ikke terminalen/IMEI, som kunden kan udskifte.

I lovforslaget nævnes faste IP-adresser og e-mail-adresser som eneste aktuelle eksempler på identifikationsoplysninger omfattet af TL § 13, og Teleindustrien forstår derfor, at bestemmelsens sigte er at forpligte teleudbyderne til at give politiet adgang til statisk tildelte identitetsoplysninger for bredbåndsabonnementer – nemlig faste IP-adresser, e-mail-adresser og evt. kredsløbsnumre – som svarer til nummeroplysningsdata/118-data for et telefoniabonnement (som politiet også har adgang til uden kendelse, jf. telelovens § 31).

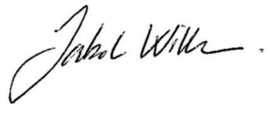
Både de nævnte statiske identifikationsoplysninger for bredbåndsabonnementer (IP-adresser, e-mail-adresser og evt. kredsløbsnumre) og for telefoniabonnementer/mobilabonnementer (telefonnummer og SIM-kort-nummer) er data, der indgår i de abonnementsoplysninger, som er fast registreret i

teleselskabernes kundedatabaser, og der er tale om registreringer som finder sted uanset logningsreglerne. Som beskrevet ovenfor er IMEI-nummer derimod data, som ikke er registreret i teleselskabernes kundedatabaser, ligesom IMEI-nummer udelukkende opbevares i 1 år som følge af logningsreglerne.

Endvidere fremgår det af lovforslagsbemærkningerne til TL § 13: ”Det skal bemærkes, at oplysninger, som udbyderne alene ligger inde med som følge af logningspligten, kun skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven”. IMEI-nummeret er som nævnt overfor netop eksempel på sådanne data, som registreres iht. logningsreglerne, og sammenhængen mellem telefonnummeret og de loggede data (både nummer->IMEI og IMEI->numre) kræver således kendelse efter reglerne i retsplejeloven.

På den baggrund er det samlet set Teleindustriens vurdering, at IMEI-oplysning ikke er omfattet af Telelovens § 13.

Med venlig hilsen



Jakob Willer, direktør, Teleindustrien

BILAG – Telelovens § 13

§ 13. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal på begæring af politiet udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

Lovforslagsbemærkningerne til Telelovens § 13 (tidligere § 15c) (TI's fremhævelser):

Den foreslåede bestemmelse vil give politiet adgang uden retskendelse til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, der ikke er indeholdt i 118-databasen, jf. § 34, stk. 2, 1. pkt., i lov om konkurrence- og forbrugerforhold på telemarkedet, og som udbyderen er i besiddelse af. Den udbyder, der har slutbrugerforholdet, vil således være forpligtet til at udlevere oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester til politiet, herunder oplysninger om slutbrugerens adgang til internettet (IP-adresser og e-mail-adresser), uden at betingelserne for edition skal være opfyldt.

Der er således **alene** tale om oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har **tildelt** slutbrugeren **som led i en konkret tjeneste**, og som således kan benyttes til at identificere den pågældende slutbruger.

Heraf følger, at der ikke er tale om oplysninger om betalingsmidler el. lign.

Det skal bemærkes, at der både er tale om navn til nummer og nummer til navn oplysninger. Det skal endvidere bemærkes, at bestemmelsen alene omfatter **statiske** oplysninger, idet registrering af dynamiske IP-adresser mv. vil ske i medfør af logningsforpligtelsen i retsplejeloven. Udlevering af dynamiske IP-adresser mv. skal ske i medfør af retsplejeloven.

Det skal yderligere bemærkes, at de oplistede eksempler er eksempler på de typer af oplysninger, der i dag kan identificere en slutbrugers adgang til kommunikationsnet og -tjenester for alle elektroniske kommunikationsformer, herunder en slutbrugers adgang til internettet. Der vil som følge af den almindelige teknologiske udvikling kunne opstå nye typer af oplysninger, der kan betegnes som oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, og som kan tjene til at identificere en bestemt slutbruger.

Formålet hermed er - i lyset af den teknologiske udvikling inden for tele- og internetkommunikation - at sikre, at politiet på den mest effektive måde kan få adgang til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester for alle elektroniske kommunikationsformer.

Udbyderne forpligtes ikke til at registrere og gemme oplysninger ud over hvad der allerede følger af § 34, stk. 2, om afgivelse af nummeroplysningsdata, men forpligtes **alene** til at udlevere oplysninger, som udbyderen i øvrigt måtte være **i umiddelbar besiddelse af** om en slutbrugers adgang til kommunikationsnet og -tjenester.

Det skal bemærkes, at oplysninger, som udbyderne alene ligger inde med som følge af logningspligten, kun skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven.

Det forudsættes, at udbyderen, der har slutbrugerforholdet, udleverer de pågældende oplysninger hurtigst muligt og uden ugrundet ophold. Det bemærkes, at en begæring om udlevering af oplysninger efter bestemmelsen i praksis vil være skriftlig.

Udbydernes omkostninger i forbindelse med udlevering af oplysninger vil blive afholdt af politiet i overensstemmelse med sædvanlig praksis.

Retsudvalget 2019-20
REU Alm.del - Bilag 533
Offentligt

Bilag D

Kammeradvokaten

JUSTITSMINISTERIET

Dato: 5. august 2020
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Larsen Vaabengaard
Sagsnr.: 2020-614-1420
Dok.: 1565749

Notat til Folketingets Europaudvalg og Folketingets Retsudvalg om afgivelse af indlæg i EU-Domstolens sag C-140/20, The Commissioner of the Garda Síochána m.fl.

1. Indledning

The Supreme Court (Højesteret) i Irland har i en sag vedrørende den irske kommunikationslov (datalagring) af 2011 forelagt EU-Domstolen seks præjudicielle spørgsmål om de EU-retlige rammer for nationale bestemmelser, som regulerer de irske myndigheders lagring af og adgang til metadata fra telekommunikation, herunder navnlig for det irske politi i forbindelse med afsløring, efterforskning og retsforfølgning af grov kriminalitet.

Fem af spørgsmålene (første, andet, tredje, fjerde og sjette spørgsmål) har dansk interesse, idet de endnu en gang angår fortolkningen af artikel 15 i direktiv 2002/58/EF[1] (e-data-beskyttelsesdirektivet) samt artikel 7, 8, 11 og 52 i Den Europæiske Unions Charter om grundlæggende rettigheder (Chartret). Der skal således tages stilling til, om de nævnte EU-bestemmelser er til hinder for en national lovgivning, der vedrører en generel ordning for lagring af data, hvilke hensyn og kriterier en national ret skal anvende og inddrage i forbindelse med vurderingen heraf, og om en national ret er forpligtet til at erklære en national foranstaltning uforenelig med artikel 15 i e-databeskyttelsesdirektivet. Endelig vedrører et spørgsmål brugen af potentiel ulovligt lagret data som bevismiddel i en straffesag.

[1] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

2. Sagens faktiske omstændigheder

Sagsøgeren, G.D., blev i en straffesag i 2015 idømt livsvarigt fængsel for drab. Sideløbende med straffesagen anlagde G.D. et civilt søgsmål med påstand om, at den nationale bestemmelse i loven af 2011, hvorefter telefonimetadata blev lagret og tilgået, blev erklæret ugyldig, idet bestemmelsen var uforenelig med artikel 15, stk. 1, i e-data-beskyttelsesdirektivet. Formålet med det civile søgsmål var at gøre det muligt i forbindelse med appelsagen om sagsøgerens straffedom at argumentere for, at telefondata ikke burde have været tilladt som bevis, og dermed fjerne en del af grundlaget for domfældelsen i første instans.

Retten i første instans (High Court) gav sagsøgeren medhold i, at section 6(1)(a) i loven af 2011, som indeholder betingelserne for udlevering af telefondata, ikke er i overensstemmelse med artikel 15, stk. 1, i e-data-beskyttelsesdirektivet sammenholdt med artikel 7, 8 og 52, stk. 1, i Chartret. Dommen blev appelleret til den irske højesteret, som har indgivet anmodningen om præjudiciel afgørelse.

Af anmodningen fremgår blandt andet, at formålet er at få præciseret de EU-retlige krav vedrørende lagring af data med henblik på bekæmpelse af grov kriminalitet og de nødvendige sikkerhedsforanstaltninger ved adgang til disse data, henset til en medlemsstats kompetence på det strafferetlige område. I den forbindelse anføres det, at det ikke er muligt at få adgang til data, der ikke er blevet lagret, og at hvis universel lagring af metadata fra telekommunikation ikke var tilladt, uanset hvor robust ordningen for adgang hertil er, ville mange alvorlige forbrydelser ikke blive opklaret eller føre til retsforfølgning.

Sagsøger har bl.a. henvist til dommen i Tele2-sagen (sag C-203/15 og C-698/15). I dommen fastslog EU-Domstolen, at de svenske regler om logning var i strid med direktiv 2002/58, sammenholdt med de grundlæggende rettigheder i EU-Chartret. EU-retten var således til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en pligt til generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

3. Den danske interesse i sagen

Det er regeringens opfattelse, at regeringen bør afgive indlæg i denne sag, idet sagen vedrører EU-medlemsstaternes muligheder for at gemme og opbevare oplysninger om tele- og internettrafik (logning) samt de nødvendige

sikkerhedsforanstaltninger ved adgang hertil til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

De danske regler om logning skal som konsekvens af EU-Domstolens afgørelse i Tele2-sagen revideres. Endvidere kan besvarelsen af de forelagte spørgsmål få betydning for de danske regler i retsplejeloven om adgang til data lagret af telekommunikationsselskaber i forbindelse med efterforskning og retsforfølgning af strafbare forhold.

EU-Domstolens besvarelse af det forelagte spørgsmål vil således kunne få indflydelse på, hvordan de danske logningsregler kan indrettes i overensstemmelse med EU-retten på en måde, hvor logning fortsat kan udgøre et centralt og effektivt efterforskningsredskab.

Tele2-dommen efterlader imidlertid væsentlig fortolkningstvivl i forhold til, hvordan nationale bestemmelser om logning kan indrettes i overensstemmelse med EU-retten. Der har således siden foråret 2017 løbende været drøftelser i EU-regi om, hvordan medlemsstaterne kan indrette nationale logningsregler i lyset af dommen. Kommissionen tilkendegav, som følge af Tele2-dommen, at Kommissionen ville udarbejde retningslinjer til medlemsstaterne om indretning af logningsregler. Disse retningslinjer er endnu ikke udarbejdet.

Der verserer for tiden en række præjudicielle sager fra andre EU-medlemsstater for EU-Domstolen, som kan få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler.

Danmark og 16 andre EU/EØS-medlemsstater har afgivet indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18 om de franske logningsregler samt i sag C-520/18 om de belgiske logningsregler. I begge sager gjorde regeringen gældende, at Domstolen bør genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen.

Det forventes, at EU-Domstolen vil afsige domme i sagerne i løbet af 2020/2021.

Derudover afgav regeringen den 15. oktober 2019 mundtligt indlæg i en præjudiciel sag vedrørende de estiske logningsregler (sag C-746/18, H.K.). På samme måde som i den franske og den belgiske sag blev der også i denne sag fra visse medlemsstater argumenteret for, at EU-Domstolen bør genoverveje retstilstanden, som Tele2-dommen har medført. Dommen i

denne sag vil navnlig kunne få betydning for, hvordan retsplejelovens regler om adgang til oplysninger, som teleselskaberne skal opbevare til brug for efterforskning og retsforfølgning af strafbare forhold i medfør af logningsbekendtgørelsen, kan udformes.

Endelig afgav regeringen den 17. februar 2020 skriftlig indlæg i en præjudiciel sag vedrørende de tyske logningsregler (de forenede sager nr. C-793/19 og C-794/19, SpaceNet AG m.fl.). Også her blev der argumenteret for, at EU-Domstolen bør genoverveje retstilstanden, som Tele2-dommen har medført. EU-Domstolen har den 15. juli 2020 meddelt, at sagen er udsat indtil domsafsigelse i de forenede sager C-511/18, C-512/18 og C-520/18 (om de franske og belgiske logningsregler).

Regeringens synspunkter i sagen

Det er overordnet regeringens opfattelse, at EU-Domstolen skal opfordres til at genoverveje visse af de udtalelser, som Domstolen afgav i Tele2-dommen. Der skal i den forbindelse henvises til, at loggede oplysninger udgør et centralt og effektivt redskab for politiet og politiets efterretningstjeneste, som i forhold til efterforskning og strafforfølgning af alvorlig kriminalitet og terror er af afgørende betydning, således som også påpeget af den irske højesteret i forelæggelseskendelsen.

Der skal efter regeringens opfattelse ligeledes argumenteres for, at EU-retten ikke er til hinder for en generel og udifferentieret logningsforpligtelse, hvis formål bl.a. er at sikre den personlige og nationale sikkerhed, som staten har en positiv forpligtelse til at sikre for alle borgere.

Det er i den sammenhæng afgørende, at der sikres en balance mellem på den ene side retshåndhævende myndigheders mulighed for at anvende centralt og effektivt redskaber til brug for efterforskning og strafforfølgning og på den anden side overholdelse af de grundlæggende rettigheder i Chartret. I den forbindelse skal EU-Domstolen efter regeringens opfattelse opfordres til at inddrage praksis fra Den Europæiske Menneskerettighedsdomstol, herunder senest dom af 30. januar 2020 i Breyer v. Germany, præmis 78-80. Efter regeringens opfattelse skal der ligeledes argumenteres for, at det må være den samlede mængde af retsgarantier, der skal indgå i vurderingen af, om det indgreb i Chartrets artikel 7 og 8, som lagring af trafik- og lokaliseringsdata udgør, er proportionalt, herunder om der foreligger en efterfølgende eller uafhængig domstolsprøvelse for så vidt angår adgangen til de lagrede trafik- og lokaliseringsdata.

Endelig skal der efter regeringens opfattelse overordnet argumenteres for, at såfremt data er lagret i henhold til en national bestemmelse, som efter EU-retten er ulovlig, er anvendelsen af sådanne data som bevismidler i en straffesag ikke generelt i strid med retten til en retfærdig rettergang som beskyttet af Chartrets artikel 47. I den forbindelse skal EU-Domstolen efter regeringens opfattelse opfordres til at inddrage praksis fra Den Europæiske Menneskerettighedsdomstol, hvorefter der i forhold til anvendelsen af ulovligt tilvejebragte bevismidler i en straffeproces må foretages en helhedsbedømmelse af, om processen har været retfærdig, herunder om beviset er det eneste eller afgørende bevis, jf. f.eks. Den Europæiske Menneskerettighedsdomstols dom af 11. juli 2006 i Jalloh mod Tyskland.

Bilag 13

JUSTITSMINISTERIET

Dato: 19. november 2020
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-614-1582
Dok.: 1682329

Notat til Folketingets Retsudvalg og Europaudvalg om dom af 6. oktober 2020 i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.

1. Justitsministeriet oplyste ved notater oversendt til Folketingets Retsudvalg og Europaudvalg den 30. november 2018 og den 3. december 2018, at regeringen agtede at afgive indlæg i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt i sag C-520/18, Ordre des barreaux francophones et germanophone m.fl. Sagerne angår det EU-retlige grundlag for at kunne pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet. Notaterne vedlægges.

2. Den mundtlige forhandling i sagerne blev afholdt den 9. og 10. september 2019, hvor i alt 16 regeringer, heriblandt den danske, og Europa-Kommissionen afgav indlæg.

Den danske regering gjorde de synspunkter gældende, som fremgår af vedlagte notater. I den forbindelse argumenterede Danmark og de 15 øvrige EU-lande samt Kommissionen for, at EU-Domstolen burde genoverveje sine konklusioner i EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2-Sverige og Watson (*Tele2-dommen*). Fra dansk side blev det bl.a. gjort gældende, at EU-retten ikke er til hinder for en generel og udifferentieret logningsforpligtelse med henblik på kriminalitetsbekæmpelse.

EU-Domstolen afsagde dom i sagerne den 6. oktober 2020.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

3. I dommen af 6. oktober 2020 gentager EU-Domstolen udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for national lovgivning, der pålægger teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata med henblik på, at offentlige myndigheder kan få adgang til disse data (logning). EU-Domstolen anfører dog samtidig under hvilke betingelser, udgangspunktet kan fraviges, således at medlemsstaterne kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata.

EU-Domstolen fastslår indledningsvist, at national lovgivning der påbyder teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet falder ind under anvendelsesområdet for direktiv 2002/58/EF[1] (herefter e-data-beskyttelsesdirektivet). Nationale lognings-regler skal således være i overensstemmelse med artikel 15, stk. 1, i e-data-beskyttelsesdirektivet sammenholdt med artikel 7 om respekt for privatlivet, artikel 8 om beskyttelse af personoplysninger og artikel 11 om ytringsfrihed i EU's Charter om Grundlæggende Rettigheder (herefter Chartret). Det er dog muligt efter Chartret at foretage begrænsninger i disse rettigheder, hvis begrænsningerne i overensstemmelse med Chartrets artikel 52, stk. 1, varetager objektive og generelle hensyn anerkendt af Unionen og ikke udgør et uforholdsmæssigt og urimeligt indgreb, som berører disse rettigheders egentlige indhold.

Alvorlig trussel mod den nationale sikkerhed
Herefter fastlår EU-Domstolen for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed (præmis 134ff).[2]

I den forbindelse bemærker EU-Domstolen, at artikel 4, stk. 2, i EU-Traktaten fastslår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, samt at beskyttelsen af national sikkerhed er et mere væsentligt formål end f.eks. hensynet til bekæmpelse af kriminalitet, hvorfor hensynet kan retfærdiggøre mere alvorlige indgreb i grundlæggende rettigheder.

[1] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor

[2] Ved national sikkerhed ("national security") forstås beskyttelse af en stats væsentligste funktioner og samfundets grundlæggende interesser. Begrebet omfatter derfor aktiviteter, der er egnet til alvorligt at destabilisere en stats forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte trusler mod samfundet og statens befolkning, som f.eks. terroraktiviteter. Derimod omfatter begrebet offentlig sikkerhed ("public security") også anden form for alvorlig kriminalitet, som f.eks. narko-, bande- og våbenkriminalitet.

Som følge heraf er EU-retten ikke til hinder for, at medlemsstaterne kan pålægge teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata for en begrænset tidsperiode, så længe der er tilstrækkelige solide grunde til at antage, at der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig. Lagringen må dog kun ske i en afgrænset periode, der skal begrænses til det strengt nødvendige. Perioden kan forlænges, hvis den alvorlige trussel fortsætter, men EU-Domstolen understreger i den forbindelse, at lagring af data ikke må blive hovedreglen ("systematic in nature"). Endelig skal den generelle og udifferentierede lagring ledsages af mulighed for en efterfølgende effektiv prøvelse af bl.a., om der foreligger en sådan alvorlig trussel mod den nationale sikkerhed.

Bekæmpelse af alvorlig kriminalitet eller beskyttelse mod alvorlige trusler mod den offentlige sikkerhed

Dernæst fastslår EU-Domstolen, at *alvorlig* kriminalitet og beskyttelse mod *alvorlige* trusler mod den offentlige sikkerhed ikke kan retfærdiggøre en generel og udifferentieret lagring af trafik- og lokaliseringsdata (præmis 140ff).

Men EU-Domstolen udelukker i den forbindelse ikke, at der med henblik på bl.a. at bekæmpe alvorlig kriminalitet kan pålægges en *målrettet* lagringsforpligtelse af trafik- og lokaliseringsdata ("targeted retention"). EU-Domstolen gentager her, hvad den tidligere sagde i bl.a. Tele2-dommen, hvorefter medlemsstaterne kan pålægge teleudbydere mv. en pligt til at lagre trafik- og lokaliseringsdata for 1) en bestemt periode, fra et geografisk område, og/eller fra en gruppe af personer, der på en eller anden måde kan knyttes til alvorlig kriminalitet, eller 2) fra andre personer, hvis data kan medvirke til at bekæmpe alvorlig kriminalitet.

For så vidt angår målrettet lagring af disse data ud fra et geografisk kriterium bemærker EU-Domstolen, at det kan være områder med høj hyppighed af alvorlig kriminalitet, steder, som er særligt sårbare over for alvorlig kriminalitet, som f.eks. infrastruktur, som jævnligt har mange besøgende, eller strategiske områder, såsom lufthavne, stationer og betalingsanlæg.

Den målrettede lagring af disse data må kun lagres, så længe det er strengt nødvendigt i lyset af formålet og de omstændigheder, der retfærdiggør laggringen. Det vil dog være muligt at forlænge foranstaltningerne, hvis fortsat lagring er nødvendig.

Lagring af IP-adresser og oplysninger om civil identitet
EU-Domstolen anfører videre – som noget nyt – at medlemsstaterne kan fastsætte national lovgivning, der muliggør generel og udifferentieret lagring af *alle brugeres IP-adresser*, der er tildelt kilden til en kommunikation (præmis 152ff). Dette må dog alene ske med henblik på at bekæmpe alvorlig kriminalitet eller forhindre alvorlige trusler mod den nationale sikkerhed eller offentlige sikkerhed. Lagring af IP-adresserne må alene ske i en periode, der er begrænset til det strengt nødvendige, og myndighedernes adgang til IP-adresserne skal være nøje reguleret i lovgivningen.

For så vidt angår oplysninger om civil identitet ("*civil identity*") fastslår EU-Domstolen, at medlemsstaterne kan pålægge teleudbydere mv. at lagre data vedrørende civil identitet med henblik på at forhindre eller efterforske alle strafbare handlinger og beskytte mod trusler mod den offentlige sikkerhed. I den forbindelse bemærker EU-Domstolen, at der ikke er noget krav om, at kriminaliteten eller truslen er alvorlig. Krav om lagring af data om den civile identitet er ikke underlagt nogen tidsbegrænsning.

Pålæg om fremskyndet lagring for at bekæmpe alvorlig kriminalitet eller handlinger, der kan skade den nationale sikkerhed
EU-Domstolen fastslår endelig, at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. en fremskyndet lagring af trafik- og lokaliseringsdata, som allerede er i udbydernes besiddelse (præmis 160ff).

Der kan således i visse situationer i et udvidet omfang ske målrettet lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds. En sådan målrettet lagring kan udelukkende ske for at efterforske eller beskytte mod alvorlig kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. En sådan lagring skal begrænses tidsmæssigt til det strengt nødvendige, og pålægget herom skal kunne underlægges en effektiv prøvelse.

4. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af alvorlig kriminalitet og terror.

Justitsministeriet studerer nu dommen med henblik på at vurdere, i hvilket omfang Danmark vil kunne opretholde de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Det sker med henblik på at kunne præsentere et udkast til revision af de danske regler på området.

Det er vigtigt for mig som justitsminister, at politiet og PET har de nødvendige værktøjer for at kunne efterforske og retsforfølge alvorlig kriminalitet og beskytte vores nationale sikkerhed. Her er loggede oplysninger af afgørende betydning.

Europaudvalget 2020-21
EUU Alm.del - Bilag 114
Offentligt

Bilag O

Kammeradvokaten

JUSTITSMINISTERIET

Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 20. november 2020
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-0030-5020
Dok.: 1680533

Hermed sendes besvarelse af spørgsmål nr. 140 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. oktober 2020. Spørgsmålet er stillet efter ønske fra Rosa Lund (EL).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 140 (Alm. del) fra Folketingets Retsudvalg:

> ”Er det ministerens opfattelse, at teleselskaber i Danmark er juridisk forpligtede til at logge teledata?”

Svar:

Det følger af retsplejelovens § 786, stk. 4, 1. pkt., at det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Der er i bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), fastsat regler om, hvilke nærmere oplysninger teleudbyderne skal registrere og opbevare.

EU-domstolen afsagde den 6. oktober 2020 dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen vedrører det EU-retlige grundlag for at kunne pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet.

Justitsministeriet er i øjeblikket i gang med at studere dommen og vurdere dens nærmere konsekvenser for de danske logningsregler.

Det bemærkes, at EU-Domstolens dom ikke betyder, at de gældende danske logningsregler sættes ud af kraft. Derfor skal teleudbydere fortsat logge og udlevere oplysninger i overensstemmelse med gældende regler, indtil ny lovgivning måtte være vedtaget og trådt i kraft.

Bilag P

Kammeradvokaten

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-0030-5121
Dok.: 1722414

Hermed sendes besvarelse af spørgsmål nr. 219 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 219 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren oversende ministerens korrespondance med Teleindustrien om konsekvenserne for de danske logningsregler som følge af EU-Domstolens dom af 6. oktober 2020?"

Svar:

Der vedlægges brev af 9. oktober 2020 fra Teleindustrien til Justitsministeriet samt Justitsministeriets svar af 30. oktober 2020 til Teleindustrien.

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Til justitsminister Nick Hækkerup

Sendt pr. mail: jm@jm.dk

9. oktober 2020

Kære Nick Hækkerup

EU-domstolen har i tirsdags den 6. oktober 2020 truffet afgørelse om, at det er i strid med EU-retten, hvis medlemslandene fastlægger nationale regler, som pålægger teleselskaberne en pligt til generel og udifferentieret masseindsamling af teledata, herunder trafik- og lokaliseringsdata. Dermed er der truffet endnu en afgørelse i rækken af EU-domme, der betyder, at de danske logningsregler skal ændres.

Vi har i telebranchen et stort behov for at få afklaret, hvilke konsekvenser dommen har for de danske logningsregler og for teleselskabernes dataindsamling. Det er branchens klare opfattelse, at de danske regler ikke kan opretholdes og skal ændres hurtigst muligt i lyset af dommen – og tidligere domme. Dén indsamling og lagring af data om de danske telekunder, som teleselskaberne efter de gældende regler er forpligtet til, kan ikke fortsætte uændret.

Teleindustrien vil naturligvis altid gerne inden for lovens og EU-reglernes rammer bistå politiet, og der har igennem mange årtier eksisteret et godt samarbejde mellem teleselskaberne og politiet, hvor teleselskaberne har givet politiet adgang til data, som teleselskaberne har besiddet, hvis betingelserne for indgreb og udlevering har været opfyldt.

Vi vil fra branchens side naturligvis gerne bidrage konstruktivt med teknisk viden og indspil til, hvordan reglerne kan og bør ændres i lyset af EU-domstolens afgørelse. Som et første skridt - og for at sikre efterlevelse af EU-retten – opfordrer vi til straks at suspendere brugen af editionskendelser vedr. adgang til logningsdata til andet end sager om alvorlig kriminalitet eller alvorlige trusler mod den nationale sikkerhed.

Jeg skal på den baggrund, på vegne af teleselskaberne, opfordre ministeren til i lyset af den afsagte dom meget hurtigt at vurdere, hvilke ændringer dommen giver anledning til i Danmark.

Med venlig hilsen

Jakob Willer
Direktør

Teleindustrien – Axeltorv 6, 3. sal - DK-1609 København V – www.teleindu.dk

JUSTITSMINISTERIET
Justitsministeren

Axeltorv 6, 3.
1609 København V

Dato: 30. oktober 2020
Dok.: 1663435

Kære Jakob Willer

Tak for dit brev af 9. oktober 2020 om de danske logningsregler.

Som du skriver i dit brev, afsagde EU-domstolen den 6. oktober 2020 dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen vedrører det EU-retlige grundlag for at kunne pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata til brug for bl.a. bekæmpelse af kriminalitet.

Justitsministeriet er nu ved at nærstudere dommen og vurdere dens konsekvenser for de danske logningsregler og den kommende revision. Det har naturligvis høj prioritet.

EU-Domstolens dom betyder ikke, at de gældende danske logningsregler sættes ud af kraft. Derfor skal telebranchen fortsat logge og udlevere oplysninger i overensstemmelse med gældende regler, indtil ny lovgivning måtte være vedtaget og trådt i kraft.

Som det fremgår af regeringens lovprogram, der blev offentliggjort den 6. oktober 2020, agter regeringen at fremsætte et lovforslag om revision af reglerne om registrering og opbevaring af oplysninger om tele- og internettrafik (logning) i dette folketingsår – nærmere bestemt til februar 2021.

Justitsministeriet vil snarest invitere til en nærmere drøftelse om det kommende arbejde.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Jeg ser frem til et godt og konstruktivt samarbejde om den kommende revision af de danske logningsregler.

Med venlig hilsen

Nick Hækkerup

Bilag Q

Kammeradvokaten

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: EU-retskontoret
Sagsbeh: Helene Fussing Clausen
Sagsnr.: 2020-0030-5121
Dok.: 1722414

Hermed sendes besvarelse af spørgsmål nr. 220 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Anders Lotterup

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 220 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren redegøre for, hvilke konsekvenser der er for de EU-lande, der efter EU-Domstolens dom af 6. oktober 2020 om datalogning opretholder logningsregler, der er i strid med EU-dommen, herunder hvilke sanktionsmuligheder der er over for de pågældende lande?"

Svar:

Den 6. oktober 2020 afsagde EU-Domstolen dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt C-520/18, Ordre des barreaux francophones et germanophone m.fl. I dommen fastslås det, at henholdsvis franske og belgiske regler, der pålagde teleudbydere mv. en generel og udifferentieret lagring af trafik- og lokaliseringsdata (såkaldte logningsregler) med henblik på, at politi og anklagemyndighed kunne få adgang hertil for at efterforske og retsforfølge personer i straffesager, var i strid med EU-retten. EU-Domstolen anførte dog samtidigt under hvilke betingelser, dette udgangspunkt kan fraviges, således at medlemsstaterne i visse tilfælde kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at imødegå en alvorlig trussel mod den nationale sikkerhed eller bekæmpe grov kriminalitet.

Medlemsstaterne er EU-retligt forpligtet til at sikre, at deres nationale logningsregler er indrettet i overensstemmelse med EU-Domstolens dom af 6. oktober 2020. Dette gælder også de EU-medlemsstaters logningsregler, som EU-Domstolen ikke var blevet anmodet om at tage stilling til i de nævnte forenede sager. Der er ikke en bestemt EU-retlig frist for, hvor hurtigt en medlemsstat skal ændre sine regler for at bringe disse i overensstemmelse med en dom fra EU-Domstolen i en sag, der vedrører en anden medlemsstats lovgivning.

Det følger imidlertid af EU-Domstolens praksis, at en ændring af nationale regler for at bringe disse i overensstemmelse med EU-retten, som fortolket af EU-Domstolen, skal ske *så hurtigt som muligt,* jf. EU-Domstolens dom af 21. juni 2007 i de forenede sager C-231/06 - C-233/06, Jonkman. Der kan også henvises til Højesterets dom af 19. januar 2017 i sag 42/2016 (UfR 2017.1243 H). Det vil i lyset heraf afhænge af den enkelte sags omstændigheder, hvor hurtigt en tilpasning skal foretages. Der vil i den forbindelse bl.a. kunne tages hensyn til, hvor teknisk vanskelige ændringer, der er tale om, og hvor store økonomiske konsekvenser, ændringerne vil kunne medføre for de virksomheder, der skal indrette sig efter de tilrettede regler.

Hvis Kommissionen finder, at en medlemsstat ikke har truffet de foranstaltninger, der er nødvendige for opfyldelse af en dom afsagt af EU-Domstolen, kan den – efter proceduren for traktatkrænkelsessager i artikel 258 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) – i sidste instans indbringe sagen for Domstolen efter at have givet medlemsstaten lejlighed til at fremsætte sine bemærkninger.

Hvis Domstolen fastslår, at en medlemsstat har overtrådt sine EU-retlige forpligtelser, og Kommissionen herefter finder, at den pågældende medlemsstat ikke har truffet de foranstaltninger, der er nødvendige for opfyldelsen af dommen, kan Kommissionen indbringe sagen for Domstolen på ny med henblik på, at Domstolen pålægger medlemsstaten et fast beløb eller en tvangsbøde. Dette vil i givet fald ske efter den procedure, der nærmere er reguleret i TEUF artikel 260.

Bilag R

Kammeradvokaten

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: EU-retskontoret
Sagsbeh: Helene Fussing Clausen
Sagsnr.: 2020-0030-5121
Dok.: 1722414

Hermed sendes besvarelse af spørgsmål nr. 221 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Anders Lotterup

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 221 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren redegøre for om Danmark som konsekvens af EU-Domstolens dom af 6. oktober 2020 kan blive pålagt at tilpasse de danske logningsregler, så de er i overensstemmelse med EU-retten?”

Svar:

Der henvises til den samtidige besvarelse af spørgsmål nr. 220 (Alm. del) fra Folketingets Retsudvalg.

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: EU-retskontoret
Sagsbeh: Helene Fussing Clausen
Sagsnr.: 2020-0030-5121
Dok.: 1722414

Hermed sendes besvarelse af spørgsmål nr. 220 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Anders Lotterup

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 220 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren redegøre for, hvilke konsekvenser der er for de EU-lande, der efter EU-Domstolens dom af 6. oktober 2020 om datalogning opretholder logningsregler, der er i strid med EU-dommen, herunder hvilke sanktionsmuligheder der er over for de pågældende lande?"

Svar:

Den 6. oktober 2020 afsagde EU-Domstolen dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl., samt C-520/18, Ordre des barreaux francophones et germanophone m.fl. I dommen fastslås det, at henholdsvis franske og belgiske regler, der pålagde teleudbydere mv. en generel og udifferentieret lagring af trafik- og lokaliseringsdata (såkaldte logningsregler) med henblik på, at politi og anklagemyndighed kunne få adgang hertil for at efterforske og retsforfølge personer i straffesager, var i strid med EU-retten. EU-Domstolen anførte dog samtidigt under hvilke betingelser, dette udgangspunkt kan fraviges, således at medlemsstaterne i visse tilfælde kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at imødegå en alvorlig trussel mod den nationale sikkerhed eller bekæmpe grov kriminalitet.

Medlemsstaterne er EU-retligt forpligtet til at sikre, at deres nationale logningsregler er indrettet i overensstemmelse med EU-Domstolens dom af 6. oktober 2020. Dette gælder også de EU-medlemsstaters logningsregler, som EU-Domstolen ikke var blevet anmodet om at tage stilling til i de nævnte forenede sager. Der er ikke en bestemt EU-retlig frist for, hvor hurtigt en medlemsstat skal ændre sine regler for at bringe disse i overensstemmelse med en dom fra EU-Domstolen i en sag, der vedrører en anden medlemsstats lovgivning.

Det følger imidlertid af EU-Domstolens praksis, at en ændring af nationale regler for at bringe disse i overensstemmelse med EU-retten, som fortolket af EU-Domstolen, skal ske *så hurtigt som muligt,* jf. EU-Domstolens dom af 21. juni 2007 i de forenede sager C-231/06 - C-233/06, Jonkman. Der kan også henvises til Højesterets dom af 19. januar 2017 i sag 42/2016 (UfR 2017.1243 H). Det vil i lyset heraf afhænge af den enkelte sags omstændigheder, hvor hurtigt en tilpasning skal foretages. Der vil i den forbindelse bl.a. kunne tages hensyn til, hvor teknisk vanskelige ændringer, der er tale om, og hvor store økonomiske konsekvenser, ændringerne vil kunne medføre for de virksomheder, der skal indrette sig efter de tilrettede regler.

Hvis Kommissionen finder, at en medlemsstat ikke har truffet de foranstaltninger, der er nødvendige for opfyldelse af en dom afsagt af EU-Domstolen, kan den – efter proceduren for traktatkrænkelsessager i artikel 258 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) – i sidste instans indbringe sagen for Domstolen efter at have givet medlemsstaten lejlighed til at fremsætte sine bemærkninger.

Hvis Domstolen fastslår, at en medlemsstat har overtrådt sine EU-retlige forpligtelser, og Kommissionen herefter finder, at den pågældende medlemsstat ikke har truffet de foranstaltninger, der er nødvendige for opfyldelsen af dommen, kan Kommissionen indbringe sagen for Domstolen på ny med henblik på, at Domstolen pålægger medlemsstaten et fast beløb eller en tvangsbøde. Dette vil i givet fald ske efter den procedure, der nærmere er reguleret i TEUF artikel 260.

Bilag S

Kammeradvokaten

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-0030-5121
Dok.: 1722414

Hermed sendes besvarelse af spørgsmål nr. 222 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 222 (Alm. del) fra Folketingets Retsudvalg:

> ”Har ministeren kendskab til, at teleselskaber i andre lande end Sverige har valgt at trodse nationale logningsregler, der strider mod EU-retten, og i stedet følge EU-Domstolens afgørelser?”

Svar:

Justitsministeriet har ikke kendskab til, at teleselskaber i andre lande end Sverige har valgt ikke at efterleve gældende nationale logningsregler.

Bilag T

Kammeradvokaten

JUSTITSMINISTERIET

Christiansborg
1240 København K
DK Danmark

Dato: 5. januar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-0030-5126
Dok.: 1722563

Hermed sendes besvarelse af spørgsmål nr. 223 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 17. november 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 223 (Alm. del) fra Folketingets Retsudvalg:

> "Kan ministeren oplyse om og i givet fald hvilke lande, der som konsekvens af EU-Domstolens afgørelser, har tilpasset deres nationale logningsregler, så de er i overensstemmelse med EU-retten?"

Svar:

Sverige vedtog på baggrund af Tele2-dommen (EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl.) en ændring af de svenske logningsregler, som trådte i kraft den 1. oktober 2019. De svenske logningsregler indebærer bl.a. en begrænset og differentieret forpligtelse til logning af oplysninger afhængig af typen af data.

Justitsministeriet kan herudover henvise til de tidligere svar af lignende spørgsmål i besvarelserne af 19. juni 2018 på spørgsmål nr. 623 og 625 (Alm. del) fra Folketingets Retsudvalg, som uddyber, hvordan en række af de øvrige EU-lande havde indrettet sig efter Tele2-dommen.

Justitsministeriet vil til brug for revisionen af de danske logningsregler indhente oplysninger om relevante landes opfølgning på EU-Domstolens dom af 6. oktober 2020 om de franske og belgiske logningsregler (de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.), herunder oplysninger om, i hvilket omfang dommen forventes at føre til ændringer af de pågældende landes logningsregler. Justitsministeriet er påbegyndt en indledende dialog med relevante lande herom.

En række medlemsstater har oplyst, at de er ved at studere dommen af 6. oktober 2020 med henblik på at vurdere, i hvilket omfang nationale regler skal tilpasses.

Eur
EU
Offe

JUSTITSMINISTERIET

Folketinget
Retsudvalget

Christiansborg
1240 København K
DK Danmark

Dato: 19. juni 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Michael Hadberg
Sagsnr.: 2018-0030-0995
Dok.: 727347

Hermed sendes endelig besvarelse af spørgsmål nr. 623 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 9. april 2018. Spørgsmålet er stillet efter ønske fra Rosa Lund (EL), Lisbeth Bech Poulsen (SF) og Josephine Fock (ALT).

Søren Pape Poulsen

/

Casper Grue Jensen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 33933510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 623 (Alm. del) fra Folketingets Retsudvalg:

> "Kan ministeren i forlængelse af Retsudvalgets samråd om logning den 5. april 2018 redegøre for, hvordan og i hvilket omfang der logges data i Tyskland, Østrig og Nederlandene i forhold til hvordan data logges i Danmark?"

Svar:

1. Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet bidrag fra de danske ambassader i henholdsvis Berlin, Wien og Haag.

2. Den danske ambassade i Berlin har på baggrund af oplysninger fra det tyske justitsministerium bl.a. oplyst, at den ansvarlige tyske styrelse, Bundesnetzagentur, i en pressemeddelelse den 28. juni 2017 meddelte, at man ville suspendere håndhævelsen af og øvrige tiltag for så vidt angår datalogning, herunder ville man ikke udstede bøder for manglende efterlevelse, indtil der forelå en retsgyldig afgørelse. Pressemeddelelsen kom i forlængelse af en foreløbig dom fra Forvaltningsdomstolen i Münster (Oberverwaltungsgericht) den 22. juni 2017. Heri fastslog domstolen, at det nuværende tyske retsgrundlag var uforeneligt med databeskyttelsesdirektivet, EU/2002/58, art. 15, afsnit 1, jf. domsafsigelse ved EU-domstolen den 21. december 2016 i sagerne C-203/15 og C-698/15.

Datalogningsloven er ligeledes indbragt for den tyske Forfatningsdomstol. I det tyske justitsministerium regner man ikke med en domsafsigelse i indeværende år. Indtil da forbliver datalogning i Tyskland suspenderet.

Retsgrundlaget for datalogning blev indført i december 2015 og var planlagt til at skulle træde i kraft fuldt ud den 1. juli 2017. Lagringsfristerne er/var 10 uger for teletrafikdata og 4 uger for lokaliseringsdata.

3. Den danske ambassade i Wien har indhentet en udtalelse fra det østrigske indenrigsministerium. Det fremgår imidlertid ikke af udtalelsen, hvorvidt den østrigske lovgivning forpligter teleselskaberne til at logge teleoplysninger.

I forbindelse med Justitsministeriets indhentelse af oplysninger fra de øvrige EU-medlemsstater til brug for den samtidige besvarelse af spørgsmål nr. 625 (Alm. del) fra Folketingets Retsudvalg har de østrigske myndigheder den 26. april 2018 oplyst, at de østrigske domstole anså de dagældende

nationale regler om logning for uforenelige med den tidligere afgørelse fra EU-Domstolen fra marts 2014 i den såkaldte Digital Rights-sag, og at reglerne derfor på daværende tidspunkt blev sat ud af kraft.

Justitsministeriet skal i forlængelse heraf bemærke, at de østrigske myndigheder i forbindelse med en høring foretaget af den franske EU-repræsentation i maj 2018 har oplyst, at det østrigske parlament har vedtaget en ny lov, som indebærer målrettet logning på baggrund af en indledende mistanke (såkaldt "quick freeze"). Loven er efter det oplyste trådt i kraft den 1. juni 2018.

4. Den danske ambassade i Haag har på baggrund af oplysninger fra det nederlandske justits- og sikkerhedsministerium oplyst, at der på nuværende tidspunkt ingen specifikke lovkrav er om datalogning i Nederlandene. Den tidligere lovgivning herom finder ikke længere anvendelse, eftersom den blev indstillet som følge af national domsafsigelse efter Den Europæiske Domstols afgørelse i Digital Rights-sagen i 2014.

Justits- og Sikkerhedsministeriet forbereder på nuværende tidspunkt et ændringsforslag til lovgivningen på datalogningsområdet. Loven skal fastlægge et krav om opbevaring af brugerdata med henblik på identifikation af hvem der brugte (eller var i besiddelse af) et specifikt telefonnummer, IP-adresser mv.

5. Justitsministeriet kan vedrørende de danske logningsregler oplyse, at udbydere af telenet eller teletjenester skal foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. retsplejelovens 786, stk. 4.

Der er i bekendtgørelse nr. 988 af 28. september 2006 (logningsbekendtgørelsen) fastsat regler om, hvilke nærmere oplysninger teleselskaberne skal registrere og opbevare. Efter denne bekendtgørelse skal teleselskaber bl.a. registrere og opbevare oplysninger om, hvilke andre telefoner en telefon har været i kontakt med, og oplysninger om hvornår samt hvilken mast telefonen var forbundet til ved kommunikationens start og afslutning.

Eur
EU
Offe

JUSTITSMINISTERIET

Folketinget
Retsudvalget

Christiansborg
1240 København K
DK Danmark

Dato: 19. juni 2018
Kontor: Sikkerhedskontoret
Sagsbeh: Michael Hadberg
Sagsnr.: 2018-0030-0997
Dok.: 727365

Hermed sendes endelig besvarelse af spørgsmål nr. 625 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 9. april 2018. Spørgsmålet er stillet efter ønske fra Rosa Lund (EL), Lisbeth Bech Poulsen (SF) og Josephine Fock (ALT).

Søren Pape Poulsen

/

Casper Grue Jensen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 33933510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 625 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren i forlængelse af Retsudvalgets samråd om logning den 5. april 2018 sende et notat om, hvordan de øvrige EU-lande har indrettet sig efter Tele2-dommen, f.eks. om logningen er ophørt, uanset om der endnu ikke er fulgt op med ny lovgivning i de pågældende lande?"

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet oplysninger fra de øvrige medlemsstater via den danske EU-repræsentation i Bruxelles.

Justitsministeriet har modtaget oplysninger fra 18 af de øvrige EU-medlemsstater.

På baggrund heraf kan Justitsministeriet oplyse, at der i 12 EU-medlemsstater gælder en uændret logningsforpligtelse efter afsigelsen af Tele2-dommen. Det drejer sig om Belgien, Kroatien, Tjekkiet, Finland, Grækenland, Ungarn, Litauen, Luxembourg, Polen, Rumænien, Spanien og Storbritannien.

I Østrig, Nederlandene og Slovenien er tidligere gældende nationale regler om logning blevet sat ud af kraft som følge af nationale domstolsafgørelser før afsigelsen af Tele2-dommen. Østrig og Nederlandene har i den forbindelse oplyst, at de nationale domstole anså de dagældende regler for uforenelige med den tidligere afgørelse fra EU-Domstolen fra marts 2014 i den såkaldte Digital Rights-sag. Af disse tre lande har kun Østrig indført nye regler om logning. Der henvises for så vidt angår Østrig og Nederlandene i øvrigt til den samtidige besvarelse af spørgsmål nr. 623 (Alm. del) fra Folketingets Retsudvalg.

I Tyskland, Slovakiet og Sverige er logningsforpligtelsen helt eller delvist ophørt eller håndhævelsen af reglerne suspenderet som følge af nationale domstolsafgørelser efter afsigelsen af Tele2-dommen, uden at der er vedtaget ny lovgivning om logning. Der henvises i øvrigt for så vidt angår Tyskland til den samtidige besvarelse af spørgsmål nr. 623 (Alm. del) fra Folketingets Retsudvalg og for så vidt angår Sverige til den samtidige besvarelse af spørgsmål nr. 626 (Alm. del) fra Folketingets Retsudvalg.

Justitsministeriet har ikke modtaget bidrag fra Bulgarien, Cypern, Estland, Frankrig, Italien, Irland, Letland, Malta og Portugal. Det kan dog oplyses, at der som led i EU-medlemsstaternes drøftelser af Tele2-dommen i DAPIX-arbejdsgruppen blev foretaget en høring i efteråret 2017, og at disse 9 EU-medlemsstater i den forbindelse oplyste, at de nationale regler om logning på daværende tidspunkt ikke var blevet ophævet eller ændret efter afsigelsen af Tele2-dommen.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 516
Offentligt

Bilag U

Kammeradvokaten

JUSTITSMINISTERIET

Dato: 12. januar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2018-0035-0034
Dok.: 1715435

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmålene J-L
fra Folketingets Retsudvalg den 13. november 2020

Samrådsspørgsmål J:

Vil ministeren redegøre for, hvorfor man ikke straks ophører den ulovlige masselogning af danskernes teledata, når EU-Domstolens afgørelse af 6. oktober 2020 præciserer, at reglerne er i strid med EU-retten og ikke kan opretholdes midlertidigt, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?

Samrådsspørgsmål K:

Vil ministeren redegøre for teleselskabernes retsstilling i forhold til afgørelsen, herunder hvordan ministeren forventer selskaberne kan agere, efter det er fastslået og præciseret, at deres praksis - også midlertidigt - er i strid med EU-retten, men den danske stat pålægger dem at fortsætte denne praksis, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Samrådsspørgsmål L:
Vil ministeren redegøre for, hvorvidt regeringen med det lovforslag, som ifølge ministeren fremsættes i februar 2021, planlægger at ændre reglerne, således at de vil være i overensstemmelse med EU-retten og regler om retten til privatliv, jf. artiklen "Justitsministeren blæser på EU-traktaten trods tre domme: »Telebranchen skal stadig logge og udlevere oplysninger«" fra Version2 den 11. november 2020?

Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

[Indledning]

Tak for spørgsmålene.

De danske logningsregler er et emne, der står højt på min dagsorden som justitsminister, fordi logning er et helt afgørende efterforskningsredskab for politiet og PET.

Den 6. oktober 2020 afsagde EU-Domstolen dom i sagerne om de franske og belgiske logningsregler. Det er en afgørelse, vi længe har ventet på.

[Dommen af 6. oktober 2020]

Og lad mig her indledningsvist lige skitsere, hvad dommen indebærer.

Dommen af 6. oktober 2020 fastslår, at vi ikke kan pålægge teleudbyderne at logge tele- og trafikoplysninger på den måde, som vi gør i dag. Den indebærer ikke et

opgør med logning generelt. Men de danske regler om logning er nødt til at blive ændret.

Det er ikke nogen hemmelighed, at dommen ikke var det, vi fra regeringens side havde håbet på.

Det er vurderingen, at dommen indebærer, at vi efter en ændring af logningsreglerne ikke kan pålægge teleudbyderne at logge tele- og trafikoplysninger med henblik på at bekæmpe almindelig kriminalitet.

Politiet vil altså komme til at miste adgang til potentielt vigtige loggede oplysninger i en lang række sager. Også sager i hvilke loggede oplysninger i dag spiller en helt central rolle.

Det betyder, at politiet fremover må finde nye redskaber eller bruge andre redskaber end logning. Hvis de kan.

Og det betyder også, at der må forventes at være kriminalitet, som politiet ikke fremover vil kunne opklare. Kriminalitet, som i dag bliver opklaret.

Vi vil fra regeringens side gøre alt, hvad vi kan for at opretholde så meget logning som muligt inden for rammerne af EU-retten.

Og dommen af 6. oktober indeholder da også en række muligheder i den forbindelse.

Dommen giver os som noget nyt adgang til at pålægge teleudbyderne at logge tele- og trafikoplysninger med henblik på beskyttelse af den nationale sikkerhed. For eksempel bekæmpelse af terror. Også uanset, om logningen foregår generelt og uden forskel på, hvem den rammer.

Der skal dog foreligge tilstrækkelige konkrete grunde til at antage, at der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

Dommen kommer også ind på, hvad der mere specifikt skal til for at have regler om målrettet logning til at bekæmpe grov kriminalitet. Her specificeres det i dommen, hvilke geografiske kriterier der f.eks. vil kunne lægges til grund for en målrettet logning.

Disse nye elementer om national sikkerhed og grov kriminalitet er essentielle. De giver os mulighed for at opretholde logning i en vis udstrækning. Men det er vurderingen, at den generelle logning, vi har i dag, og som kan bruges til at opklare almindelig kriminalitet, altså må ophøre.

Derfor er der behov for at gennemtænke de nye elementer i dommen grundigt og afklare, hvad de helt præcist betyder for den kommende indretning af de danske logningsregler.

Der er tale om komplicerede spørgsmål, og forskellige væsentlige hensyn skal afvejes grundigt. Det drejer sig om:

- Hensynet til den enkeltes ret til privatliv,
- hensynet til, at teleselskaberne ikke pålægges unødige byrder, og
- hensynet til, at vores politi og efterretningstjeneste kan holde os alle sammen trygge.

Det kræver grundige overvejelser, både juridisk og teknisk – og ikke mindst i samspil med andre EU-lande.

Baseret på de hidtidige bilaterale drøftelser med en række EU-lande er det vurderingen, at de fleste EU-lande endnu ikke har taget stilling til, hvad dommen kommer til at betyde for deres nationale regler, heriblandt Frankrig og Belgien [som dommen af 6. oktober 2020 retter sig imod].

Når andre EU-lande heller ikke er kommet frem til en løsning endnu, er det fordi, at det tager tid. Det gør det også i Danmark.

Vi skal finde den rette balance mellem de forskellige hensyn.

Og finde en løsning, der i videst muligt omfang gør vores politi og efterretningstjeneste i stand til at passe på os – og på Danmark.

[Samrådsspørgsmål L om lovforslaget på lovprogrammet]

Lad mig så vende mig mod de tre samrådsspørgsmål.

Jeg vil egentlig gerne besvare dem "bagfra", dvs. begynde med samrådsspørgsmål L om regeringens planer for det lovforslag, der er på lovprogrammet til februar 2021.

Min holdning er som sagt klar: Politiet skal have de nødvendige værktøjer for at kunne efterforske og retsforfølge kriminalitet, herunder terror. Vi skal i videst muligt omfang sikre, at det også vil være tilfældet i fremtiden.

Som sagt skal vi finde den rette balance mellem de forskellige hensyn. Og finde den rette løsning. Det tager tid.

Regeringen forventer derfor først at kunne fremsætte et lovforslag, der materielt ændrer logningsreglerne, i åbningsugen i den kommende folketingssamling.

Det lovforslag, der vil blive fremsat i indeværende samling, vil altså være et forslag om at udskyde revisionen.

Men det betyder på ingen måde, at regeringen bare vil læne sig tilbage indtil næste folketingsår.

Samtidig med fremsættelsen af lovforslaget om udskydelse af revisionen vil jeg fremlægge en skitse til det kommende lovforslag om den materielle ændring af reglerne.

Det gør jeg for at lægge op til en åben drøftelse med bl.a. Folketingets partier, telebranchen og andre interessenter.

Jeg vil gerne tage debatten åbent og på et tidligt stadie. Så vi finder den rette løsning og sikrer, at politiet fortsat kan bruge loggede oplysninger i videst muligt omfang.

[Samrådsspørgsmål J om suspension af logningsregler]

Samrådsspørgsmål J handler, om hvorfor regeringen ikke suspenderer reglerne om logning.

Ifølge EU-retten er der ikke en bestemt frist for, hvor hurtigt en medlemsstat skal tage højde for en dom fra EU-Domstolen i en sag, der vedrører en anden medlemsstats regler.

Men man skal så hurtigt som muligt iværksætte foranstaltninger til opfyldelse af en sådan dom. Hvor hurtigt dette så skal ske, afhænger af sagens konkrete omstændigheder.

Og det her er – som jeg har været inde på – en kompliceret sag.

Og loggede oplysninger er simpelthen for vigtige til, at vi bare kan ophæve reglerne uden at have noget andet at sætte i stedet. Det er der i øvrigt heller ikke noget, der tyder på, at de andre EU-lande har tænkt sig at gøre på baggrund af dommen fra oktober 2020.

Og det er Justitsministeriets vurdering, at en materiel ændring af logningsreglerne i efteråret vil være tids nok i

forhold til at overholde princippet om ”så hurtigt som muligt”.

[Samrådsspørgsmål K om teleselskabernes retsstilling]

Lad mig så endelig vende mig mod samrådsspørgsmål K om teleselskaberne retsstilling. Det kan jeg også besvare ganske kort.

EU-Domstolens dom betyder ikke, at de gældende danske logningsregler sættes ud af kraft. De danske logningsregler er altså ikke pludseligt ophørt med at eksistere eller pludseligt blevet umiddelbart ugyldige.

Indtil vi får vedtaget en ny logningslovgivning til efteråret, håber jeg, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og terror.

Som sagt arbejder vi hårdt på at finde en løsning, der kan skabe klare rammer og sikre, at politiet har de bedst mulige redskaber til at kunne bekæmpe grov kriminalitet og terror i fremtiden.

[Afslutning]

Igen tak for samrådsspørgsmålene.

Som I ved, ligger det mig som justitsminister meget på sinde at sikre Danmarks og danskernes tryghed og sikkerhed.

Logning er et helt afgørende redskab i den forbindelse.

Derfor arbejder vi fra dansk side – sammen med ligesindede EU-partnere – også aktivt for at sætte logning på dagsordenen og finde en vej frem på EU-plan for at kunne bevare mest mulig adgang til at benytte logning som redskab. Det har vi bl.a. gjort på stats- og regeringschefniveau ved mødet i Det Europæiske Råd i december, ligesom jeg rejser det med mine kolleger i Rådet.

Men det bliver ikke let. Og jeg tror desværre, at chancerne for, at vi grundlæggende kan ændre EU-Domstolens opfattelse af de EU-retlige rammer for logning, er forsvindende små.

Derfor er det helt centralt, at vi i fællesskab finder den rette løsning og balance inden for rammerne af EU-retten.

Jeg ser frem til debatten – både her i dag og frem mod efteråret.

Tak for ordet.

TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Justitsministeriet
Att.: Justitsminister Nick Hækkerup

15. januar 2021

Kære Nick Hækkerup

Teleindustrien (TI) har noteret sig, at du på samrådet i Retsudvalget i går, den 14. januar 2021, kom med nogle tilkendegivelser, der rejser betydelig usikkerhed om retsgrundlaget for teleselskabernes fortsatte logning af trafik- og lokaliseringsdata.

I dit brev til TI den 30. oktober 2020 meddelte du følgende:

"EU-Domstolens dom betyder ikke, at de gældende danske lognings-regler sættes ud af kraft. Derfor skal telebranchen fortsat logge og udlevere oplysninger i overensstemmelse med gældende regler, indtil ny lovgivning måtte være vedtaget og trådt i kraft." (min understregning).

Teleselskaberne har på den baggrund indrettet sig på, at der fortsat efter danske regler påhviler en forpligtelse for selskaberne til at foretage logning og udlevere data til myndighederne.

På samrådet gentog du, at EU-Domstolens dom ikke betyder, at de gældende danske logningsregler sættes ud af kraft, men du udtalte også følgende:

"Indtil vi får vedtaget nye logningsregler, der håber jeg på teleselskabernes forståelse for, at politiet har adgang til at logge oplysninger til at efterforske grov kriminalitet og terror".

"Visse dele af de danske logningsregler strider mod EU-retten (EU Charteret), således som fortolket af EU-Domstolen og kan ikke håndhæves overfor teleudbyderne. Teleudbyderne kan derfor ikke straffes, hvis de undlader at logge teleoplysninger fremover".

De nævnte udtalelser efterlader en tvivl om, hvorvidt telebranchen fortsat skal logge og udlevere oplysninger i overensstemmelse med

gældende logningsregler, indtil ny lovgivning måtte være vedtaget og trådt i kraft.

Såfremt det kun er "visse dele" af logningsreglerne, som ikke længere er gældende, er det uklart, om det betyder, at teleselskaberne helt kan undlade at efterleve logningsbekendtgørelsen i sin helhed, eller om teleselskaberne blot kan undlade at efterleve visse dele af logningsbekendtgørelsen. Såfremt det alene vedrører visse dele af logningsbekendtgørelsen, bedes ministeren nærmere præcisere, hvilke dele af logningsbekendtgørelsen, som strider mod EU-retten, og i givet fald om teleselskaberne ikke længere er forpligtet til at logge disse oplysninger.

Hvis justitsministeren mener, at der ikke længere påhviler en pligt efter de danske logningsregler (helt eller delvist), men at det alene er op til teleselskabernes "forståelse" at fortsætte logning som anført i logningsbekendtgørelsen, bedes ministeren uddybende redegøre for, om en sådan logning vil være i overensstemmelse med databeskyttelsesreglerne, jf. §§ 10-11 i bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Vi noterede os også, at du håber på "teleselskabernes forståelse for, at politiet har adgang til at logge oplysninger til at efterforske grov kriminalitet og terror" (min understregning). Ministeren bedes i den sammenhæng oplyse, om ministerens udtalelse skal forstås således, at ministeren allerede nu vil at sikre, at politi- og anklagemyndigheden alene indhenter loggede data og hastesikrede data til sager, der vedrører grov kriminalitet og terror, og at ministeren således vil suspendere den mulighed, der findes i dag efter editionsreglerne, hvorefter politiet kan få loggede data og hastesikrede data udleveret til opklaring af sager, der vedrører mindre alvorlig kriminalitet.

Med venlig hilsen

Jakob Willer
Direktør

JUSTITSMINISTERIET
Justitsministeren

Teleindustrien
Att: Direktør Jakob Willer
Axeltorv 6, 3.
1609 København V

Dato: 29. januar 2021
Dok.: 1800609

Kære Jakob Willer

Tak for dit brev af 15. januar 2021, hvor du stiller en række spørgsmål om retsgrundlaget for teleselskabernes fortsatte logning af trafik- og lokaliseringsdata efter EU-Domstolens dom af 6. oktober 2020.

Det er vigtige og gode spørgsmål, du stiller, og jeg vil i det følgende besvare dem så præcist som muligt.

Om teleselskabernes logningsforpligtelse
I dit brev spørger du til det retlige grundlag for teleselskabernes logningsforpligtelse, herunder om det kan præciseres, hvilke dele af de danske logningsregler der strider mod EU-retten.

EU-Domstolens dom af 6. oktober 2020 indebærer ikke, at de gældende danske logningsregler sættes ud af kraft eller bliver umiddelbart ugyldige.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler.

Det fremgår af § 1 i logningsbekendtgørelsen, at "[u]dbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold".

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Det nærmere omfang af logningsforpligtelsen efter logningsbekendtgørelsens § 1 er reguleret i bekendtgørelsens kapitel 2 (§§ 4-9).

Disse regler om teleselskabernes logningsforpligtelse er således ikke efter EU-Domstolens dom af 6. oktober 2020 sat ud af kraft eller gjort umiddelbart ugyldige.

Det er imidlertid Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter dommen af 6. oktober 2020 ikke vil kunne begrundes af hensyn til bekæmpelsen af almindelig kriminalitet. Da de gældende logningsregler pålægger teleselskaberne at registrere og opbevare oplysninger om teletrafik til brug for efterforskning af alle strafbare forhold, er det således Justitsministeriets opfattelse, at teleselskaberne, indtil vi har de nye logningsregler på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke med afsæt i de danske regler vil kunne sondres mellem til, hvilke formål oplysningerne er blevet logget.

Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og terror, skal således ses i dette lys.

EU-Domstolen gentog i dommen af 6. oktober 2020 udgangspunktet fra Tele2-dommen om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse. Samtidig anførte EU-Domstolen dog, under hvilke betingelser udgangspunktet kan fraviges. Det gælder især logning med henblik på beskyttelse af den nationale sikkerhed, som f.eks. bekæmpelse af terror, samt målrettet logning vedrørende grov kriminalitet.

På den baggrund er det Justitsministeriets vurdering, at dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed og en målrettet logningsforpligtelse med henblik på bekæmpelse af grov kriminalitet under nærmere betingelser.

Om overensstemmelse med databeskyttelsesforordningen
Du spørger i dit brev også til, om det vil være i overensstemmelse med databeskyttelsesreglerne, hvis teleselskaberne fortsætter med at logge som hidtil.

EU-Domstolens dom af 6. oktober 2020 indebærer som anført ikke, at de gældende danske logningsregler sættes ud af kraft eller bliver umiddelbart ugyldige.

Teleselskabernes behandling (såsom indsamling, opbevaring og videregivelse, f.eks. til politiet på baggrund af en retskendelse) af loggede teleoplysninger skal bl.a. overholde databeskyttelsesforordningens (GDPR) grundlæggende krav om, at alle typer af behandling skal have et lovligt formål, jf. artikel 5, stk. 1, litra a og b.

I det omfang teleselskabernes behandling af loggede teleoplysninger er i overensstemmelse med dansk ret eller EU-retten som fortolket af EU-Domstolen, vil GDPR ikke være til hinder for teleselskabernes fortsatte behandling af loggede teleoplysninger i overensstemmelse med logningsbekendtgørelsens bestemmelser.

Som anført ovenfor er det Justitsministeriets vurdering, at dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed og en målrettet logningsforpligtelse med henblik på bekæmpelse af grov kriminalitet under nærmere betingelser. Trafik- og lokaliseringsdata vil således efter GDPR fortsat kunne logges som hidtil med henblik på beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet.

Når teleselskaber derudover ved retskendelse bliver pålagt at videregive logningsoplysninger til politiet, vil der være hjemmel i GDPR for teleselskaberne til videregivelsen (artikel 6, stk. 1, litra c, om opfyldelse af en retlig forpligtelse).

Videregivelsen vil herudover også skulle opfylde det grundlæggende krav i GDPR artikel 5, stk. 1, litra a og b, om, at al behandling (herunder videregivelse til politiet) skal forfølge et lovligt formål. Det er således Justitsministeriets vurdering, at det vil være i overensstemmelse med artikel 5 at videregive oplysningerne til politiet, i det omfang det sker på bagrund af en retskendelse, idet en sådan kendelse således i sig selv vil udgøre et tilstrækkeligt lovligt formål for teleselskabernes videregivelse til politiet.

Om politiets og anklagemyndighedens adgang til loggede data

Endelig spørger du i dit brev til, om de gældende regler om politiets og anklagemyndighedens adgang til loggede data med henblik på bekæmpelse af almindelig kriminalitet vil blive suspenderet.

Der er – på nuværende tidspunkt – ingen planer om at suspendere de danske regler om politi og anklagemyndigheds adgang til loggede oplysninger. Dette vil kunne ændre sig, når den endelige lovskitse til de nye logningsregler foreligger.

Som nævnt på samrådet den 14. januar 2021 er det vurderingen, at dommen indebærer, at loggede oplysninger efter en revision af logningsreglerne ikke vil kunne anvendes som bevismiddel i straffesager om almindelig kriminalitet.

Der er i dag ikke en klar afgrænsning af, hvad der udgør henholdsvis almindelig kriminalitet og grov kriminalitet – hverken i dansk eller EU-retlig sammenhæng. Justitsministeriet arbejder derfor på at klarlægge, hvad der skal forstås som henholdsvis almindelig og grov kriminalitet i forbindelse med forberedelsen af de nye logningsregler.

Når anklagemyndigheden indtil videre fortsat kan anvende loggede oplysninger som bevismiddel og under efterforskningen af en straffesag, også om almindelig kriminalitet, skal det bl.a. ses i sammenhæng med, at loggede oplysninger altid vil indgå som ét blandt flere beviser i en straffesag, og at betydningen af et bevis i form af teledata altid vil bero på en konkret vurdering af dels det enkelte bevis, dels sagens omstændigheder i øvrigt.

Opsamling
Det er således vurderingen, at den logningsforpligtelse, der følger af logningsbekendtgørelsen, fortsat er i kraft, men at teleselskaberne, indtil vi har de nye logningsregler på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen. Efter GDPR vil der fortsat kunne logges trafik- og lokaliseringsdata som hidtil med henblik på beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet. Endvidere vil det være i overensstemmelse med GDPR at videregive disse oplysninger til politiet på baggrund af en retskendelse.

Afslutningsvist vil jeg gerne takke for den konstruktive dialog om revisionen af logningsreglerne. Det er komplicerede spørgsmål, hvor det er centralt, at vi kan inddrage jeres erfaringer og mangeårige indsigt.

Jeg ser derfor frem til det kommende samarbejde om revision af lognings-reglerne mv.

Med venlig hilsen

Nick Hækkerup

Retsudvalget 2020-21
REU Alm.del - Bilag 174
Offentligt

Bilag Æ

Kammeradvokaten

JUSTITSMINISTERIET

Dato: 29. januar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-187-0037
Dok.: 1753473

Forslag
til
Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige
(Ændring af revisionsbestemmelse)

§ 1

I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006, lov nr. 650 af 15. juni 2010, lov nr. 573 af 18. juni 2012, lov nr. 635 af 12. juni 2013, lov nr. 640 af 8. juni 2016, lov nr. 673 af 8. juni 2017, lov nr. 716 af 8. juni 2018 og lov nr. 644 af 19. maj 2020, foretages følgende ændring:

1. I *§ 8* ændres »2020-21« til: »2021-22«.

§ 2

Loven træder i kraft [den 1. juni 2021].

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Det påhviler justitsministeren i folketingsåret 2020-21 at fremsætte lovforslag om revision af retsplejelovens § 786, stk. 4, der fastsætter en pligt for teleudbyderne til at registrere og opbevare (logge) oplysninger om tele- og internettrafik til brug for efterforskning og retsforfølgning af strafbare forhold, jf. § 8 i lov nr. 378 af 6. juni 2002 om ændring af retsplejeloven mv., som senest ændret ved lov nr. 644 af 19. maj 2020.

Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende logningsregler. Logningsreglerne indebærer overordnet set, at en række oplysninger om tele- og internetkommunikation skal registreres og opbevares hos teleudbyderne, således at politiet, herunder Politiets Efterretningstjeneste (PET), til brug for efterforskning og retsforfølgning af strafbare forhold kan indhente nærmere specificerede oplysninger, som de har brug for i konkrete sager. Det er en betingelse for politiets indhentelse af oplysninger, at oplysningerne i hvert enkelt tilfælde indhentes i overensstemmelse med retsplejelovens almindelige regler om indgreb i meddelelseshemmeligheden og edition. Det forudsætter som udgangspunkt, at rettens kendelse opnås forud for indhentelsen. De almindelige regler i retsplejeloven om tvangsindgreb gælder også for PET, jf. PET-lovens § 6.

Ved lov nr. 644 af 19. maj 2020 om ændring af retsplejeloven og visse andre love (Ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2020-21.

Baggrunden for udskydelsen var bl.a., at udformningen af de nye logningsregler efter Justitsministeriets vurdering burde ske på et fuldt oplyst grundlag, og at rækkevidden af Tele2-dommen (EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson

m.fl.) skulle fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Endvidere verserede der på tidspunktet sager for EU-Domstolen (de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.), som kunne få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler. Som følge heraf og i lyset af, at EU-Domstolens kommende domme i de ovenfor omtalte logningssager ville kunne give svar på, hvordan logningsregler kan indrettes, fandt Justitsministeriet det derfor rigtigst at afvente EU-Domstolens domme, inden der blev taget stilling til den fremtidige indretning af de danske logningsregler.

EU-Domstolen har den 6. oktober 2020 afsagt dom i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af grov kriminalitet og terror. Der henvises til notat af 19. november 2020, som er sendt til Folketingets Retsudvalg og Folketingets Europaudvalg (EUU Alm. del – bilag 101).

I dommen af 6. oktober 2020 indgår en række nye elementer. Selvom EU-Domstolen gentager udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse, så fastslår EU-Domstolen samtidig under hvilke betingelser og i hvilke situationer, udgangspunktet kan fraviges. Det gælder bl.a. logning med henblik på beskyttelse af den nationale sikkerhed.

Det er Justitsministeriets vurdering, at der på baggrund af dommen af 6. oktober 2020 er behov for at ændre i de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Endvidere vurderes det nødvendigt at ændre reglerne om adgang til loggede oplysninger, herunder retsplejelovens bestemmelser om edition, indgreb i meddelelseshemmeligheden mv.

Det er fortsat Justitsministeriets vurdering, at udformningen af de nye logningsregler bør ske på et fuldt oplyst grundlag, og at rækkevidden af dommen af 6. oktober 2020 bør fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Dette vil sikre, at de nye regler holdes inden for EU-rettens rammer. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen i Danmark ikke pålægges unødige byrder. Justitsministeriet er derfor i tæt dialog med de øvrige medlemsstater, om hvordan dommen skal

fortolkes. Regeringen forventer at kunne præsentere en skitse til revision af de danske regler på området i løbet af foråret 2021.

Som følge heraf foreslås det at udskyde revisionen af logningsreglerne til folketingsåret 2021-22.

2. Gældende ret

2.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og energi-, forsynings- og klimaministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at udbyderne alene skal logge oplysninger om trafikdata og ikke selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom pkt. 2.3.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition. Det betyder bl.a., at udlevering af

oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at rettens kendelse opnås forud for udleveringen.

2.2. Revisionsbestemmelsen vedrørende retsplejelovens § 786, stk. 4

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres.

Efter § 8 i lov nr. 378 af 6. juni 2002 skulle justitsministeren således i folketingsåret 2005-06 fremsætte forslag om revision af retsplejelovens § 786, stk. 4. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3.1.3.3 i de almindelige bemærkninger til L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 854), at en ordning med pligtmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning var en nyskabelse, og at Justitsministeriet fandt det hensigtsmæssigt at evaluere ordningen nogle år efter dens iværksættelse.

Ved § 7 i lov nr. 542 af 8. juni 2006 blev revisionen udskudt til folketingsåret 2009-10. Baggrunden herfor var ifølge lovens forarbejder (pkt. 10.2 i de almindelige bemærkninger til L 217 som fremsat, jf. Folketingstidende 2005-2006, Tillæg A, side 7217), at der i 2006 endnu ikke forelå nogen erfaringer med anvendelsen af retsplejelovens § 786, stk. 4, som – sammen med logningsbekendtgørelsen – først blev sat i kraft den 15. september 2007. Logningsbekendtgørelsens regler gennemførte bl.a. Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet).

Ved lov nr. 650 af 15. juni 2010 blev revisionen udskudt til folketingsåret 2011-12, således at bl.a. resultatet af en evaluering af logningsdirektivet i EU-regi kunne indgå i overvejelserne i forbindelse med revisionen. Justitsministeriet var endvidere enig med bl.a. Rigspolitiet i, at det ville være hensigtsmæssigt at indhente yderligere erfaring med logningsreglerne med henblik på at vurdere behovet for eventuelle ændringer. Der henvises til lovens forarbejder (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2009-10, A, L 180 som fremsat, side 7).

Ved lov nr. 573 af 18. juni 2012 blev revisionen udskudt til folketingsåret 2012-13. Revisionen blev oprindeligt foreslået udskudt til folketingsåret

2013-14 under hensyn til, at Kommissionen i tilknytning til offentliggørelsen af en evalueringsrapport om logningsdirektivet havde bebudet et forslag til revision af logningsdirektivet i løbet af 2012. Under behandlingen af lovforslaget i Folketinget blev revisionsbestemmelsen imidlertid ændret, idet et flertal i Folketinget ønskede at fremrykke revisionen til folketingsåret 2012-13. Der henvises til lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2011-12, A, L 53 som fremsat, side 4, og Retsudvalgets betænkning af 31. maj 2012, B, side 3).

Ved lov nr. 635 af 12. juni 2013 blev revisionen udskudt til folketingsåret 2014-15. Baggrunden herfor var ifølge lovens forarbejder (pkt. 5 i de almindelige bemærkninger, jf. Folketingstidende 2012-2013, A, L 142 som fremsat, side 5), at Kommissionens tidligere bebudede forslag til revision af logningsdirektivet nu først forventedes fremsat i løbet af 2013 eller eventuelt 2014. Justitsministeriet tilkendegav endvidere i forbindelse med behandlingen af forslaget, at reglerne om logning af oplysninger om internettrafik (sessionslogning) efter ministeriets opfattelse burde revideres i folketingsåret 2014-15, uanset om revisionen af logningsdirektivet måtte blive yderligere forsinket med den konsekvens, at de logningsregler, der byggede på direktivet, ikke kunne revideres i det pågældende folketingsår, jf. besvarelsen af spørgsmål nr. 14 (L 142) fra Folketingets Retsudvalg.

Der blev i folketingsåret 2014-15 fremsat lovforslag om at udskyde revisionen til folketingsåret 2015-16. Baggrunden herfor var ifølge forslaget (pkt. 4 i de almindelige bemærkninger, jf. Folketingstidende 2014-15 (1. samling), A, L 193 som fremsat, side 5) at afvente en afklaring af, om – og i givet fald hvornår – Kommissionen ville fremsætte forslag om nye EU-regler på området efter EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights Ireland Ltd. Lovforslaget nåede dog ikke at blive vedtaget på grund af udskrivelsen af folketingsvalg den 27. maj 2015.

Ved lov nr. 640 af 8. juni 2016 blev revisionen udskudt til folketingsåret 2016-17. Baggrunden herfor var, at et eksternt konsulentfirma havde foretaget beregninger vedrørende en række anbefalinger, som Rigspolitiet var fremkommet med til brug for revisionen, som pegede på, at omstillingsomkostninger for udbyderne ved at følge anbefalingerne var i omegnen af en milliard kr. Det oversteg efter Justitsministeriets opfattelse grænsen for det acceptable. Samtidig havde Justitsministeriet indledt en dialog med en række store udbydere og interesseorganisationer inden for tele- og internetbranchen, og ministeriet fandt det hensigtsmæssigt at fortsætte denne dialog,

før revisionen blev foretaget. Der henvises til lovens forarbejder (pkt. 2.2 i de almindelige bemærkninger, jf. Folketingstidende 2015-16, A, L 183 som fremsat, side 4).

Ved lov nr. 673 af 8. juni 2017 blev revisionen udskudt til folketingsåret 2017-18. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2016-17, A, L 191 som fremsat, side 6-7) navnlig, at Justitsministeriet var ved at udrede, hvordan de danske logningsregler kunne tilpasses i lyset af EU-Domstolens dom i Tele2-sagen, jf. pkt. 2.3 nedenfor, at et centralt element i den udredning var en dialog med de andre EU-lande, og at EU-Kommissionen havde tilkendegivet at ville udarbejde retningslinjer for, hvordan medlemsstaterne kunne fastsætte nationale logningsregler i lyset af dommen i Tele2-sagen.

Ved lov nr. 716 af 8. juni 2018 blev revisionen udskudt til folketingsåret 2018-19. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2017-18, A, L 218 som fremsat, side 5-6), at det efter Justitsministeriets opfattelse var afgørende, at udformningen af nye logningsregler skete på et fuldt oplyst grundlag, og at udlægningen af Tele2-dommens konsekvenser skete i fællesskab med de øvrige EU-lande og EU-Kommissionen. Den fælles proces var vigtig for at sikre, at de nye regler holdes inden for EU-rettens rammer, og at politiet, herunder PET, samtidig har de redskaber, der skal til for at bekæmpe alvorlig kriminalitet. Endvidere ville en fælles tilgang i EU efter Justitsministeriets opfattelse være med til at sikre, at telebranchen ikke pålagdes unødige byrder.

Justitsministeren fremsatte den 24. april 2019 et lovforslag om udskydelse af revision af logningsreglerne til folketingsåret 2019-20. Lovforslaget bortfaldt som følge af udskrivelsen af folketingsvalg den 7. maj 2019.

Ved lov nr. 644 af 19. maj 2020 blev revisionen udskudt til folketingsåret 2020-21. Baggrunden herfor var ifølge lovens forarbejder (pkt. 3 i de almindelige bemærkninger, jf. Folketingstidende 2019-20, A, L 87 som fremsat, side 6) bl.a., at udformningen af de nye logningsregler efter Justitsministeriets vurdering burde ske på et fuldt oplyst grundlag, og at rækkevidden af Tele2-dommen (EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl.) skulle fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Endvidere verserede der på tidspunktet sager for EU-Domstolen (de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.), som kunne få betydning for

medlemsstaternes mulighed for at fastsætte nationale logningsregler. Som følge heraf og i lyset af, at EU-Domstolens kommende domme i de ovenfor omtalte logningssager ville kunne give svar på, hvordan logningsregler kan indrettes, fandt Justitsministeriet det derfor rigtigst at afvente EU-Domstolens domme, inden der blev taget stilling til den fremtidige indretning af de danske logningsregler.

2.3. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i § 2, nr. 1, i lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer om elektroniske kommunikationsnet og -tjenester (teleloven). Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger

og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til på kommunikationstidspunktet, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Det gælder bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

2.4. EU-Domstolens dom af 6. oktober 2020 i de forenede sager forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. (om de franske og belgiske logningsregler)

I EU-Domstolens dom af 6. december 2020 i sagerne om de franske og belgiske logningsregler gentager EU-Domstolen udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for national lovgivning, der pålægger teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata med henblik på, at offentlige myndigheder kan få adgang til disse data (logning). EU-Domstolen anfører dog samtidig under hvilke betingelser, udgangspunktet kan fraviges, således at medlemsstaterne kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata.

2.4.1. Alvorlig trussel mod den nationale sikkerhed

EU-Domstolen fastslår for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed (præmis 134-139). I den forbindelse bemærker EU-Domstolen, at artikel 4, stk. 2, i EU-Traktaten fastslår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, samt formålet om beskyttelsen af national sikkerhed vejere tungere end f.eks. formålet om bekæmpelse af kriminalitet, hvorfor formålet kan retfærdiggøre mere alvorlige indgreb i grundlæggende rettigheder.

Som følge heraf er EU-retten ikke til hinder for, at medlemsstaterne kan pålægge teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata for en begrænset tidsperiode, så længe der er tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig. Lagringen må dog kun ske i en afgrænset periode, der skal begrænses til det strengt nødvendige. Perioden kan forlænges, hvis den alvorlige trussel fortsætter, men EU-Domstolen understreger i den forbindelse, at lagring af data ikke må have en systematisk karakter (”systematic in nature”). Endelig skal den generelle og udifferentierede lagring ledsages

af mulighed for en efterfølgende effektiv prøvelse af bl.a., om der foreligger en sådan alvorlig trussel mod den nationale sikkerhed.

2.4.2. Bekæmpelse af grov kriminalitet eller beskyttelse mod alvorlige trusler mod den offentlige sikkerhed

Dernæst fastslår EU-Domstolen, at *grov* kriminalitet og beskyttelse mod *alvorlige* trusler mod den offentlige sikkerhed ikke kan retfærdiggøre en generel og udifferentieret lagring af trafik- og lokaliseringsdata (præmis 140-151).

Men EU-Domstolen udelukker i den forbindelse ikke, at der med henblik på bl.a. at bekæmpe grov kriminalitet kan pålægges en *målrettet* lagringsforpligtelse af trafik- og lokaliseringsdata ("targeted retention"). EU-Domstolen gentager her, hvad den tidligere sagde i bl.a. Tele2-dommen, hvorefter medlemsstaterne kan pålægge teleudbydere mv. en pligt til at lagre trafik- og lokaliseringsdata "vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af grov kriminalitet".

For så vidt angår målrettet lagring af disse data ud fra et geografisk kriterium bemærker EU-Domstolen, at det kan være områder med høj hyppighed af grov kriminalitet, steder, hvor der i særlig grad kan begås grov kriminalitet, som f.eks. infrastruktur, som regelmæssigt har mange besøgende, eller strategiske områder, såsom lufthavne, banegårde og vejafgiftsområder.

Den målrettede lagring af disse data må kun lagres, så længe det er strengt nødvendigt i lyset af formålet og de omstændigheder, der retfærdiggør laggringen. Det vil dog være muligt at forlænge foranstaltningerne, hvis fortsat lagring er nødvendig.

2.4.3. Lagring af IP-adresser og oplysninger om personers identitet

EU-Domstolen anfører videre – som noget nyt – at medlemsstaterne kan fastsætte national lovgivning, der muliggør generel og udifferentieret lagring af *alle brugeres IP-adresser*, der er tildelt kilden til en forbindelse (præmis 152-159). Dette må dog alene ske med henblik på at bekæmpe grov kriminalitet eller forhindre alvorlige trusler mod den nationale sikkerhed eller offentlige sikkerhed. Lagring af IP-adresserne må alene ske i en periode, der er begrænset til det strengt nødvendige, og myndighedernes adgang til IP-adresserne skal være nøje reguleret i lovgivningen.

For så vidt angår oplysninger om identiteten på brugerne af elektroniske kommunikationsmidler (”*civil identity*”) fastslår EU-Domstolen, at medlemsstaterne kan pålægge teleudbydere mv. at lagre data vedrørende personers identitet med henblik på at forhindre eller efterforske alle strafbare handlinger og beskytte mod trusler mod den offentlige sikkerhed. I den forbindelse bemærker EU-Domstolen, at der ikke er noget krav om, at kriminaliteten eller truslen er alvorlig. Krav om lagring af data om personers identitet er ikke underlagt nogen tidsbegrænsning.

2.4.4. Pålæg om hurtig lagring for at bekæmpe grov kriminalitet eller handlinger, der kan skade den nationale sikkerhed
EU-Domstolen fastslår endelig, at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. en hurtig lagring af trafik- og lokaliseringsdata, som de allerede råder over (præmis 160-165).

Der kan således i visse situationer i et udvidet omfang ske målrettet lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds. En sådan målrettet lagring kan udelukkende ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. En sådan lagring skal begrænses tidsmæssigt til det strengt nødvendige, og pålægget herom skal kunne underlægges en effektiv prøvelse.

3. Justitsministeriets overvejelser og den foreslåede ordning

Ved lov nr. 644 af 19. maj 2020 om ændring af retsplejeloven og visse andre love (Ændring af revisionsbestemmelse) udskød Folketinget revisionen af logningsreglerne til samlingen 2020-21.

Baggrunden for udskydelsen var bl.a., at udformningen af de nye logningsregler efter Justitsministeriets vurdering burde ske på et fuldt oplyst grundlag, og at rækkevidden af Tele2-dommen (EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 og Watson m.fl.) skulle fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Endvidere verserede der på tidspunktet sager for EU-Domstolen

(de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl.), som kunne få betydning for medlemsstaternes mulighed for at fastsætte nationale logningsregler. Som følge heraf og i lyset af, at EU-Domstolens kommende domme i de ovenfor omtalte logningssager ville kunne give svar på, hvordan logningsregler kan indrettes, fandt Justitsministeriet det derfor rigtigst at afvente EU-Domstolens domme, inden der blev taget stilling til den fremtidige indretning af de danske logningsregler.

EU-Domstolen har den 6. oktober 2020 afsagt dom i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af grov kriminalitet og terror. Der henvises til notat af 19. november 2020, som er sendt til Folketingets Retsudvalg og Folketingets Europaudvalg (EUU Alm. del – bilag 101).

I dommen af 6. oktober 2020 indgår en række nye elementer. Selvom EU-Domstolen gentager udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse, så fastslår EU-Domstolen samtidig under hvilke betingelser og i hvilke situationer, udgangspunktet kan fraviges. Det gælder bl.a. logning med henblik på beskyttelse af den nationale sikkerhed.

Det er Justitsministeriets vurdering, at der på baggrund af dommen af 6. oktober 2020 er behov for at ændre i de gældende regler om registrering og opbevaring af oplysninger om tele- og internettrafik. Endvidere vurderes det nødvendigt at ændre reglerne om adgang til loggede oplysninger, herunder retsplejelovens bestemmelser om edition, indgreb i meddelelseshemmeligheden mv.

Det er fortsat Justitsministeriets vurdering, at udformningen af de nye logningsregler bør ske på et fuldt oplyst grundlag, og at rækkevidden af dommen af 6. oktober 2020 bør fastlægges i fællesskab med de øvrige EU-lande og EU-Kommissionen. Dette vil sikre, at de nye regler holdes inden for EU-rettens rammer. Desuden vil en fælles tilgang i EU være med til at sikre, at telebranchen i Danmark ikke pålægges unødige byrder. Justitsministeriet er derfor i tæt dialog med de øvrige medlemsstater, om hvordan dommen skal fortolkes. Regeringen forventer at kunne præsentere en skitse til revision af de danske regler på området i løbet af foråret 2021.

Som følge heraf foreslås det at udskyde revisionen af logningsreglerne til folketingsåret 2021-22.

Der henvises til lovforslagets § 1, nr. 1.

Det bemærkes i den forbindelse, at efter EU-Domstolens praksis skal medlemsstaterne så hurtigt som muligt iværksætte foranstaltninger til opfyldelse af en dom. Hvor hurtigt det skal ske, afhænger af sagens konkrete omstændigheder.

Spørgsmålet om, hvordan logningsregler, der er inden for EU-rettens rammer, kan indrettes, er kompliceret, og rækkevidden af dommen af 6. oktober 2020, der som nævnt ovenfor indeholder nye elementer, bør fastlægges i fællesskab med de øvrige EU-lande og Kommissionen. Som følge heraf og i lyset af, at regeringen forventer at kunne præsentere et udkast til revision af de danske regler på området i løbet af 2021, vurderer Justitsministeriet, at det vil være muligt at udskyde et lovforslag om revision af logningsreglerne.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget har ingen økonomiske konsekvenser eller implementeringskonsekvenser for stat, kommuner og regioner.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Lovforslaget har ingen økonomiske eller administrative konsekvenser for erhvervslivet mv.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget har ikke i sig selv EU-retlige aspekter. Det bemærkes dog, at det forventes, at der i lyset af EU-Domstolens dom af 6. oktober 2020 vil skulle foretages tilpasninger af de danske logningsregler og reglerne om adgang til loggede oplysninger, herunder retsplejelovens bestemmelser om edition, indgreb i meddelelseshemmeligheden mv., jf. nærmere herom pkt. 2.4 og pkt. 3.

9. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den [dato – dato] været sendt i høring hos følgende myndigheder og organisationer mv.:

[Østre Landsret, Vestre Landsret, Sø- og Handelsretten, samtlige byretter, Domstolsstyrelsen, Den Danske Dommerforening, Dommerfuldmægtigforeningen, HK-Landsklubben Danmarks Domstole, Rigsadvokaten, Foreningen af Offentlige Anklagere, Rigspolitiet, Politiets Efterretningstjeneste, Politiforbundet, HK-Landsklubben for Politiet, Datatilsynet, Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Forbrugerrådet TÆNK, Landsforeningen af Forsvarsadvokater, Ingeniørforeningen IDA, Institut for Menneskerettigheder, Dansk Journalistforbund, Justitia, Rådet for Digital Sikkerhed, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Brancheorganisationen Forbruger Elektronik, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, DI Digital, PROSA, SAMDATA (HK), Business Software Alliance Danmark, IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter og Cafeer, Danhostel og KLID.]

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Ingen
Administrative konsekvenser for erhvervslivet	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget har ikke i sig selv EU-retlige aspekter. Der henvises til pkt. 8.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering /Går videre end minimumskrav i EU-regulering (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Ifølge § 8 i lov nr. 378 af 6. juni 2002, som senest ændret ved lov nr. 644 af 19. maj 2020, skal justitsministeren i folketingsåret 2020-21 fremsætte forslag om revision af retsplejelovens § 786, stk. 4, om teleudbyderes registrering og opbevaring (logning) af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Med den foreslåede bestemmelse udskydes denne revision til folketingsåret 2021-22.

Der henvises til pkt. 3 i de almindelige bemærkninger i lovforslaget.

Til § 2

Det foreslås, at loven træder i kraft [den 1. juni 2021].

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 1
	I lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.), som ændret bl.a. ved § 7 i lov nr. 542 af 8. juni 2006 og senest ved lov nr. 644 af 19. maj 2020, foretages følgende ændring:
§ 8. Justitsministeren fremsætter i folketingsåret 2020-21 forslag om revision af retsplejelovens § 786, stk. 4, som affattet ved denne lovs § 2, nr. 3.	**1.** I *§ 8* ændres »2020-21« til: »2021-22«.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 562
Offentligt

Bilag Ø

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. februar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2021-0030-5502
Dok.: 1810766

Besvarelse af spørgsmål nr. 562 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 562 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. januar 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 562 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren i forlængelse af samrådet den 14. januar 2021 om logningsbekendtgørelsen, hvor ministeren oplyste, at logningsbekendtgørelsen ikke kan håndhæves grundet EU-retten og dennes forrang, men at ministeren stadig ønskede, at teleselskaberne skal fortsætte praksis, redegøre for teleselskabernes retsstilling, herunder for retsstillingen i forhold til GDPR artikel 6, stk. 1, litra c, som forudsætter en retlig forpligtelse til at gemme oplysninger, som selskaberne ikke selv har et forretningsmæssigt behov for?"

Svar:

1. Retsplejelovens § 786, stk. 4, udgør – sammen med bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014 (logningsbekendtgørelsen), der er udstedt med hjemmel i bestemmelsen – de gældende danske logningsregler.

Følgende fremgår af § 1 i logningsbekendtgørelsen:

> "**§ 1.** Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold."

Det nærmere omfang af logningsforpligtelsen efter logningsbekendtgørelsens § 1 er reguleret i bekendtgørelsens kapitel 2 (§§ 4-9).

2. EU-Domstolen har som bekendt den 6. oktober 2020 afsagt dom i EU-Domstolens forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen har betydning for medlemsstaternes mulighed for at pålægge teleudbydere mv. at lagre oplysninger om tele- og internettrafik til brug for bl.a. efterforskning og retsforfølgning af kriminalitet og terror. Der henvises til notat af 19. november 2020, som er sendt til Folketingets Retsudvalg og Folketingets Europaudvalg (EUU Alm. del – bilag 101).

I dommen af 6. oktober 2020 indgår en række nye elementer. Selvom EU-Domstolen gentager udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse, fastslår EU-Domstolen samtidig, under hvilke betingelser og i hvilke situationer dette udgangspunkt kan fraviges. Det gælder især logning med henblik på beskyttelse af den nationale sikkerhed, som f.eks. bekæmpelse af terror, samt målrettet logning med henblik på bekæmpelse af grov kriminalitet.

3. EU-Domstolens dom af 6. oktober 2020 indebærer ikke, at de gældende danske logningsregler sættes ud af kraft eller bliver umiddelbart ugyldige.

Det er imidlertid Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter dommen af 6. oktober 2020 ikke vil kunne begrundes af hensyn til bekæmpelsen af *almindelig kriminalitet*.

Da de gældende logningsregler pålægger teleselskaberne at registrere og opbevare oplysninger om teletrafik til brug for efterforskning af alle strafbare forhold, er det således Justitsministeriets opfattelse, at teleselskaberne, indtil nye logningsregler er på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke i de gældende danske regler sondres mellem, til hvilke formål oplysningerne logges.

Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske *grov kriminalitet* og *beskytte den nationale sikkerhed*, skal ses i dette lys.

Som nævnt ovenfor anfører EU-Domstolen i dommen af 6. oktober 2020 betingelser, hvorunder det er muligt at fravige udgangspunktet om, at EU-retten er til hinder for en generel og udifferentieret logningsforpligtelse.

Det er Justitsministeriets vurdering, at dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på *beskyttelse af den nationale sikkerhed* og en målrettet logningsforpligtelse med henblik på *bekæmpelse af grov kriminalitet* under nærmere betingelser.

4. Teleselskabernes behandling (såsom indsamling, opbevaring og videregivelse, f.eks. til politiet på baggrund af en retskendelse) af loggede teleop-

lysninger skal bl.a. overholde databeskyttelsesforordningens grundlæggende krav om, at alle typer af behandling skal have et lovligt formål, jf. artikel 5, stk. 1, litra a og b.

I det omfang teleselskabernes behandling af loggede teleoplysninger er i overensstemmelse med dansk ret eller EU-retten som fortolket af EU-Domstolen, vil databeskyttelsesforordningen ikke være til hinder for teleselskabernes fortsatte behandling af loggede teleoplysninger i overensstemmelse med logningsbekendtgørelsens bestemmelser.

Som anført ovenfor er det Justitsministeriets vurdering, at dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed og en målrettet logningsforpligtelse med henblik på bekæmpelse af grov kriminalitet under nærmere betingelser.

Trafik- og lokaliseringsdata vil således efter databeskyttelsesforordningen fortsat kunne logges som hidtil med henblik på beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet.

Når teleselskaber derudover ved retskendelse bliver pålagt at videregive logningsoplysninger til politiet, vil der være hjemmel i databeskyttelsesforordningen for teleselskaberne til videregivelsen (artikel 6, stk. 1, litra c, om opfyldelse af en retlig forpligtelse).

Videregivelsen vil herudover også skulle opfylde det grundlæggende krav i databeskyttelsesforordningens artikel 5, stk. 1, litra a og b, om, at al behandling (herunder videregivelse til politiet) skal forfølge et lovligt formål. Det er således Justitsministeriets vurdering, at det vil være i overensstemmelse med artikel 5 at videregive oplysningerne til politiet, i det omfang det sker på bagrund af en retskendelse, idet en sådan kendelse således i sig selv vil udgøre et tilstrækkeligt lovligt formål for teleselskabernes videregivelse til politiet.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 563
Offentligt

Bilag Å

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. februar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2021-0030-5503
Dok.: 1810784

Besvarelse af spørgsmål nr. 563 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 563 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. januar 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 563 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren i forlængelse af samrådet den 14. januar 2021 om logningsbekendtgørelsen redegøre for det juridiske afsæt for ministerens udtrykte ønske om, at selskaberne fortsætter logningspraksis? Vil ministeren herunder redegøre for, hvorledes ministerens udtrykte ønske er i overensstemmelse med EU-retten, i lyset af at ministeren har erkendt, at logningsbekendtgørelsen ikke kan håndhæves og den retlige forpligtelse til logning ikke foreligger?”

Svar:

Der henvises til den samtidige besvarelse af spørgsmål nr. 562 (Alm. del) fra Folketingets Retsudvalg.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 564
Offentligt

Bilag AA

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. februar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2021-0030-5504
Dok.: 1810793

Besvarelse af spørgsmål nr. 564 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 564 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. januar 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 564 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren i forlængelse af samrådet den 14. januar 2021 om logningsbekendtgørelsen oplyse, hvorvidt teleselskaberne kan sanktioneres efter GDPR, såfremt selskaberne fortsætter med at logge?”

Svar:

Der henvises til den samtidige besvarelse af spørgsmål nr. 562 (Alm. del) fra Folketingets Retsudvalg.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 565
Offentligt

Bilag AB

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. februar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2021-0030-5505
Dok.: 1810806

Besvarelse af spørgsmål nr. 565 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 565 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. januar 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 565 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren i forlængelse af samrådet den 14. januar 2021 om logningsbekendtgørelsen redegøre for, hvorvidt han mener, at man sætter teleselskaberne i en acceptabel situation, såfremt ministeren fastholder sit ønske om, at teleselskaberne skal fortsætte logningen?”

Svar:

Der henvises til den samtidige besvarelse af spørgsmål nr. 562 (Alm. del) fra Folketingets Retsudvalg.

Retsudvalget 2020-21
REU Alm.del - endeligt svar på spørgsmål 566
Offentligt

Bilag AC

Kammeradvokaten

JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 17. februar 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2021-0030-5506
Dok.: 1810818

Besvarelse af spørgsmål nr. 566 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 566 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 21. januar 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Louise Mariegaard

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 566 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren i forlængelse af samrådet den 14. januar 2021 om logningsbekendtgørelsen oplyse, hvorvidt de eksempler om bomben ved Skattestyrelsen og drabet på forfatteren Nedim Yasar, som ministeren fremhævede under samrådet som sager, hvor logning havde bidraget til efterforskningen, kunne have været efterforsket og opklaret ved hjælp af den såkaldte hastesikringsmulighed som EU-retten tillader ved alvorlig kriminalitet, og hvor politiet har mulighed for at stoppe sletning af trafikdata i et givent tidsrum?"

Svar:

Som oplyst på samrådet den 14. januar 2021 er der på baggrund af dommen af 6. oktober 2020 i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C520/18, Ordre des barreaux francophones et germanophone m.fl., behov for at ændre i de gældende danske logningsregler. Bl.a. er det Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter dommen af 6. oktober 2020 ikke vil kunne begrundes af hensyn til bekæmpelsen af *almindelig kriminalitet*.

Politiet vil altså efter en revidering af logningsreglerne i Danmark miste adgang til potentielt vigtige loggede oplysninger i en lang række sager, herunder i sager om almindelig kriminalitet, hvor loggede oplysninger i dag spiller en helt central rolle.

Det følger af dommens præmis 160ff, at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. en hurtig lagring af de trafik- og lokaliseringsdata, som de råder over, f.eks. som led i lovlig forretningspraksis eller lignende eller som følge af en retlig forpligtelse. De trafikdata og lokaliseringsdata, som behandles og lagres af teleudbyderne, skal principielt slettes eller gøres anonyme efter udløbet af de lovbestemte frister, der er fastsat i overensstemmelse med gennemførelsen af e-data-beskyttelsesdirektivet[1]. Der kan imidlertid opstå situationer, hvori det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed.

[1]Direktiv 2002/58/EF1.

Der kan således i visse situationer i et udvidet omfang ske hurtig lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået eller planlagt, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds.

En sådan hurtig lagring kan udelukkende ske for at efterforske eller beskytte mod *grov kriminalitet* og handlinger, der kan skade den *nationale sikkerhed*, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske.

Justitsministeriet er ved at studere dommen nærmere, herunder hvilken betydning de nævnte præmisser har for bestemmelsen i retsplejelovens § 786 a, hvorefter politiet kan pålægge udbydere af telenet eller teletjenester at foretage hastesikring af elektroniske data, herunder trafikdata, der skønnes nødvendig for efterforskningen. Dette vil indgå i den kommende revision af logningsreglerne mv.

Når jeg på samrådet den 14. januar 2021 nævnte de to sager om sprængningen ved Skattestyrelsen og drabet på Nedim Yasar, var det for at illustrere den værdi, loggede oplysninger har haft for efterforskningen i to konkrete sager.

Det er imidlertid ikke på det foreliggende grundlag muligt at konkludere, om de to sager ville kunne have været opklaret ved de muligheder for hurtig lagring, som EU-Domstolen angiver i præmisserne 160ff i sin dom af 6. oktober 2020.

JUSTITSMINISTERIET

Dato: 23. marts 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-187-0036
Dok.: 1899781

Skitse for revision af logningsreglerne mv.

1. Indledning

Det er af afgørende betydning for regeringen at sikre, at politiet og Politiets Efterretningstjeneste har de efterforskningsredskaber, der skal til for at kunne bekæmpe kriminalitet og sikre borgernes tryghed, og for at anklagemyndigheden kan strafforfølge tiltalte ved domstolene.

Det har i årevis været centralt for politiets efterforskning at kunne indhente loggede oplysninger om teletrafik. I større straffesager om alvorlig kriminalitet indgår dette redskab ofte i politiets efterforskning. Det gælder bl.a. i sager om bandekriminalitet, drab, narkotikakriminalitet og terrorisme, hvor politiet bl.a. kan bruge loggede oplysninger til at se, hvor en potentiel gerningsmand har befundet sig på et givent tidspunkt eller som baggrund for at indhente yderligere kendelser eller indlede internationalt samarbejde.

EU-Domstolen har den 6. oktober 2020 afsagt dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen medfører, at der er behov for at ændre i de gældende danske regler om registrering og opbevaring af oplysninger om teletrafik (logning[1]). Samtidig skal det vurderes, i hvilket omfang dommen giver anledning til at ændre reglerne om adgang til loggede oplysninger i retsplejelovens bestemmelser om edition og indgreb i meddelelseshemmeligheden.

Den teknologiske udvikling gør det endvidere nødvendigt at opdatere politiets efterforskningsredskaber, så reglerne i større omfang tager højde for, at brugernes kommunikation i stigende grad går fra traditionel telebaseret kommunikation (som er omfattet af den nuværende logningsforpligtelse) til internetbaseret kommunikation (som i det væsentligste ikke er omfattet af den nuværende logningsforpligtelse).

I lyset af at politiets anvendelsesmuligheder for loggede teleoplysninger i fremtiden bliver meget begrænset, er der behov for, at de få tilbageværende redskaber bliver så effektive som muligt. Med henblik på at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse, har Justitsministeriet således fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til nærmere overvejelse. Dette er begrundet i hensynet til at minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede

[1] Ordene "logning" og "lagring" anvendes som synonymer i skitsen.

taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle mv.

I det følgende præsenteres Justitsministeriets foreløbige og overordnede overvejelser vedrørende den kommende revision af logningsreglerne mv. Skitsen er tænkt som et oplæg til de videre drøftelser med Folketinget, interessenter og telebranchen med henblik på, at regeringen til oktober 2021 vil fremsætte et lovforslag om revision af logningsreglerne mv.

Indledningsvist redegøres der for EU-Domstolens praksis vedrørende medlemsstaternes logningsregler (afsnit 2). Herefter præsenteres Justitsministeriets overvejelser vedrørende logning med henblik på beskyttelse af den nationale sikkerhed (afsnit 3), logning med henblik på bekæmpelse af grov kriminalitet mv. (afsnit 4), hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed (afsnit 5), udlevering af basale oplysninger, krav om registrering af taletidskort og logning af oplysninger om civil identitet (afsnit 6) samt adgang til loggede oplysninger (afsnit 7). I afsnit 8 redegøres der for Justitsministeriets umiddelbare overvejelser for perioden, indtil et nyt regelsæt træder i kraft, og endelig sammenfattes overvejelserne under afsnit 9.

2. EU-Domstolens praksis vedrørende medlemsstaters logningsregler

EU-Domstolen har afsagt flere domme, der angår medlemsstaternes logningsregler mv. I det følgende redegøres der for Digital Rights-sagen (dom af 8. april 2014), Tele2-sagen (dom af 21. december 2016), Ministerio Fiscal-sagen (dom af 2. oktober 2018), La Quadrature du Net-sagen (dom af 6. oktober 2020) og H.K.-sagen (dom af 2. marts 2021).

2.1. Dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (Digital Rights-sagen)

Ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights, erklærede EU-Domstolen direktiv 2006/24/EF (logningsdirektivet) for ugyldigt.

I dommen udtaler Domstolen, at logningsdirektivet ikke fastsætter et objektivt kriterium, der gør det muligt at afgrænse myndighedernes adgang til lagrede data og den efterfølgende anvendelse af disse med henblik på fore-

byggelse, afsløring eller strafferetlig retsforfølgning vedrørende kriminalitet, der kan anses for tilstrækkeligt grov til at begrunde et sådant indgreb – henset til rækkevidden og alvoren af indgrebet i rettighederne, der er beskyttet i artikel 7 om respekt for privatliv og artikel 8 om beskyttelse af personoplysninger i EU's Charter om Grundlæggende Rettigheder (herefter Chartret). I direktivets artikel 1, stk. 1, er der i stedet alene henvist til "grov kriminalitet" som defineret i national ret.

Domstolen udtaler videre, at logningsdirektivet ikke indeholder materielle og processuelle betingelser for myndighedernes adgang til dataene og den efterfølgende anvendelse heraf. Direktivet foreskriver således ikke udtrykkeligt, at denne adgang og efterfølgende anvendelse skal være strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger eller strafferetlig retsforfølgning heraf.

Domstolen bemærker herefter, at logningsdirektivet ikke fastsætter noget objektivt kriterium, der gør det muligt at begrænse antallet af personer, der er bemyndigede til at få adgang til og efterfølgende anvende lagrede data til det strengt nødvendige henset til formålet.

Domstolen udtaler endvidere, at myndighedernes adgang til lagrede data ikke med direktivet er undergivet en forudgående kontrol, der udøves enten af en retsinstans eller af en uafhængig administrativ enhed.

Endelig fastslår dommen, at logningsdirektivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre en effektiv beskyttelse mod risikoen for misbrug og mod enhver ulovlig adgang til og benyttelse af disse data, idet direktivet ikke indeholder regler, som er specifikke og tilpasset den meget store mængde data, til disse datas følsomme karakter samt til risikoen for ulovlig adgang til dataene. Der er således ikke med direktivet fastsat en klar og streng regulering af beskyttelsen og sikkerheden af dataene med henblik på at sikre deres integritet og fortrolighed, navnlig giver direktivet ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden, og der er ikke fastsat krav om, at dataene skal lagres inden for EU's område. I den forbindelse fastslår EU-Domstolen, at det heller ikke kan antages, at det fuldt ud er sikret, at overholdelse af kravene om beskyttelse og sikkerhed kontrolleres af en uafhængig myndighed.

2.2. Dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15 (Tele2-sagen)

EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2, har sit afsæt i dels de svenske logningsregler, dels de britiske regler for myndigheders adgang til kommunikationsdata, og omhandler fortolkningen af direktiv 2002/58 (herefter e-databeskyttelsesdirektivet) sammenholdt med Chartrets artikel 7, 8 og 11 (om respekt for privat- og familieliv, beskyttelse af personoplysninger og ytrings- og informationsfrihed).

E-databeskyttelsesdirektivet indeholder regler om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor. Det fremgår af e-databeskyttelsesdirektivet artikel 15, stk. 1, at det er muligt for medlemsstaterne under iagttagelse af de i direktivet fastsatte betingelser at vedtage "retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i [direktivets] artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9". Dette omfatter bl.a. retsforskrifter, der pålægger udbyderne af elektroniske kommunikationstjenester at lagre trafik- og lokaliseringsdata.

I dommen udtaler EU-Domstolen sig om *logningsforpligtelsen for teleudbyderne*. Den anfører indledningsvist, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere, er et meget vidtrækkende og særligt alvorligt indgreb i de grundlæggende rettigheder som fastslået i Chartrets artikel 7 og 8. Domstolen bemærker hertil, at lagringen af trafik- og lokaliseringsdata kan have en indvirkning på brugen af de elektroniske kommunikationsmidler, og følgelig på brugernes udøvelse af deres ytringsfrihed, som er sikret ved Chartrets artikel 11.

Domstolen udtaler herefter, at henset til alvoren af indgrebet i de grundlæggende rettigheder er det alene bekæmpelse af grov kriminalitet, som kan begrunde en sådan foranstaltning. Desuden bemærker Domstolen, at selv om effektiviteten af bekæmpelsen af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker, kan et sådant mål af almen interesse, hvor grundlæggende det end er, ikke i sig selv begrunde, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata, anses for nødvendig.

En national lovgivning, der forskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata bevirker, at lagringen af trafik- og lokaliseringsdata er hovedreglen, hvorimod e-databeskyttelsesdirektivet opstiller et krav om, at denne lagring af data skal være undtagelsen.

Domstolen udtaler herefter, at en lovgivning, der omfatter alle abonnenter og registrerede brugere generelt, og som er rettet mod alle elektroniske kommunikationsmidler og samtlige trafikdata, ikke foreskriver nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål. Den omfatter generelt alle personer, der gør brug af elektroniske kommunikationstjenester, uden at disse personer – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning. Den finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til grove straffelovsovertrædelser. Endvidere indeholder den ikke nogen undtagelsesbestemmelse, således at den tilmed finder anvendelse på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt.

Domstolen udtaler videre, at det for en sådan lovgivning gælder, at den ikke kræver nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel mod den offentlige sikkerhed. Den er navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af kriminalitet.

Domstolen konkluderer herefter, at en sådan lovgivning overskrider det strengt nødvendige og ikke i et demokratisk samfund kan anses for at være begrundet, således som det er påkrævet i henhold til EU-retten.

Domstolen fastslår herefter, at artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet. Dette forudsat, at lagringen af disse data begrænses til det strengt nødvendige for

så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen.

En sådan national lovgivning skal *for det første* fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, så de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige.

Hvad *for det andet* angår de materielle betingelser som en sådan national lovgivning skal opfylde, bemærker Domstolen, at lagringen af trafik- og lokaliseringsdata altid skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds.

Hvad angår afgrænsningen af en sådan foranstaltning med hensyn til personkredsen og de potentielt omfattede situationer, skal den nationale lovgivning være baseret på objektive forhold. Disse skal gøre det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået.

I dommen udtaler EU-Domstolen sig derudover om de nærmere betingelser for myndighedernes *adgang* til de lagrede trafik- og lokaliseringsdata. Domstolen udtaler, at for at sikre at myndighedernes adgang til lagrede data begrænses til det strengt nødvendige, skal betingelserne for, hvornår udbyderne af elektroniske kommunikationstjenester skal give en sådan adgang til myndighederne, fastsættes i national ret. Den nationale lovgivning kan ikke begrænse sig til at opstille et krav om, at adgangen opfylder et af målene i artikel 15, stk. 1, i e-databeskyttelsesdirektivet, men skal også fast-

sætte de materielle og processuelle betingelser, der skal gælde for myndighedernes adgang til de lagrede data. Dette gælder også, når der er tale om, at formålet er bekæmpelse af grov kriminalitet.

Domstolen fastslår i den forbindelse i dommens præmis 119:

> ”119. For så vidt som en generel adgang til samtlige lagrede data – uafhængigt af, om der foreligger nogen forbindelse, selv indirekte, til det forfulgte mål – ikke kan anses for at være begrænset til det strengt nødvendige, skal den pågældende nationale lovgivning således være baseret på objektive kriterier med henblik på fastlæggelsen af de omstændigheder og betingelser, hvorunder de kompetente nationale myndigheder skal gives adgang til abonnenters eller registrerede brugeres data.”

Domstolen bemærker videre, at der i forbindelse med målet om bekæmpelse af kriminalitet i princippet kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan. I særlige situationer, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, kan der imidlertid også gives adgang til andre personers data, når der foreligger objektive forhold, som gør det muligt at antage, at disse data i en konkret sag kan bidrage effektivt til bekæmpelsen af en sådan virksomhed.

Domstolen bemærker herefter, at det er afgørende, at de nationale myndigheders adgang til lagrede data i princippet er undergivet en forudgående kontrol, der foretages enten af en domstol eller af en uafhængig administrativ enhed. Dette gælder dog ikke i behørigt begrundede hastende tilfælde. Domstolen eller enhedens afgørelse skal træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af myndighederne inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning.

Endelig udtaler Domstolen, at myndighederne, som har fået adgang til de lagrede data, så snart det ikke kan skade efterforskningen, skal underrette de berørte personer inden for rammerne af de gældende nationale procedurer. Det skyldes, at underretningen er nødvendig for at gøre det muligt for de berørte personer at bruge den adgang til retsmidler, som er fastsat i artikel 15, stk. 2, i e-databeskyttelsesdirektivet sammenholdt med artikel 22 i di-

rektiv 95/46 (dagældende persondatadirektiv, i dag erstattet af databeskyttelsesforordningen, forordning 2016/679), hvis deres rettigheder er blevet tilsidesat.

2.3. Dom af 2. oktober 2018 i sag C-207/16 (Ministerio Fiscal-sagen)

Dommen af 2. oktober 2018 i sag C-207/16, Ministerio Fiscal, vedrørte ligeledes fortolkningen af e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7 og 8. Sagen angik en situation, hvor den spanske anklagemyndighed havde fået afslag på at få adgang til de telefonnumre og SIM-kort, der var blevet aktiveret på en stjålen mobiltelefons identitetskode (et såkaldt IMEI-nummer), samt de tilknyttede personoplysninger, såsom navn og adresse. Spørgsmålet for Domstolen var, hvorvidt og i hvilket omfang det formål, som anmodningen forfulgte, var tilstrækkelig alvorligt til at begrunde offentlige myndigheders adgang til sådanne data (data med henblik på at identificere indehavere af SIM-kort, der er blevet aktiveret med en stjålet mobiltelefon, såsom efternavn, fornavn og eventuelt adresse).

Domstolen udtaler i den forbindelse, at det formål, der forfølges med en lovgivning, der regulerer en adgang til loggede oplysninger, skal stå i forhold til alvoren af det indgreb i de omhandlede grundlæggende rettigheder, som denne adgang indebærer. I overensstemmelse med proportionalitetsprincippet er et alvorligt indgreb således kun begrundet med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet. Når indgrebet ikke er alvorligt, kan det derimod begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt.

Domstolen bemærker i den forbindelse, at den adgang til data, der var omfattet af sagen, kun gjorde det muligt i en bestemt periode at sammenkæde det eller de SIM-kort, der var blevet aktiveret med den stjålne mobiltelefon, med indehaverne af disse SIM-korts identitet. Uden sammenholdning af data vedrørende den kommunikation, der var foretaget med de nævnte SIM-kort, med lokaliseringsdata, gjorde disse data det hverken muligt at kende datoen, tidspunktet, varigheden og modtagerne af den kommunikation, der var foretaget med det eller de omhandlede SIM-kort, eller de steder, hvor denne kommunikation havde fundet sted eller hyppigheden heraf med visse personer i en bestemt periode. De nævnte data gjorde det dermed ikke muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis

data er omhandlet. Under disse omstændigheder fandt Domstolen, at adgangen til de data alene ikke kan kvalificeres som et "alvorligt" indgreb i de grundlæggende rettigheder for de personer, hvis data er omhandlet.

Adgangen til data med henblik på at identificere indehavere af SIM-kort, der er blevet aktiveret med en stjålet mobiltelefon, såsom efternavn, fornavn og eventuelt adresse, kan derfor begrundes i formål om forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt, uden at det er nødvendigt, at disse forbrydelser kvalificeres som "alvorlige".

2.4. Dom af 6. oktober 2020 i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. (La Quadrature du Net-sagen)

EU-Domstolens dom af 6. oktober 2020 i de forenede sager forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl., vedrører foreneligheden af de franske og belgiske logningsregler med e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7 om respekt for privatlivet, artikel 8 om beskyttelse af personoplysninger og artikel 11 om ytringsfrihed.

I dommen gentager Domstolen udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for national lovgivning, der pålægger teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata med henblik på, at offentlige myndigheder kan få adgang til disse data. Domstolen anfører dog samtidig under hvilke betingelser, udgangspunktet kan fraviges, således at medlemsstaterne kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata.

Domstolen fastslår således for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at *beskytte den nationale sikkerhed* (præmis 134-139). I den forbindelse bemærker Domstolen, at artikel 4, stk. 2, i EU-Traktaten fastslår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, samt at formålet om beskyttelse af national sikkerhed vejer tungere end f.eks. formålet om bekæmpelse af kriminalitet, hvorfor formålet kan retfærdiggøre mere alvorlige indgreb i grundlæggende rettigheder.

Som følge heraf er EU-retten ikke til hinder for, at medlemsstaterne kan pålægge teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata for en begrænset tidsperiode, så længe der er tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig. Lagringen må dog kun ske i en afgrænset periode, der skal begrænses til det strengt nødvendige. Perioden kan forlænges, hvis den alvorlige trussel fortsætter, men EU-Domstolen understreger i den forbindelse, at lagring af data ikke må have en systematisk karakter. Endelig skal den generelle og udifferentierede lagring ledsages af mulighed for en efterfølgende effektiv prøvelse af bl.a., om der foreligger en sådan alvorlig trussel mod den nationale sikkerhed.

Dernæst fastslår Domstolen, at *grov kriminalitet* og *beskyttelse mod alvorlige trusler mod den offentlige sikkerhed* ikke kan retfærdiggøre en generel og udifferentieret lagring af trafik- og lokaliseringsdata (præmis 140-151).

Men Domstolen udelukker i den forbindelse ikke, at der med henblik på bl.a. at bekæmpe grov kriminalitet kan pålægges en målrettet lagringsforpligtelse af trafik- og lokaliseringsdata. Domstolen gentager her, hvad den tidligere sagde i bl.a. Tele2-dommen, hvorefter medlemsstaterne kan pålægge teleudbydere mv. en pligt til at lagre trafik- og lokaliseringsdata "vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af grov kriminalitet".

Domstolen bemærker – som noget nyt – at det kan være berettiget at logge målrettet i områder med høj hyppighed af grov kriminalitet samt steder, hvor der i særlig grad kan begås grov kriminalitet. Det kan f.eks. være steder eller infrastrukturer, som regelmæssigt har mange besøgende-. Endelig bemærker Domstolen, at det kan være berettiget at logge målrettet i strategiske områder, såsom lufthavne, banegårde og vejafgiftsområder.

Den målrettede lagring af disse data må kun lagres, så længe det er strengt nødvendigt i lyset af formålet og de omstændigheder, der retfærdiggør laggringen. Det vil dog være muligt at forlænge foranstaltningerne, hvis fortsat lagring er nødvendig.

Domstolen anfører videre – som noget nyt – at medlemsstaterne kan fastsætte national lovgivning, der muliggør *generel og udifferentieret lagring af IP-adresser* på kilden til kommunikationen (præmis 152-159). Dette må dog alene ske med henblik på at bekæmpe grov kriminalitet eller forhindre alvorlige trusler mod den nationale sikkerhed eller offentlige sikkerhed. Lagring af IP-adresserne må alene ske i en periode, der er begrænset til det strengt nødvendige, og myndighedernes adgang til IP-adresserne skal være nøje reguleret i lovgivningen.

Domstolen anfører endvidere i præmis 140, at det kun er indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, der ikke er alvorlige, som kan begrundes i formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

For så vidt angår *oplysninger om identiteten* på brugerne af elektroniske kommunikationsmidler fastslår Domstolen, at medlemsstaterne kan pålægge teleudbydere mv. at lagre data vedrørende personers identitet med henblik på at forhindre eller efterforske alle strafbare handlinger og beskytte mod trusler mod den offentlige sikkerhed.

Lagring af data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, kan principielt ikke kvalificeres som et alvorligt indgreb. Det skyldes, at disse data ikke i sig selv gør det muligt at få kendskab til datoen og tidspunktet for en kommunikation, varigheden og modtagerne af en kommunikation, de steder, hvorfra en kommunikation har fundet sted, eller oplysning om, hvor ofte en kommunikation har været foretaget med visse personer i en bestemt periode. Det indebærer, at disse data bortset fra de pågældendes kontaktoplysninger, såsom deres adresser, ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om disse personers privatliv (præmis 157).

I den forbindelse bemærker Domstolen, at der ikke er noget krav om, at kriminaliteten eller truslen er alvorlig. Krav om lagring af data om personers identitet er ikke underlagt nogen tidsbegrænsning.

Domstolen fastslår endelig, at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. *en hurtig lagring af trafik- og lokaliseringsdata, som de allerede råder over*, f.eks. som led i lovlig forretningspraksis eller lignende eller som følge af en retlig forpligtelse (præmis 160-165). De trafik- og lokaliseringsdata,

som behandles og lagres af teleudbyderne, skal principielt slettes eller gøres anonyme efter udløbet af de lovbestemte frister, der er fastsat i overensstemmelse med gennemførelsen af e-databeskyttelsesdirektivet. Der kan imidlertid opstå situationer, hvori det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed.

Der kan således i visse situationer i et udvidet omfang ske hurtig lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået eller planlagt, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds.

En sådan hurtig lagring kan udelukkende ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske.[2]

2.5. Dom af 2. marts 2021 i sag C-746/18 (H.K.-sagen)

EU-Domstolens dom af 2. marts 2021 i sag C-746/18 (H.K.-sagen) vedrører de estiske regler om adgang til loggede trafik- og lokaliseringsdata i forbindelse med en konkret straffesag, hvor en kvinde var blevet idømt en frihedsstraf på to år for bl.a. tyveri. I straffesagen indgik bl.a. trafik- og lokaliseringsdata, som anklagemyndigheden havde fået adgang til fra teleudbydere, idet teleudbyderne var underlagt en lovbestemt forpligtelse til i et år at foretage generel og udifferentieret lagring af sådanne data. Efter de estiske regler kunne anklagemyndigheden anmode om adgang til oplysningerne for enhver form for straffelovsovertrædelse. Spørgsmålet var bl.a., om adgangen til disse data var i strid med e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, idet adgangen ikke var begrænset til formålet om at bekæmpe grov kriminalitet.

EU-Domstolen anfører indledningsvist, at EU-retten er til hinder for lovgivningsmæssige foranstaltninger, der i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafik- og lokaliseringsdata. I overensstemmelse med proportionalitetsprincippet er det kun bekæmpelsen af grov

[2] Derudover forholdt Domstolen sig til en særlig fransk regel vedrørende mulighederne for at få kunne adgang til trafik- og lokaliseringsdata i realtid, jf. dommens pr. 183-189.

kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde de indgreb, som lagring af trafik- og lokaliseringsdata indebærer, uanset om der er tale om generel og udifferentieret lagring eller målrettet lagring (præmis 33). Derimod kan bekæmpelsen af kriminalitet i almindelighed godt begrunde mindre alvorlige indgreb, som for eksempel behandling af data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, idet disse data ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om brugernes privatliv (præmis 34).

Domstolen fastslår således, at det kun er bekæmpelsen af grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde offentlige myndigheders adgang til lagrede trafik- eller lokaliseringsdata. Andre faktorer vedrørende forholdsmæssigheden af en anmodning om adgang, såsom varigheden af den periode, for hvilken der er anmodet om adgang til de nævnte data, og mængden eller arten af de data, der er tilgængelige i en sådan periode, kan derimod ikke føre til, at formålet om bekæmpelse af kriminalitet i almindelighed kan begrunde en sådan adgang (præmis 39). Domstolen medgiver, at sådanne momenter indgår i vurderingen af, om en adgang i det konkrete tilfælde er begrænset til det strengt nødvendige, men det kan altså ikke medføre, at der kan gives adgang til sådanne oplysninger uden krav om, at adgangen har til formål at bekæmpe grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed.

Endelig anfører Domstolen, at der i princippet kun kan gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse. I særlige situationer, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, kan der imidlertid også gives adgang til andre personers data, når der foreligger objektive forhold, som gør det muligt at antage, at disse data i en konkret sag kan bidrage effektivt til bekæmpelsen af en sådan virksomhed (præmis 50). Adgangen til de lagrede data skal endvidere være undergivet en kontrol, der sker forudgående – eller i hastende tilfælde hurtigst muligt – og som foretages af enten en domstol eller en uafhængig administrativ enhed.

3. Logning med henblik på beskyttelse af den nationale sikkerhed

3.1. Gældende ret

3.1.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og klima, energi- og forsyningsministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Bestemmelsen blev foreslået med henblik på at styrke politiets efterforskningsmuligheder, jf. pkt. 1.2 i de almindelige bemærkninger i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 816. Formålet med bestemmelsen var at sikre tilstedeværelsen af de oplysninger, som politiet kan få adgang til ved blandt andet indgreb i meddelelseshemmeligheden i form at teleoplysning og udvidet teleoplysning. Forslaget berørte ikke de materielle og formelle betingelser for, at politiet kan foretage indgreb i meddelelseshemmeligheden herunder kravet om retskendelse.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at der alene er tale om registrering og opbevaring af trafikdata og ikke af selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom nedenfor under pkt. 3.1.2.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. nærmere herom nedenfor under pkt. 7.1. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at rettens kendelse opnås forud for udleveringen, ligesom teleudbyderen er forpligtet til at udlevere oplysninger i henhold til rettens kendelse.

Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786, stk. 4, for teleudbydere til at registrere både tele- og internetkommunikation til brug for efterforskning og retsforfølgning af strafbare forhold ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for logning med henblik på beskyttelse af den nationale sikkerhed.

3.1.2. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i deres net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i § 2, nr. 1, i lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer om elektroniske kommunikationsnet og -tjenester (teleloven). Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler, som en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Efter logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, skal en udbyder således bl.a. registrere oplysninger om tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

Efter logningsbekendtgørelsens § 6 skal udbyderne registrere en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser.

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

3.2. Relevante dele af La Quadrature du Net-dommen

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår logning med henblik på beskyttelse af den nationale sikkerhed er de relevante dele af dommen præmis 134-139. Det fremgår heraf navnlig,

- at der kan fastsættes nationale regler, der foreskriver generel og udifferentieret logning af trafik- og lokaliseringsdata vedrørende alle brugere i en begrænset periode, når der foreligger tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed,
- at dette gælder i situationer, hvor staten har en interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt

kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed,

- at truslen mod den nationale sikkerhed skal kunne anses for at være reel og aktuel eller forudsigelig,
- at lagringen tidsmæssigt skal begrænses til det strengt nødvendige, og at selv om en lagring kan forlænges som følge af, at en trussel fortsat består, må varigheden af hvert enkelt påbud ikke overstige et forudseeligt tidsrum,
- at en sådan lagring skal være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug,
- at lagringen således ikke må have en systematisk karakter, og
- at en afgørelse, hvorved der pålægges en sådan lagring, skal kunne gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ enhed med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

3.3. Justitsministeriets overvejelser og den foreslåede ordning

3.3.1. Alvorlig trussel mod national sikkerhed, der er reel og aktuel eller forudsigelig

Justitsministeriet har overvejet, hvad der kan udgøre et velunderbygget og tilstrækkeligt grundlag til at vurdere, om der er en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, således at der er basis for en generel og udifferentieret logning af trafik- og lokaliseringsdata[3] vedrørende alle brugere i en begrænset periode.

[3] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata".

Center for Terroranalyse (CTA)[4] udgiver i dag "Vurderingen af Terrortruslen mod Danmark". Vurderingen er CTA's samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet. Vurderingen, der i udgangspunktet udgives årligt, bygger på et stort antal underliggende analyser fra CTA, der strækker sig fra vurderinger af truslen mod konkrete personer, lokaliteter og begivenheder til bredere tendensanalyser og vurderinger af fænomener med betydning for terrortruslen mod Danmark og danske interesser i udlandet. Vurderingen er baseret på bl.a. efterretninger fra Politiets Efterretningstjenestes operationer, oplysninger fra internationale partnere, indberetninger fra myndigheder og privatpersoner samt offentligt tilgængeligt materiale.

Vurderingen af Terrortruslen mod Danmark indeholder en overordnet vurdering af terrortruslen mod Danmark fra bl.a. militant islamisme, højreekstremisme og venstreekstremisme. Inden for hver af disse kategorier vurderes terrortruslen mod Danmark. Som led heri vurderes det bl.a., om det er sandsynligt, at en eller flere aktører har kapacitet og/eller intention om at begå et terrorangreb, og om planlægning af et terrorangreb i det kommende år er sandsynlig. Endvidere vurderes det mest sandsynlige terrorangreb og de mest sandsynlige mål.

CTA anvender trusselsniveauer og sandsynlighedsgrader for at sikre analytisk stringens og give offentligheden et redskab til at sammenligne og forstå, hvordan forskellige trusler udvikler sig over tid. Skalaen for terrortrusselsniveauer og niveauernes definitioner fremgår af figur 1 herunder.

[4] CTA er opbygget som et fusionscenter, der består af medarbejdere fra Forsvarets Efterretningstjeneste (FE), Politiets Efterretningstjeneste (PET), Udenrigsministeriet, Beredskabsstyrelsen og Rigspolitiets Nationale Efterforskningscenter. CTA-konstruktionen medvirker til at sikre hurtig og effektiv koordination samt udveksling af information mellem relevante danske myndigheder med henblik på at imødegå eventuelle trusler på et så tidligt tidspunkt som muligt. Arbejdet bidrager bl.a. til dimensioneringen af det nationale beredskab på terrorområdet.

Figur 1: Terrortrusselsniveauer og deres definitioner	
Terrortrusselsniveau	**Definition**
Meget alvorlig	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse.
Alvorlig	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.
Generel	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.
Begrænset	Der er en potentiel trussel. Der er begrænset kapacitet og/eller hensigt.
Ingen	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

Seneste Vurdering af Terrortruslen mod Danmark blev udgivet den 20. marts 2020. Det fremgår heraf, at CTA vurderer, at terrortruslen mod Danmark er alvorlig. Det fremgår også af tidligere vurderinger af terrortruslen, at CTA har vurderet, at truslen mod Danmark er alvorlig, jf. CTA's vurderinger i årene fra 2014-2020.[5] Siden 2014 har CTA brugt terrortrusselsniveauerne og definitionerne gengivet ovenfor i figur 1, herunder begrebet "alvorlig", som en indikation på et specifikt defineret trusselsniveau.[6]

Terrortruslen mod Danmark og danske interesser i udlandet udgik ved oprettelsen af CTA i 2007 primært fra militante islamister, der var motiveret af Danmarks aktive udenrigs- og sikkerhedspolitik, herunder engagementet i Irak og Afghanistan. Danmark blev betragtet som et legitimt, men ikke prioriteret terrormål.

Terrortruslen mod Danmark har således ikke altid været på trusselniveauet "alvorlig".

Det generelle trusselsbillede, der påvirker terrortrusselsniveauet for Danmark, er dynamisk og komplekst, hvilket blandt andet kan ses ved markante

[5] Vurdering af Terrortruslen mod Danmark af 20. marts 2020, Vurdering af Terrortruslen mod Danmark af 12. januar 2018, Vurdering af Terrortruslen mod Danmark af 7. februar 2017, Vurdering af Terrortruslen mod Danmark af 28. april 2016, Vurdering af Terrortruslen mod Danmark af 18. marts 2015, Vurdering af Terrortruslen mod Danmark af 12. december 2014 og 24. januar 2014.

[6] Før 2014 var CTA's vurdering af Terrortruslen mod Danmark en mere beskrivende gengivelse af trusselsbilledet. Vurderingen var ikke niveauinddelt, og indeholdt således ikke en konklusion på det samlede niveau for terrortruslen. Af samme årsag kan brugen af begreberne "generel" og "alvorlig", der har været anvendt i Vurderingen af Terrortruslen før 2014, ikke i sig selv anvendes til at konkludere, om trusselsniveauet har haft et niveau, der er sammenligneligt med niveauinddelingen i figur 1.

udsving i antal gennemførte og afværgede angreb mod lande i Vesten. Fastsættelse af et terrortrusselsniveau er således et udtryk for en samlet vurdering baseret på konkrete hændelser og tilgængelige oplysninger.

Udviklingen i terrortrusselsniveauet i Danmark har over en årrække især været præget af konflikter i udlandet, herunder i Syrien og Irak, og sager om opfattede krænkelser af islam. Disse forhold har i de seneste år medvirket til at skærpe terrortruslen mod Danmark og danske interesser i udlandet.

Der er også løbende faktorer i trusselsbilledet i Danmark eller udlandet, herunder terrorgruppers intention og kapacitet der kan tiltage eller aftage, som kan have effekt på det generelle trusselsbillede, således at terrortruslen i Danmark også kan skærpes eller reduceres. Dette vil som nævnt bero på en samlet vurdering af relevante forhold og tilgængelige oplysninger.

Det er Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark bygger på tilstrækkeligt konkrete omstændigheder, herunder konkrete efterforskninger og straffesager i Danmark, der gør det muligt at vurdere og sandsynliggøre, om der er en alvorlig trussel mod den nationale sikkerhed, hvor f.eks. aktiviteter alvorligt kan destabilisere Danmarks grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed. Endvidere er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark ud fra dens analytiske kvalitet, systematik og metodik kan sandsynliggøre, at en sådan trussel er reel og aktuel eller forudsigelig.

Endelig er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark er tilstrækkelig dynamisk i karakter til, at logningen ikke herved vil få en systematisk karakter. Der henvises til, at der tidligere har været perioder, hvor truslen mod Danmark har været vurderet anderledes af nationale myndigheder, samt at vurderingen efter Justitsministeriets opfattelse har en kvalitet, systematik og metodik, der sandsynliggør det valgte trusselsniveau, uanset at vurderingen i en årrække har været på samme niveau.

Ud over Vurderingen af Terrortruslen mod Danmark, kan også en række andre analyseprodukter udgivet af enten Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center For Cybersikkerhed, belyse en trussel mod Danmarks sikkerhed inden for et specifikt område. Det kunne

f.eks. være Center For Cybersikkerheds årlige "Trusselsvurdering 2020: Cybertruslen mod Danmark", men også andre relevante trusselsvurderinger vil kunne indgå.

Disse analyser vil kunne indgå i en samlet vurdering af truslen mod Danmark, der vil kunne foretages regelmæssigt, så det sikres, at både nationale og internationale forhold af betydning for Danmarks nationale sikkerhed inddrages. Inddragelsen af flere af hinanden uafhængige analyseprodukter vil kunne styrke det vurderingsmæssige grundlag af det samlede trusselsbillede.

Det er således Justitsministeriets vurdering, at der bl.a. på baggrund af Vurderingen af Terrortruslen mod Danmark og øvrige analyseprodukter, kan foretages en velunderbygget vurdering af truslen mod Danmarks nationale sikkerhed med henblik på at konstatere, om der er tilstrækkelige solide grunde til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

Det foreslås på den baggrund, at der indføres en ordning, hvorefter justitsministeren, såfremt der foreligger en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, kan fastsætte en forpligtelse for teleudbydere mv. til at foretage logning af teleoplysninger mv.

Forpligtelsen vil gælde generelt og udifferentieret. Forpligtelsen vil være tidsmæssigt afgrænset, jf. nærmere nedenfor. Det forventes, at Vurderingen af Terrortruslen mod Danmark kan indgå som et hovedmoment i en samlet vurdering, hvor også andre analyseprodukter udgivet af Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed kan indgå.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master,

mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra "ikke-aktiv" kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

3.3.2. Tidsmæssig udstrækning

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen tidsmæssigt begrænses til det strengt nødvendige, og at varigheden af hvert enkelt påbud ikke overstiger et forudseeligt tidsrum, således at logningen ikke får en systematisk karakter.

De sager, der er omfattet af straffelovens kapitel 12 om forbrydelser vedrørende landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed og kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv., herunder efterforskningen af sådanne sager, har ofte en kompleksitet og et tidsmæssigt perspektiv, der kan strække sig over lang tid.

Det foreslås på den baggrund, at der indføres en ordning, hvorefter justitsministeren kan fastsætte en forpligtelse for teleudbydere mv. til i op til 1 år

at foretage logning af teleoplysninger mv. af hensyn til beskyttelse mod en alvorlig trussel mod den nationale sikkerhed.

En sådan tidsmæssig udstrækning vurderes at være proportionel under hensyn til sagernes alvorlige karakter og kompleksiteten af sagerne, herunder nødvendigheden af bagudrettet at kunne afdække miljøer og netværk, der er kendetegnet ved en meget høj grad af sikkerhedsbevidsthed. Den tidsmæssige udstrækning skal begrænses til det strengt nødvendige, og udstrækningen kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt. Endvidere vil begrænsningen sikre, at varigheden af hvert enkelt påbud ikke overstiger et forudseeligt tidsrum.

3.3.3. Retsgarantier og domstolsprøvelse mv.

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen er underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug, og hvordan afgørelsen, hvorved der pålægges en sådan logningsforpligtelse, kan gøres til genstand for en effektiv prøvelse.

Det er Justitsministeriets umiddelbare opfattelse, at de nuværende regler om teleudbydernes behandling af loggede oplysninger, herunder de sektorspecifikke databeskyttelsesregler, samt krav om sikkerhedsgodkendelse mv. kan videreføres, og at disse regler effektivt beskytter mod risikoen for misbrug.[7]

Som nævnt ovenfor, forventes Vurderingen af Terrortruslen mod Danmark samt andre uklassificerede efterretningsmæssige analyseprodukter at kunne udgøre grundlaget for vurderingen af, om der er en alvorlig trussel mod den nationale sikkerhed. Justitsministeriets vurdering kan gøres til genstand for en domstolsprøvelse af, om der foreligger en sådan situation, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

Det er Justitsministeriets opfattelse, at detaljeringsgraden i den uklassificerede udgave af Vurderingen af Terrortruslen mod Danmark udgør et tilstrækkeligt sikkert grundlag til, at der kan foretages en effektiv retlig prøvelse af Justitsministeriets vurdering af grundlaget for et pålæg om logning.

[7] Der kan bl.a. henvises til bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, herunder bekendtgørelsens §§ 10 og 11 om krav til udbydernes behandling af trafik- og lokaliseringsdata.

Ved domstolsprøvelsen er det alene Justitsministeriets vurdering, der kan efterprøves, da de efterretningsmæssige analyseprodukter i vidt omfang baserer sig på klassificeret materiale. Det kan i den forbindelse nævnes, at der vil være betydelige fordele forbundet med, at prøvelsen sker i en sædvanlig retsproces, hvor den fremlagte dokumentation – i det omfang det vurderes nødvendigt – evt. kan suppleres med vidneforklaringer fra ledende medarbejdere, der kan forklare om metodikken og tilblivelsesprocessen af de konkrete vurderinger mv.

Det er endvidere Justitsministeriets opfattelse, at der vil kunne fastsættes nærmere tekniske krav til udbydernes målrettede logning, herunder nærmere regler om opbevaringsformat, foranstaltninger med henblik på at sikre oplysningernes integritet og beskyttelse mod uautoriseret adgang, opbevaringssted mv. Det vil medvirke til at sikre, at der løbende kan ske den fornødne tilpasning i lyset af den teknologiske udvikling.

Det foreslås på den baggrund, at der med den foreslåede ordning sikres mulighed for, at der kan ske en efterfølgende prøvelse af den fastsatte forpligtelse ved domstolene af, om der foreligger en situation, hvor der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

3.3.4. Forpligtelser for teleudbyderne mv.

Justitsministeriet har overvejet, hvilke forpligtelser for teleudbyderne mv. den foreslåede logning vil medføre, udover selve logningsforpligtelsen.

Det foreslås, at i det omfang, der måtte blive fastsat regler om et fælles opbevaringsformat, og dette adskiller sig fra det af teleudbyderen anvendte, vil det påhvile udbyderen at foretage konvertering af den relevante data, herunder sikring af den fornødne dataintegritet og -kvalitet. Det følger af telelovens § 10, stk. 1, nr. 1, at det påhviler udbyderne uden udgift for staten at sikre, at deres tekniske systemer og tekniske udstyr er indrettet således, at politiet kan få adgang til oplysninger om bl.a. teletrafik. Det foreslås, at denne ordning videreføres. Udbyderne vil således være forpligtede til at indrette deres tekniske systemer og tekniske udstyr således, at de har kapaciteten til at understøtte de krav, som forslagene medfører.

4. Logning med henblik på bekæmpelse af grov kriminalitet mv.

4.1. Gældende ret

Der henvises til beskrivelsen ovenfor under pkt. 3.1 vedrørende retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786, stk. 4, for teleudbydere til at registrere både tele- og internetkommunikation til brug for efterforskning og retsforfølgning af alle typer strafbare forhold ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for logning med henblik på bekæmpelse af grov kriminalitet mv.

4.2. Relevante dele af La Quadrature du Net-dommen

De centrale dele af EU-Domstolens dom af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår målrettet logning er de relevante dele af dommen præmis 140-151. Det fremgår heraf navnlig,

- at der kan vedtages lovgivning, der som en forebyggende foranstaltning muliggør en målrettet logning af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt med henblik på beskyttelse af den nationale sikkerhed,
- at dette forudsætter, at en sådan logning begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal logges, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af logningen,
- at logningsforpligtelsen kan fastsættes på baggrund af objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafik- og lokaliseringsdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed eller endog en risiko for den nationale sikkerhed (personbestemt målrettet logning),
- at logningsforpligtelsen kan fastsættes på baggrund af et geografisk kriterium, når der på grundlag af objektive og ikke-diskriminerende forhold findes, at der i et eller flere geografiske områder er en forhøjet risiko for, at grov kriminalitet bliver planlagt eller begået, samt at disse områder navnlig kan være steder, der er kendetegnet ved et

højt antal tilfælde af grov kriminalitet, steder, hvor der i særlig grad kan begås grov kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder (geografisk målrettet logning), og

- at varigheden af sådanne foranstaltninger ikke må overstige, hvad der er strengt nødvendigt i forhold til det forfulgte formål og de omstændigheder, der begrunder dem, dog med forbehold af muligheden for at forlænge foranstaltningen som følge af, at det fortsat er nødvendigt at foretage en sådan lagring.

For så vidt angår logning af IP-adresser er de relevante dele af dommen præmis 152-156. Det fremgår heraf navnlig,

- at der kan fastsættes lovgivningsmæssige foranstaltninger, der foreskriver generel og udifferentieret logning af de IP-adresser, der er tildelt kilden til en forbindelse, såfremt det kan begrundes af hensyn til bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, i lighed med beskyttelsen af den nationale sikkerhed,
- at logningsperioden ikke må overstige, hvad der er strengt nødvendigt for at nå det forfulgte formål, og
- at en sådan foranstaltning skal indeholde strenge betingelser og garantier for så vidt angår brugen af disse data, bl.a. ved hjælp af sporing, med hensyn til de kommunikationer og de aktiviteter, som de berørte personer foretager online.

4.3. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan en ordning med logning med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed, kan indrettes. Når der i det følgende henvises til grov kriminalitet "mv.", dækker dette udtryk foruden grov kriminalitet også over alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed.

Det er i den forbindelse af central betydning, hvordan grov kriminalitet mv. defineres. Der henvises til pkt. 7.3.1 nedenfor.

Som det fremgår ovenfor, kan fastsættelse af en forpligtelse til logning med henblik på bekæmpelse af grov kriminalitet mv. ske ved en målrettet logning

(pkt. 4.3.1 og 4.3.2 nedenfor) og en generel og udifferentieret logning af IP-adresser (pkt. 4.3.3 nedenfor).

4.3.1. Personbestemt målrettet logning

Justitsministeriet har overvejet, hvordan en logningsforpligtelse fremadrettet kan målrettes bestemte persongrupper med henblik på bekæmpelse af grov kriminalitet mv.

Efter Justitsministeriets opfattelse har EU-Domstolen fastsat en forholdsvis lav tærskel – jf. anvendelsen af begrebet *"kan afsløre en forbindelse"* – for kravet til, hvor underbygget grundlaget skal være for beslutningen om, at en given person skal være omfattet af et pålæg om personbestemt målrettet logning.

Det er på denne baggrund Justitsministeriets vurdering, at personer kan være omfattet af et pålæg om personbestemt målrettet logning, når myndighederne finder, at visse objektive forhold tilsiger, at trafik- og lokaliseringsdata[8] om den pågældende – direkte eller indirekte – på et senere tidspunkt *kan* tjene til at afsløre en forbindelse til grov kriminalitet mv. Justitsministeriet tillægger det i den forbindelse vægt, at et sådant pålæg alene indebærer, at de pågældende oplysninger opbevares af de berørte teleudbydere i en nærmere fastsat og tidsbegrænset periode. Udlevering af oplysningerne til retshåndhævende myndigheder til brug for efterforskningen mv. af en konkret straffesag vil alene kunne ske, når en domstol konkret vurderer, at retsplejelovens krav er opfyldt, jf. beskrivelsen nedenfor under afsnit 7.

Det foreslås på den baggrund, at en afgrænsning af personkredsen omfattet af et pålæg om personel målrettet logning af hensyn til bekæmpelsen af grov kriminalitet mv. kan indeholde følgende kategorier af personer:

[8] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata".

- Personer der inden for en nærmere bestemt årrække er dømt for grov kriminalitet mv., idet personer, der er dømt for sådan kriminalitet bl.a. må antages at have en forhøjet tendens til at pleje omgang og relationer med personer tilknyttet miljøer, hvor der begås sådan kriminalitet.
- Personer der tidligere har været genstand for indgreb efter retsplejelovens kapitel 71 med henblik på bekæmpelse af grov kriminalitet mv., idet der for at foretage sådanne indgreb stilles særlige krav til navnlig mistankegrundlaget. Således vil det ved en retskendelse være konstateret, at der er grundlag for en mistanke, hvilket efter Justitsministeriets opfattelse kan betegnes som objektive forhold, der kan begrunde, at en person omfattes at et pålæg om personbestemt målrettet logning.
- Personer der tidligere har været i kontakt med personer, som har været aflyttet med henblik på bekæmpelse af grov kriminalitet mv., idet der i givet fald er en indirekte tilknytning til grov kriminalitet mv., der kan bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde, ligesom der må antages at være en vis forhøjet tendens til, at personer, der for nylig har haft kontakt til en aflyttet person, selv er involveret i grov kriminalitet mv., hvilket ofte er tilfældet i efterforskning af alvorlig organiseret kriminalitet, herunder menneskesmugling, handel med euforiserende stoffer samt rocker- og bandekriminalitet.
- Personer som retshåndhævende myndigheder har en konkret formodning om har forbindelse til grov kriminalitet mv., uden at der har været tilstrækkeligt grundlag for at iværksætte indgreb i meddelelseshemmeligheden eller domfælde pågældende. Dette kan f.eks. være personer, som Politiets Efterretningstjeneste behandler oplysninger om, mistænkte inden for områder, der er undergivet systematisk, politimæssig monitering, eksempelvis rocker- og bandemiljøer, personer, der indgår i militant islamistiske grupper, randpersoner fra rocker-/bandemiljøet, personer med kontakt til menneskesmuglere eller andre organiserede kriminelle, herunder nære relationer, som f.eks. ægtefæller eller samlevere til personer, der er genstand for målrettet personel logning eller en konkret efterforskning af grov kriminalitet mv. En sådan kategori indebærer et lavere krav til mistanken mod den enkelte end det, der f.eks. skal opfyldes for at retten kan tillade politiet at foretage aflytning efter retsplejelovens § 780, stk. 1, nr. 1, som er et mere vidtgående indgreb.

Det foreslås på den baggrund, at der indføres en hjemmel til, at politiet kan pålægge teleudbydere mv. personbestemt målrettet logning.

Efterforskningen af sager om grov kriminalitet, der ofte kan have en international dimension, vil ofte strække sig over længere perioder, ligesom grove kriminelle handlinger eller forberedelseshandlinger dertil ofte også vil strække sig over længere perioder. Det opleves endvidere, at når større sager om grov kriminalitet efterforskes over længere tid, vil efterforskningen mange gange kaste lys over ældre forhold, hvor det viser sig, at der er brug for oplysninger længere tilbage i tid. Der henvises endvidere til oven for under afsnit 3.3.2 vedrørende alvorlige trusler mod den nationale sikkerhed.

Det foreslås på den baggrund, at oplysninger, der logges på baggrund af en personbestemt eller geografisk afgrænset logning, skal opbevares i op til 1 år. Det foreslås endvidere, at tidsrummet for pålægget om registrering og opbevaring af oplysninger skal være så kort som muligt og højst kan fastsættes for 1 år ad gangen. Den tidsmæssige udstrækning kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt, så logningen begrænses til det strengt nødvendige.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra ”ikke-aktiv” kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet

(IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

Der foreslås endvidere, at der fastsættes nærmere regler om, hvordan det afgøres hvilke telefoner eller kommunikationsenheder, der konkret vil være omfattet af den personbestemte målrettede logning. Dette kan f.eks. indebære, at teleudbydere modtager CPR-numre på de personer, som er genstand for målrettet logning, hvorefter det vil påhvile udbyderne at foretage logning af de abonnementer og enheder, der er tilknyttet den pågældende person. En sådan indretning vil således imødegå, at målpersoner skifter telefoner eller abonnementer.

4.3.2. Geografisk målrettet logning

Justitsministeriet har endvidere overvejet, hvordan logningsforpligtelsen fremadrettet kan målrettes et eller flere geografiske områder med henblik på bekæmpelse af grov kriminalitet mv.

Det er Justitsministeriets opfattelse, at teleudbydere mv. vil kunne pålægges at etablere geografisk målrettet logning ud fra myndighedernes vurdering af – på grundlag af objektive og ikke-diskriminerende forhold – en forhøjet risiko for, at der planlægges eller begås alvorlig kriminalitet i et givent område.

Det vil for det første være muligt at pålægge etablering af målrettet logning på steder, der er kendetegnet ved et højt antal tilfælde af grov kriminalitet mv., f.eks. hvis politiet har konstateret, at der i et givent område – f.eks. en bydel – statistisk set oftere begås grov kriminalitet end andre steder. Der kan

også være tale om, at politiet konstaterer, at der ligger "rockerborge" eller hashklubber mv. i det pågældende område, eller at der aktuelt verserer en rocker/bande konflikt i området. Politiets vurdering af om et område bør omfattes af målrettet logning vil bl.a. kunne baseres på efterretninger og oplysninger fra politiets registre og sagsbehandlingssystemer (eksempelvis POLSAS), der indikerer en varig eller tiltagende tendens til, at grov kriminalitet planlægges eller fuldbyrdes i området.

For det andet vil det være muligt, at pålægge etablering af målrettet logning på steder, hvor der i særlig grad kan begås grov kriminalitet mv., såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer. Herudover kan der i et område også vurderes at være en forhøjet risiko for grov kriminalitet mv. i forbindelse med konkrete begivenheder – f.eks. sportsarrangementer, konferencer eller statsbesøg.

Endelig, og for det tredje, vil det være muligt, at pålægge etablering af målrettet logning på strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

Det vil kunne variere over tid hvor i landet, der er en forhøjet risiko for, at der planlægges eller begås grov kriminalitet mv. Logningen vil således skulle tilpasses løbende ud fra en vurdering af de aktuelle forhold.

Myndighederne – i praksis Rigspolitiet og Politiets Efterretningstjeneste – vil i den forbindelse have pligt til at dokumentere og underbygge grundlaget for den vurdering, der danner baggrund for at pålægge geografisk målrettet logning i et givet område, samt eventuelle efterfølgende revurderinger om, at logning skal opretholdes, således at behovet kan underbygges ved en eventuel efterfølgende domstolsprøvelse. Det bemærkes i den forbindelse, at der i visse områder vil kunne være behov for løbende forlængelser.

Det foreslås på den baggrund, at der indføres hjemmel til, at politiet for op til 1 år kan pålægge teleudbydere mv. målrettet logning for et nærmere afgrænset geografisk område, hvis der på baggrund af objektive og ikke-diskriminerende forhold er grund til at antage, at der er en forhøjet risiko for, at grov kriminalitet mv. bliver planlagt eller begået i området.

Efterforskningen af sager om grov kriminalitet, der ofte kan have en international dimension, vil ofte strække sig over længere perioder, ligesom grove kriminelle handlinger eller forberedelseshandlinger dertil ofte også

vil strække sig over længere perioder. Det opleves endvidere, at når større sager om grov kriminalitet efterforskes over længere tid, vil efterforskningen mange gange kaste lys over ældre forhold, hvor det viser sig, at der er brug for oplysninger længere tilbage i tid. Der henvises endvidere til oven for under afsnit 3.3.2 vedrørende alvorlige trusler mod den nationale sikkerhed.

Det foreslås på den baggrund, at oplysninger, der logges på baggrund af en personbestemt eller geografisk afgrænset logning skal opbevares i op til 1 år. Det foreslås endvidere, at tidsrummet for pålægget om registrering og opbevaring af oplysninger skal være så kort som muligt og kan højst fastsættes for 1 år ad gangen.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra "ikke-aktiv" kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

4.3.3. Generel og udifferentieret logning af IP-adresser

Justitsministeriet har endvidere overvejet, hvordan der kan fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser med henblik på bekæmpelse af grov kriminalitet mv.

Politiet har ofte behov for at kunne afdække, hvilke brugere, der benytter givne IP-adresser på givne tidspunkter, idet sådanne oplysninger er helt afgørende i forbindelse med efterforskningen af en lang række sager om grov kriminalitet mv. Dette gør sig særligt gældende i forhold til forbrydelser begået i den digitale verden, navnlig digitale sexkrænkelser og seksuelt misbrug af mindreårige, hvor det er en central del af politiets efterforskning at kunne bevise, hvem der har anvendt en IP-adresse på gerningstidspunktet. De seneste års stigning i forekomsten af grov kriminalitet begået gennem brug af internettet, f.eks. hacking, digitale sexkrænkelser og seksuelt misbrug af mindreårige mv., tilsiger generelt, at politiets behov for entydigt og effektivt at kunne fastlægge identiteten på en bruger af en given IP-adresse vil blive af stadig mere central betydning.

Det er Justitsministeriets overordnede vurdering, at de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, der foreskriver generel og udifferentieret logning af de tildelte brugeridentiteter (herunder IP-adresser), der er anvendt ved adgang til internettet, er i overensstemmelse med La Quadrature du Net-dommen.

Samtidig er det Justitsministeriets opfattelse, at det bl.a. på baggrund af den teknologiske udvikling er nødvendigt med en modernisering af de nugældende regler, samt at der er behov for en revision af de regler, der giver adgang til loggede IP-adresser. Det er således Justitsministeriets vurdering, at det af EU-Domstolen anførte i pr. 156 om, at der kan fastsættes nationale regler om generel og udifferentieret logning af IP-adresser, såfremt det kan begrundes af hensyn til bekæmpelsen af grov kriminalitet og forebyggelsen

af alvorlige trusler mod den offentlige sikkerhed, i lighed med beskyttelsen af den nationale sikkerhed, vil kunne sikres ved opstilling af materielle betingelser for politiets adgang til loggede oplysninger om IP-adresser. Der henvises til afsnit 7 for nærmere om adgang til loggede oplysninger.

Det er endvidere Justitsministeriets vurdering, at der foruden logning af selve den IP-adresse, der er anvendt ved adgangen til internettet, også vil kunne ske logning af de såkaldte portnumre (”source port number”), som teleudbydere mv. tildeler slutbrugerne for at identificere trafikken til og fra den enkelte slutbruger. Det skyldes, at der i dag anvendes teknologi, der gør det muligt for et større antal brugere at anvende den samme IP-adresse samtidig, hvorfor en IP-adresse således ikke alene kan tjene til at identificere den fysiske person, der ejer det udstyr gennem teleudbydere mv., hvorfra en kommunikation via internettet foretages. Portnummeret kan – i lighed med IP-adressen – ikke afsløre indholdet af, hvad der bliver kommunikeret om og hvem, der bliver kommunikeret med.

Endvidere vil der efter Justitsministeriets vurdering også kunne ske registrering af det tidspunkt, hvor en slutbruger har været tildelt en given IP-adresse. Det skyldes, at IP-adressen kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som en IP-adresse var tildelt på det tidspunkt, hvor en overtrædelse blev begået. En identifikation af slutbrugeren forudsætter således også registrering af de tidspunkter, hvor en slutbruger har været tildelt en given IP-adresse.

Det foreslås på den baggrund, at der for en periode på 1 år fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser for en brugers adgang til internettet (”kilde-IP-adressen”), logning af det portnummer, der er anvendt ved internetkommunikationen, samt registrering af tidspunktet for tildeling af kilde-IP-adressen og tilhørende portnummer.

Det bemærkes, at det er Justitsministeriets vurdering, at en opbevaringsperiode på 1 år kan anses for begrænset til det strengt nødvendige, idet den helt grundlæggende betydning som internettets udbredelse og anvendelse har for det danske samfund, generelt tilsiger, at politiet skal have mulighed for effektivt at efterforske grov kriminalitet mv. begået eller understøttet gennem brug af internettet i en længere periode. Det bemærkes i den forbindelse, at sager om alvorlig kriminalitet online ofte er komplekse og derfor tager lang tid at efterforske, bl.a. fordi der ofte er en international dimension som f. eks. seksuelt misbrug af børn. Endvidere kan der i sager om alvorlig

organiseret kriminalitet være behov for logning af kilde-IP-adresser i længere tid, idet disse sagstyper ofte involverer en større mængde kommunikationsenheder, som computere og mobiltelefoner, som skal beslaglægges og undersøges med henblik på udfindelse af IT-tekniske spor, såsom IP-adresser på bagmænd.

Det foreslås endvidere, at der kan fastsættes regler, der forpligter teleudbydere til at registrere oplysninger, der identificerer det abonnement, der er benyttet til internetadgangen, f.eks. telefonnummer, der identificerer det benyttede mobilabonnement ved internetadgang via mobildatatjenester, eller ID-nummer, f.eks. kredsløbsnummer, som identificerer det benyttede bredbåndsabonnement ved internetadgang via faste net. Ved afgrænsningen af hvilke oplysninger der kan registreres i tilknytning til en kilde-IP-adresse, tillægger Justitsministeriet det vægt, om de registrerede oplysninger gør det muligt for teleudbyderne over for politiet helt umiddelbart at foretage en entydig identifikation af den slutbruger, der på et givent tidspunkt har været tildelt kilde-IP-adressen til en forbindelse. Der vil ikke kunne fastsættes regler om registrering af oplysninger, der afslører, hvem der er kommunikeret med via kilde-IP-adressen, eller hvad der er kommunikeret om. Der henvises endvidere til EU-Domstolens praksis om identitetsoplysninger som redegjort for i pkt. 2.3 og 2.4.

4.3.4. Retsgarantier og domstolsprøvelse mv.

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen er underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug, og hvordan afgørelsen, hvorved der pålægges en målrettet logningsforpligtelse, kan gøres til genstand for en effektiv prøvelse.

Det er Justitsministeriets umiddelbare opfattelse, at de nuværende regler om teleudbydernes behandling af loggede oplysninger, herunder de sektorspecifikke databeskyttelsesregler, samt krav om sikkerhedsgodkendelse mv. kan videreføres, og at disse regler effektivt beskytter mod risikoen for misbrug.[9]

[9] Der kan bl.a. henvises til bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, herunder bekendtgørelsens §§ 10 og 11 om krav til udbydernes behandling af trafik- og lokaliseringsdata

Det er endvidere Justitsministeriets opfattelse, at der vil kunne fastsættes nærmere tekniske krav til udbydernes logning, herunder nærmere regler om opbevaringsformat, foranstaltninger med henblik på at sikre oplysningernes integritet og beskyttelse mod uautoriseret adgang, opbevaringssted mv. Det vil medvirke til at sikre, at der løbende kan ske den fornødne tilpasning i lyset af den teknologiske udvikling.

Der vil endvidere kunne fastsættes nærmere regler om fremgangsmåde mv. for udstedelse af pålæg til teleudbyderne om de personer, der er omfattet af et pålæg om målrettet personel logning.

Der vil også kunne fastsættes nærmere regler om, at oplysninger om f.eks., hvilke konkrete telefoner og kommunikationsenheder der er genstand for personbestemt målrettet logning, samt hvilke geografiske områder, der er omfattet af et pålæg om geografisk afgrænset logning, skal være fortrolige. Endvidere vil der kunne fastsættes regler om, at ansatte ved udbydere, der er underlagt en logningsforpligtelse, har tavshedspligt med hensyn til alle oplysninger modtaget som led i opfyldelsen af logningsforpligtelsen, og at straffelovens §§ 152 og 152 c-152 f finder tilsvarende anvendelse. En sådan regulering vil i øvrigt svare til den gældende tavshedspligt, der er fastsat i telelovens § 7, stk. 2, men vil omfatte enhver, der opnår kendskab til indholdet af et pålæg uanset om de er omfattet af telelovens regulering.

Forpligtelsen til at holde ovennævnte oplysninger fortrolige vil også kunne omfatte en forpligtelse til at sikre, at den enkelte bruger ikke, f.eks. gennem anmodninger om indsigt i egne oplysninger efter de databeskyttelsesretlige regler – eller på anden vis – kan tilegne sig oplysninger om, hvordan den geografiske og personbestemte målrettede logning på et givet tidspunkt er tilrettelagt.

Endelig vil der være mulighed for, at der kan ske en efterfølgende prøvelse ved domstolene ved politiets adgang til loggede oplysninger, hvor der i den forbindelse vil ske en prøvelse af, om proportionalitetskravet er opfyldt.

4.3.5. Forpligtelser for teleudbyderne mv.

Justitsministeriet har overvejet, hvilke forpligtelser for teleudbyderne mv. den foreslåede logning vil medføre, udover selve logningsforpligtelsen.

Det foreslås, at i det omfang, der måtte blive fastsat regler om et fælles opbevaringsformat, og dette adskiller sig fra det af teleudbyderen anvendte, vil det påhvile udbyderen at foretage konvertering af den relevante data, herunder sikring af den fornødne dataintegritet og -kvalitet. Det følger af telelovens § 10, stk. 1, nr. 1, at det påhviler udbyderne uden udgift for staten at sikre, at deres tekniske systemer og tekniske udstyr er indrettet således, at politiet kan få adgang til oplysninger om bl.a. teletrafik. Det foreslås, at denne ordning videreføres. Udbyderne vil således være forpligtede til at indrette deres tekniske systemer og tekniske udstyr således, at de har kapaciteten til at understøtte de krav, som forslagene medfører.

Det vil dog kunne fastsættes nærmere regler om økonomisk godtgørelse for udgifter forbundet med et konkret pålæg om personbestemt eller geografisk målrettet logning. De nærmere regler vil kunne omfatte regler om betingelserne for at yde godtgørelse for udgifter forbundet med et konkret pålæg mv., om standardtakster for godtgørelsen og eventuelt om betingelser for at yde godtgørelse ud over standardtaksterne. I det omfang sådanne regler fastsættes, forudsættes det, at der ikke ydes godtgørelse ud over standardtaksterne, medmindre der ekstraordinært måtte være tale om, at et konkret pålæg mv. medfører uforholdsmæssige udgifter for en udbyder.

Det bemærkes, at det forudsættes, at teleudbyderne ved udstedelse af pålæg om personbestemt eller geografisk målrettet logning kan have fuld klarhed over deres forpligtelser, således at de kan opfylde dem på den hurtigste og mest effektive måde.

Så snart adressaterne modtager og bliver gjort bekendt politiets pålæg, er disse underlagt en retlig handlepligt til at efterkomme pålægget.

Det følger i dag af telelovens § 10, stk. 4, at det påhviler udbyderen at sikre, at politiets anmodninger om fremskaffelse af oplysninger om teletrafik samt historisk teleoplysning og historisk udvidet teleoplysning behandles straks og på en sådan måde, at hensigten med indgrebet ikke forspildes.

Der vil for politiets pålæg om at påbegynde logning kunne fastsættes tilsvarende regler, der specificerer den ovenfor nævnte retlige handlepligt, og som forpligter teleudbyderne til at efterkomme pålægget straks efter modtagelse, således at formålet med pålægget ikke forspildes.

Det bemærkes, at det er Justitsministeriets vurdering, at det ikke vil udgøre en overtrædelse af de sektorspecifikke regler i bl.a. teleloven, hvis en teleudbyder, i overensstemmelse med et pålæg fra f.eks. Rigspolitiet, har foretaget logning, og pålægget senere f.eks. måtte blive underkendt ved en domstolsprøvelse. Ansvaret for at betingelserne for at påbegynde logning er opfyldt ligger således alene hos de myndigheder, der er kompetente til at pålægge logning, og der er ikke noget selvstændigt ansvar for, eller adgang til, at teleudbyderen vælger at foretage en retlig efterprøvelse af, om betingelserne konkret er opfyldt. Enhver efterprøvelse af et pålægs grundlag, udstrækning mv., ligger således i sidste ende hos domstolene. Teleudbyderne vil fra modtagelsen af pålægget være retligt forpligtet til straks at iværksætte logningen.

Foretager teleudbyderen behandling af en eller flere slutbrugeres personoplysninger i form af logning på baggrund af den retlige forpligtelse, et pålæg om logning indebærer, påhviler det samtidig alene teleudbyderen at kunne dokumentere, at et sådant pålæg er udstedt. Såfremt et pålæg konkret måtte give anledning hertil, f.eks. grundet dets omfang, er der imidlertid ikke noget til hinder for, at teleudbyderen søger pålæggets udstrækning bekræftet hos politiet. Politiets bekræftelse heraf vil i den forbindelse være tilstrækkelig dokumentation for, at teleudbyderen har sikret den fornødne dokumentation af grundlaget for den iværksatte logning.

5. Hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed

5.1. Gældende ret

Retsplejelovens § 786 a blev indsat ved § 2 i lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven. Bestemmelsen trådte i kraft den 1. juli 2004.

Retsplejelovens § 786 a blev indsat med henblik på at opfylde forpligtelserne til at fastsætte regler om hastesikring af elektronisk data efter artikel 16 og 17 i Europarådets konvention om IT-kriminalitet (CETS nr. 185), jf. pkt. 7.3 i de almindelige bemærkninger i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1812. Formålet med bestemmelsen var at sikre, at politiet kan udstede pålæg og sikring af elektroniske data med henblik på, at oplysningerne er tilstede og – hvis betingelserne herfor

er opfyldt – på et senere tidspunkt kan udleveres til politiet til brug for efterforskningen.

Efter retsplejelovens § 786 a, stk. 1, kan politiet som led i en efterforskning, hvor elektronisk bevismateriale kan være af betydning, meddele udbydere af telenet og teletjenester pålæg om at foretage hastesikring af elektroniske data, herunder trafikdata.

Det følger af retsplejelovens § 786 a, stk. 2, at et pålæg om hastesikring alene kan omfatte elektroniske data, som opbevares på det tidspunkt, hvor pålægget meddeles. I pålægget skal det anføres, hvilke data der skal sikres, og i hvilket tidsrum de skal sikres (sikringsperioden). Pålægget skal afgrænses til alene at omfatte de data, der skønnes nødvendige for efterforskningen, og sikringsperioden skal være så kort som mulig og kan ikke overstige 90 dage. Et pålæg kan ikke forlænges.

Det fremgår af forarbejderne til loven (bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827), at retsplejelovens § 786 a, stk. 1, omfatter alle elektroniske data - det vil sige både indholdsdata, trafikdata og øvrige elektroniske data, f.eks. oplysninger om navn og adresse på en internetudbyder eller et teleselskabs kunder (kundeoplysninger).

Det fremgår endvidere af forarbejderne til loven (bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827), at både udbydere af offentlige telenet og teletjenester samt udbydere, der henvender sig til specifikke, på forhånd afgrænsede kundesegmenter, er omfattet af bestemmelsen.

Efter retsplejelovens § 786 a, stk. 3, påhviler det udbydere af telenet og teletjenester som led i hastesikring efter retsplejelovens § 786 a, stk. 1, uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere, hvis net eller tjenester har været anvendt i forbindelse med den elektroniske kommunikation, som kan være af betydning for efterforskningen.

Retsplejelovens § 786 a, stk. 3, omfatter alene trafikdata. Oplysningerne, som udbydere af telenet og teletjenester skal videregive til politiet, er alene oplysninger om de elektroniske stier, som føres fra den pågældende udbyder

til en eller flere andre udbydere, jf. bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827.

Forsætlig eller uagtsom overtrædelse af pligten til at sikre elektroniske data og pligten til uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere kan straffes med bøde, jf. retsplejelovens § 786 a, stk. 4.

De nærmere betingelser for, hvornår teleudbydere skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. nærmere herom nedenfor under pkt. 7.1.

Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786 a for teleudbydere til at sikre elektroniske data og pligten til uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for hastesikring af data med henblik på bekæmpelse af grov kriminalitet eller beskyttelsen af den nationale sikkerhed.

5.2. Relevante dele af La Quadrature du Net-dommen

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår hastesikring af elektronisk data er de relevante dele af dommen præmis 160-165. Det fremgår heraf navnlig,

- at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. en hurtig lagring af trafik- og lokaliseringsdata, som de allerede råder over, f.eks. som led i lovlig forretningspraksis eller lignende eller som følge af en retlig forpligtelse,
- at de trafik- og lokaliseringsdata, som behandles og lagres af teleudbyderne, principielt skal slettes eller gøres anonyme efter udløbet af de lovbestemte frister, der er fastsat i overensstemmelse med gennemførelsen af e-databeskyttelsesdirektivet,
- at der kan opstå situationer, hvori det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed,

- at der således i visse situationer i et udvidet omfang kan ske hurtig lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået eller planlagt, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds,
- at en sådan hurtig lagring udelukkende kan ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske.

5.3. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan en ordning med hastesikring af trafik- og lokaliseringsdata[10] med henblik på bekæmpelse af grov kriminalitet samt beskyttelse af den nationale sikkerhed kan indrettes. Ved hastesikring forstås et indgreb, der pålægger udbyderne at sikre og opbevare trafik- og lokaliseringsdata, som de råder over, i en længere periode end det sædvanligvis er tilladt (”hurtig lagring” i La Quadrature du Net-dommen).

Det er Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter La Quadrature du Net-dommen ikke vil kunne begrundes af hensyn til bekæmpelsen af almindelig kriminalitet.

I lyset af Domstolens bemærkninger i dommens præmis 160ff er det Justitsministeriets opfattelse, at denne vurdering tillige gør sig gældende for regler, der tillader, at politiet i konkrete tilfælde kan pålægge udbydere af elektroniske kommunikationsnet- og tjenester at foretage en hastesikring af de trafik- og lokaliseringsdata, som de råder over. Det er således Justitsministeriets opfattelse, at politiets adgang til at pålægge hastesikring af trafik- og lokaliseringsdata, som udbyderne råder over, alene vil kunne anvendes, når

[10] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til ”lokaliseringsdata”. Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter ”lokaliseringsdata” forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet ”historiske masteoplysninger”. Når begrebet ”lokaliseringsdata” i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb ”signaleringsdata”.

det sker af hensyn til bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed.

Der er på den baggrund tillige behov for en ændring af de gældende regler i retsplejelovens § 786 a om hastesikring af elektronisk data, så der for trafik- og lokaliseringsdata indføres et kriminalitetskrav, der lever op til EU-Domstolens praksis. Det bemærkes, at § 786 a som nævnt ovenfor også omfatter indholdsdata og øvrige elektroniske data, som ikke umiddelbart er omfattet af dommen. Disse elementer vil blive nærmere overvejet.

Det er Justitsministeriets vurdering, at et pålæg om hastesikring af trafik- og lokaliseringsdata fremadrettet vil kunne ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. For Justitsministeriets overvejelser vedrørende den nærmere afgrænsning af grov kriminalitet henvises til nedenfor under pkt. 7.1.3.

Brugen af et pålæg om hastesikring kan overordnet tænkes anvendt i to forskellige scenarier.

For det første kan et pålæg tænkes anvendt i forhold til trafik- og lokaliseringsdata, der ikke er logningspligtige, men som udbyderen behandler som led i dets egen lovlige forretningspraksis, f. eks. data, der behandles til brug for fejlretning og debitering.

I sådanne tilfælde vil et pålæg om hastesikring indebære, at udbyderen skal opbevare data ud over de frister, der ellers måtte gælde for opbevaring til sådanne formål. Eksempelvis må udbyderne behandle og opbevare trafikdata til brug for debitering af abonnenter og afregning for samtrafik, indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger. I et sådant tilfælde vil et pålæg om hastesikring kunne anvendes til at opbevare data i en periode ud over denne frist.

For det andet kan et pålæg tænkes anvendt i forhold til trafik- og lokaliseringsdata, som udbyderne opbevarer som følge af en retlig forpligtelse, der er vedtaget i henhold til e-databeskyttelsesdirektivets artikel 15, stk. 1, f.eks. en logningsforpligtelse.

I sådanne tilfælde vil et pålæg om hastesikring indebære, at udbyderen skal opbevare data ud over de frister, der følger af logningsforpligtelsen. Er der eksempelvis grundlag for at udstede et pålæg om hastesikring af data, der tillige er genstand for målrettet geografisk logning, vil pålægget kunne anvendes til at forlænge den periode, som udbyderne ellers måtte være forpligtet til at opbevare den pågældende data i henhold til reglerne for målrettet geografisk logning.

Justitsministeriet har overvejet, hvilke betingelser der skal til for et pålæg om hastesikring. Det vil som nævnt være et krav, at et pålæg om hastesikring sker af hensyn til at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. Det er dog ikke et krav, at oplysningerne vedrører personer, der konkret er mistænkt for at have begået en grov strafbar handling eller et angreb mod den nationale sikkerhed, men oplysningerne skal kunne bidrage til opklaringen af en sådan handling eller angreb.

Ifølge La Quadrature du Net-dommen kan dette omfatte oplysninger om offeret for den strafbare handling eller angrebet, om den pågældendes sociale og arbejdsmæssige omgangskreds eller om bestemte geografiske områder, såsom de steder, hvor den omhandlede strafbare handling eller det omhandlede angreb mod den nationale sikkerhed blev begået eller planlagt.

Det forslås på den baggrund, at der indføres hjemmel til at udstede et pålæg om hastesikring af trafik- og lokaliseringsdata i følgende situationer, hvor en given handling er begået, planlagt eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske:

- Hvis der på et bestemt sted er blevet begået eller planlagt en grov kriminalitet eller et angreb mod den nationale sikkerhed. I den situation vil der kunne pålægges hastesikring af trafik- og lokaliseringsdata med tilknytning til området, f.eks. data fra de master, der dækker området.
- Hvis der på et bestemt sted er indikationer på, at et pålæg om hastesikring kan bidrage til efterforskningen af grov kriminalitet eller et angreb mod den nationale sikkerhed. Dette kan for eksempel være tilfældet, når der i efterforskningen foreligger indikationer på, at en

eller flere gerningsmænd i tiden umiddelbart op til eller efter gerningstidspunktet har passeret bestemte områder, og hvor oplysninger vedrørende disse steder kan bidrage til opklaringen.

- Hvis der ud fra en konkret vurdering er grundlag for et pålæg vedrørende en mistænkt person eller en person eller personkreds, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen. Dette vil bero på en politifaglig vurdering af den konkrete sags omstændigheder om hvilke personers data, der kan bidrage til efterforskningen. Disse personer og personkredse kan bl.a. omfatte offeret og den mistænktes sociale og arbejdsmæssige omgangskreds foruden den mistænkte selv.

Pålægget vil kunne anvendes både i de tilfælde, hvor politiet får kendskab til en grov strafbar handling umiddelbart efter gerningstidspunktet, men også i tilfælde, hvor politiet først får kendskab til handlingen en rum tid efter, at den blev begået. Råder udbyderne konkret over data, der kan bidrage til opklaringen af en grov strafbar handling mv., vil disse således også kunne omfattes af et pålæg om hastesikring, uanset hvor gamle de er.

Den udløsende faktor for, om data kan være genstand for et pålæg om hastesikring, er, at oplysningerne kan bidrage til opklaringen af grov kriminalitet eller et angreb mod den nationale sikkerhed. De pågældende trafik- og lokaliseringsdata skal med andre ord have efterforskningsmæssig værdi, hvilket er et parameter, det i første række tilkommer politiet at vurdere.

Det bemærkes i den forbindelse, at navnlig de indledende stadier af en efterforskning ofte er kendetegnet ved en meget bred indsamling af oplysninger, herunder om personer, der umiddelbart eller over tid viser sig ikke at have betydning for sagen.

Særligt for så vidt angår de pålæg om hastesikring af trafik- og lokaliseringsdata, der sker i nær tilknytning til en strafbars handlings gerningstidspunkt, kan der derfor efter Justitsministeriets opfattelse ikke stilles store krav til, i hvor høj grad disse efterfølgende kan antages at bidrage til opklaringen. Det tillægges i den forbindelse vægt, at et pålæg om hastesikring ikke giver politiet adgang til de pågældende oplysninger, men alene tjener det formål at sikre, at oplysningerne er til rådighed, når politiet opnår rettens som udgangspunkt forudgående godkendelse til, at der kan gives adgang hertil. Eksempelvis vil det forhold, at der på en given lokation er konstateret

en grov strafbar handling i sig selv være nok til, at der kan pålægges hastesikring af data med tilknytning til området.

For så vidt angår de processuelle betingelser for at pålægge hastesikring foreslås det, at politiet gives beføjelse til at vurdere og beslutte, hvilke trafik- og lokaliseringsdata, herunder for hvilken periode, der i den konkrete sag kan bidrage til opklaringen, og derefter udstede pålæg om hastesikring af disse til de relevante udbydere.

Politiet vil endvidere også indledningsvis skulle vurdere, om en hændelse konkret udgør en grov strafbar handling, og der må i den forbindelse indrømmes politiet en vis skønsmargin. Det kan f.eks. ikke afvises, at der vil være tilfælde, hvor det ikke øjeblikkeligt står klart, om der er tale om en grov strafbar handling eller et angreb på den nationale sikkerhed, f. eks. ved større ulykkestilfælde eller større uvarslede hændelser. Der vil således kunne udstedes pålæg, når politiet har rimelig grund til at mistænke, at der er begået en grov strafbar handling mv. For Justitsministeriets overvejelser vedrørende den nærmere afgrænsning af grov kriminalitet henvises til nedenfor under pkt. 7.1.3.

Det vil også kunne påhvile politiet at vurdere og beslutte et pålægs tidsmæssige udstrækning. Ved et pålægs tidsmæssige udstrækning forstås den periode, som udbyderne forpligtes til at opbevare den pågældende data i. Fælles for både den omhandlede data og opbevaringsperioden er, at politiet skal begrænse dette til det strengt nødvendige.

Der forudsættes ikke forudgående høring af adressaterne for pålægget, som endvidere vil være pligtige til at efterkomme pålægget straks efter modtagelse. Den udbyder, der mødes med et pålæg om hastesikring, vil kunne være forpligtet til at sikre integriteten af den data, som er genstand for pålægget, og pålægget vil gælde for dataen i udbyderens samlede net. Det foreslås, at dette indebærer, at der ikke må ske aggregering af dataen i forbindelse med sikringen og opbevaringen.

Endelig vil der kunne sikres mulighed for, at et pålæg om hastesikring på begæring kan indbringes for domstolene med henblik på at opnå rettens stillingtagen til, hvorvidt betingelserne for at pålægge hastesikring i den konkrete situation er opfyldt. Indbringelse for retten foreslås dog ikke at have opsættende virkning.

6. Udlevering af basale oplysninger, krav om registrering af taletidskort og logning af oplysninger om civil identitet

6.1. Gældende ret

6.1.1. Teleloven

Det følger af telelovens § 13, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere på begæring af politiet skal udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester.

Telelovens § 13 er en uændret videreførelse af den tidligere § 15 c i telekonkurrenceloven. Det fremgår af de specielle bemærkninger til denne bestemmelse, at bestemmelsen vil give politiet adgang uden retskendelse til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, der ikke er indeholdt i 118-databasen, og som udbyderen er i besiddelse af. Den udbyder, der har slutbrugerforholdet, vil således være forpligtet til at udlevere oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester til politiet, herunder oplysninger om slutbrugerens adgang til internettet (IP-adresser og e-mailadresser), uden at betingelserne for edition skal være opfyldt. Der er således alene tale om oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger. Heraf følger, at der ikke er tale om oplysninger om betalingsmidler el. lign.

Der er både tale om navn til nummer og nummer til navn oplysninger. Bestemmelsen omfatter alene statiske oplysninger, idet registrering af dynamiske IP-adresser mv. vil ske i medfør af logningsforpligtelsen i retsplejeloven.

Telelovens § 13 har til formål at sikre politiet en hurtig og effektiv adgang til samtlige relevante oplysninger om en mistænkts eventuelle kommunikationsmuligheder og skabe overblik over pågældendes kommunikationsmuligheder – uden at skulle afvente kendelse om edition.

Telelovens § 13 berører derimod ikke den adgang til oplysninger om forbindelser mellem telefoner mv., som reguleres af reglerne retsplejelovens kap. 71 om indgreb i meddelelseshemmeligheden.

Bestemmelsen blev indsat på baggrund af overvejelser om danske samfunds beredskab og indsats mod terrorhandlinger, men bestemmelsen har efter dens ordlyd og forarbejder ingen kriminalitetskrav mv. Bestemmelsen vil således kunne anvendes til brug for politiets efterforskning af ethvert strafbart forhold, men også som led i politiets øvrige opgavevaretagelse, jf. politilovens § 2.

En anmodning fra politiet efter telelovens § 13, og et pålæg om edition fra domstolene, har således det til fælles, at de undergiver adressaten en aktiv handlepligt til at fremkomme med alle de oplysninger, som pålægget omhandler, og i den form som oplysningerne foreligger.

6.1.2. Logningsbekendtgørelsen

Som nævnt ovenfor under pkt. 3.1. følger det af logningsbekendtgørelsens § 4, stk. 1, nr. 8, at der skal foretages registrering af tidspunktet for første aktivering af anonyme tjenester (taletidskort).

Udbydere af forudbetalte anonyme tjenester (taletidskort) skal således registrere dato og tidspunkt for første aktivering af tjenesten og oplysninger om den mast, hvorfra aktiveringen blev foretaget. Udbyderne skal herudover registrere de oplysninger, der i øvrigt skal registreres for mobiltelefoni, jf. bekendtgørelsens § 3, på en bruger, der anvender taletidskort i udbyderens net. Dog vil oplysninger om f.eks. navn og adresse ikke nødvendigvis kunne registreres for brugere, der anvender taletidskort i udbyderens net, idet disse oplysninger typisk er ukendte for udbyderen. Oplysningerne vil – i overensstemmelse med bekendtgørelsens anvendelsesområde – alene skulle registreres, hvis de er kendte for udbyderne eller genereres eller behandles i udbydernes systemer.

6.2. Relevante dele af EU-Domstolens praksis

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen samt Ministerio Fiscal-dommen er gennemgået under afsnit 2.

For så vidt angår identitetsoplysninger er de relevante dele af La Quadrature du Net-dommen præmis 157-159. Det fremgår heraf navnlig,

- at data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, principielt ikke kan kvalificeres som et alvorligt

indgreb i grundlæggende rettigheder, og at logning og adgang til disse data alene med henblik på at identificere den pågældende bruger, og uden at de nævnte data kan kædes sammen med oplysninger om den foretagne kommunikation, kan begrundes i det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed samt beskyttelse af den offentlige sikkerhed, og

- at dette også gælder i tilfælde, hvor der ikke foreligger nogen forbindelse mellem samtlige brugere af elektroniske kommunikationsmidler og de forfulgte mål, eller der ikke er fastsat en særlig frist for en sådan logning.

6.3. Justitsministeriets overvejelser og den foreslåede ordning

Oplysninger om identiteten på brugerne af elektroniske kommunikationsmidler må efter Justitsministeriets opfattelse omfatte abonnentoplysninger i form af den fysiske eller juridiske persons navn, adresse og telefonnumre for både fastnet- og mobilabonnenter, og for mobilabonnenters vedkommende også numre, der identificerer det anvendte mobilabonnement, f.eks. IMSI-numre.

Afgrænsningen, af hvilke oplysninger der i øvrigt kan være omfattet af den generelle og udifferentierede logningsforpligtelse, må efter Justitsministeriets vurdering på baggrund af EU-Domstolens praksis kunne finde sted på baggrund af, om oplysningerne kun kan anvendes til at identificere den omhandlede bruger, og at de ikke i sig selv gør det muligt at fastlægge datoen, tidspunktet, varigheden og modtagerne af foretagne kommunikationer, eller de steder, hvor en kommunikation har fundet sted eller hyppigheden heraf med visse personer i en bestemt periode.

Det vurderes på den baggrund, at der tillige kan pålægges registrering og opbevaring af oplysninger, der entydigt identificerer den enhed (mobiltelefon, tablet, PC mv.), som brugeren ejer eller anvender (herunder IMEI-numre og MAC-adresser mv.).

6.3.1. Behov for ændring af telelovens § 13 og overførsel af bestemmelsen til retsplejeloven

Det følger af den gældende bestemmelse i telelovens § 13, at teleselskaberne på begæring af politiet skal udlevere oplysninger, der identificerer en slut-

brugers adgang til elektroniske kommunikationsnet eller -tjenester. Bestemmelsen giver politiet adgang, uden kendelse, til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, herunder IP-adresser og mail-adresser.

Bestemmelsen omfatter alene oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger.

Bestemmelsen omfatter ikke en pligt for udbyderen til at udlevere oplysninger om hvilke telefonnumre, der er anvendt i forbindelse med et givent IMEI-nummer/mobilterminal, henholdsvis hvilke IMEI-numre/mobilterminaler, der er anvendt i forbindelse med et telefonnummer (såkaldt IMEI-oplysning). Bestemmelsen indebærer dog heller ikke, at udleveringen af sådanne oplysninger ikke må finde sted.

Det er nødvendigt at ændre bestemmelsen for at tage højde for det nye foreslåede regime for logning af IP-adresser, jf. ovenfor under pkt. 4.3.3. Behovet for at ændre bestemmelsen er endvidere aktualiseret af en varierende praksis hos teleudbyderne med hensyn til, om udlevering af oplysninger knyttet til et IMEI-nummer forudsætter editionskendelse.

Indhentelse af oplysninger om hvilke mobiltelefoner mv., der har været anvendt til et mobilabonnement og omvendt, er et centralt indledende efterforskningsskridt, der sætter politiet i stand til umiddelbart at træffe beslutning om, hvorvidt der er grundlag for at iværksætte indgreb efter retsplejelovens regler, herunder indgreb i meddelelseshemmeligheden eller pålæg om edition. Hvis dette er tilfældet, iværksættes indgrebet i overensstemmelse med retsplejelovens regler på baggrund af enten forudgående retskendelse, eller på øjemedet efterfulgt af rettens kendelse.

Dette indledende efterforskningsskridt anvendes ofte på den måde, at politiet, der kender et telefonnummer, anmoder teleudbyderne om at oplyse nærmere om aktiviteten på teleudbyderens net knyttet til dette telefonnummer i en given periode. Det foreslås, at det fastsættes entydigt, at teleudbyderen i den forbindelse vil kunne pålægges at oplyse, hvilket IMEI-nummer der f.eks. har været knyttet til et konkret telefonnummer, jf. nærmere herom nedenfor. Dette IMEI-nummer vil derefter blive sendt retur til teleudbyderne med henblik på at fastslå, om det er kendt med andre telefonnumre.

Hvis politiet omvendt kender IMEI-nummeret, vil teleudbyderne blive anmodet om at oplyse tilknyttede telefonnumre.

Dette efterforskningsskridt anvendes til helt indledningsvis at fastlægge en mulig sammenhæng mellem fysiske personer og kommunikationsenheder, f.eks. i forhold til mistænkte målpersoner, eller i tilfælde, hvor en telefon er blevet stjålet. Efterforskningsskridtet er f.eks. særligt relevant i de tilfælde, hvor personer under mistanke for strafbar virksomhed skifter mellem flere SIM-kort og flere telefoner.

Ved at ændre og flytte bestemmelsen til retsplejeloven skabes der således dels en entydig forpligtelse for udbydere af elektroniske kommunikationsnet og -tjenester til slutbrugere til at udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester. Dels skabes der ensretning og transparens på området for indhentning af oplysninger fra udbyderne af elektroniske kommunikationsnet og -tjenester til slutbrugere.

Det foreslås på den baggrund, at telelovens § 13 nyaffattes og overflyttes til retsplejeloven, så der skabes en klar hjemmel til, at udbydere af elektroniske kommunikationsnet og -tjenester – i overensstemmelse med EU-Domstolens praksis – kan pålægges at udlevere basale oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet og -tjenester til politiet.

Dette omfatter oplysninger, der angiver, om en slutbruger har benyttet udbyderens elektroniske kommunikationsnet eller -tjenester inden for en nærmere angiven periode, herunder oplysninger om IMEI-nummer, og de nødvendige oplysninger om aktiviteten knyttet hertil. Dermed vil bestemmelsen således også omfatte oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt. Bestemmelsen vil i den forbindelse også omfatte basale oplysninger om slutbrugeren, herunder oplysninger om hvilke mobilabonnementer og kommunikationsenheder en slutbruger er registreret med. Bestemmelsen vil dog ikke omfatte IP-adresser, der vil blive omfattet af det foreslåede regime for logning af IP-adresser, jf. ovenfor under pkt. 4.3.3.

Bestemmelsen foreslås udformet teknologineutralt, således at hvis der som følge af den almindelige teknologiske udvikling opstår nye oplysningstyper, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet

eller -tjenester, eller som identificerer en mobiltelefon mv., eller et mobilabonnement, vil disse således også kunne omfattes af bestemmelsen.

På teknologiens nuværende stadie betyder det, at navnlig IMEI-nummer, IMSI-nummer og telefonnummer, vil være omfattet.

I overensstemmelse med det almindelige proportionalitetsprincip forudsættes det, at politiet kun indhenter de omhandlede oplysninger, for en begrænset periode, og at denne periode er så kort som muligt, vurderet ud fra den enkelte sags omstændigheder.

I modsætning til det nuværende anvendelsesområde for telelovens § 13, foreslås det, at den nye bestemmelse i retsplejeloven i dets helhed fremover kun vil kunne anvendes til brug for politiets efterforskning af lovovertrædelser, men ikke til politiets øvrige opgavevaretagelse.

Denne indsnævring i anvendelsesområdet er begrundet i behovet for at bringe bestemmelsen i fuld overensstemmelse med EU-Domstolens dom af 2. oktober 2018, Ministerio Fiscal, der som nævnt fastlog, at adgang til oplysninger svarende til den foreslåede bestemmelse ikke kunne kvalificeres som et "alvorligt" indgreb i de grundlæggende rettigheder for de personer, hvis data er omfattet, og at adgangen hertil kunne begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af "straffelovsovertrædelser" generelt.

På den baggrund foreslås det, at udlevering vil kunne ske med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt.

6.3.2. Behov for registrering af identitetsoplysninger på taletidskort

Når man tegner et mobilabonnement, skal man identificere sig selv over for mobilselskabet. Et sådan krav er der ikke ved køb af taletidskort. Der kan man gå ind fra gaden og købe et taletidskort og et nyt nummer, uden nogen som helst form for registrering.

Det har tidligere været diskuteret, hvorvidt der skulle indføres regler for registrering af taletidskort, idet teleoplysninger er en central del af politiets

efterforskning. I lyset af, at politiets anvendelsesmuligheder for loggede teleoplysninger i fremtiden bliver meget begrænset, er der behov for, at de få tilbageværende redskaber bliver så effektive som muligt.

Den forsatte adgang til at benytte uregistrerede taletidskort – sammenholdt med de fremtidige begrænsninger i logningen af teleoplysninger – må anses for at udgøre en væsentlig risiko for at omgå disse redskaber, med en deraf følgende negativ påvirkning af politiets muligheder for at forebygge, efterforske, afsløre og retsforfølge kriminalitet. Det må endvidere forventes, at organiserede kriminelle mv. vil udnytte sådanne sårbarheder.

Med henblik på at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse i forhold til oplysninger om brugeres civile identitet, har Justitsministeriet således fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til nærmere overvejelse. Dette er begrundet i hensynet til at minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle mv.

Det er Justitsministeriets vurdering, at La Quadrature du Net-dommen giver mulighed for at fastsætte regler om generel og udifferentieret logning af identitetsoplysninger på brugere af elektroniske kommunikationsmidler med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed samt beskyttelse af den offentlige sikkerhed, og at dette kan ske, uden er at der fastsæt en særlig frist for en sådan logning.

Det foreslås på den baggrund, at der stilles krav om, at der ved uregistrerede taletidskort fremadrettet ved salget af taletidskort er en forpligtelse til at registrere oplysninger om køberens civile identitet.

Det vil blive nærmere overvejet, om der herudover er behov for yderligere at forpligte teleudbydere mv. til at foretage registrering og opbevaring af oplysninger om alle brugeres civile identitet, både fysiske eller juridiske personer, herunder navn, adresse og telefonnumre for både fastnet- og mobilabonnenter og SIM-kortnumre (IMSI-nummer), og oplysninger der entydigt identificerer den anvendte enhed i form af IMEI-nummer og MAC-adresse.

7. Adgang til loggede oplysninger

7.1. Gældende ret

7.1.1. Retsplejelovens regler om myndighedernes adgang til loggede trafikdata

Retsplejelovens regler om edition giver myndighederne mulighed for at meddele teleudbydere mv. pålæg om at udlevere oplysninger, jf. retsplejelovens § 804, stk. 1. Lovens § 801, stk. 3, 1. pkt., fastslår imidlertid, at reglerne i lovens kapitel 71 om indgreb i meddelelseshemmeligheden mv. gælder for bl.a. oplysning om forbindelse mellem telefoner mv. Det kan i den forbindelse nævnes, at Højesteret i to afgørelser gengivet i Ugeskrift for Retsvæsen 1993, s. 1, og 1995, s. 374, har fastslået, at retten kun kan give telefonselskaber pålæg om edition med hensyn til teleoplysninger, dvs. trafikdata, hvis også betingelserne i retsplejelovens § 781 om indgreb i meddelelseshemmeligheden er opfyldt.

Betingelserne for myndighedernes mulighed for at få adgang til teleoplysninger, som teleudbyderne har lagret i medfør af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsens regler, reguleres derfor i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden mv.

Efter retsplejelovens § 780, stk. 1, nr. 3, kan politiet foretage indgreb i meddelelseshemmeligheden ved at indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsmiddel, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning). Ved indgrebet opnår politiet ikke kendskab til kommunikationens indhold, men kun til dens eksistens.

Retsplejelovens § 780, stk. 1, nr. 3, er efter sin ordlyd ikke begrænset til bestemte typer af oplysninger, der kan indhentes. Det fremgår af forarbejderne til bestemmelsen, at "teleoplysning" omfatter telefonnumre, jf. pkt. 2.4.1 i de almindelige bemærkninger til lovforslag nr. L 164A af 1. februar 1985, jf. Folketingstidende 1984-85, Tillæg A, sp. 2972. Teleoplysninger kan også være oplysninger om, hvilken eller hvilke master og masteceller den omhandlede telefon registreres på (masteoplysninger).

Udlevering af oplysninger om, hvilke telefoner eller tilsvarende kommunikationsapparat der har taget kontakt til en bestemt telefon mv., udgør ikke et indgreb i meddelelseshemmeligheden, hvis der er samtykke fra indehaveren af telefonen, jf. bemærkningerne til § 780 i lovforslag nr. L 164A af 1. februar 1985, jf. Folketingstidende, 1984-85, Tillæg A, sp. 3000. Udbydere af telenet eller telefontjenester kan pålægges at udlevere sådanne oplysninger, uden at betingelserne for at foretage indgreb i meddelelseshemmeligheden skal være opfyldt, jf. retsplejelovens § 786, stk. 2.

Reglerne vedrørende teleoplysning finder kun anvendelse, når der skal indhentes oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater, der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat. Hvis der alene er tale om oplysninger om, at eksempelvis en bestemt telefon har været registreret på en bestemt sendemast (historisk), indhentes der efter reglerne om edition, jf. nærmere nedenfor under pkt. 7.1.3 om edition.

Højesteret fastslog ved kendelse af 7. maj 1997, gengivet i Ugeskrift for Retsvæsen, 1997, s. 1021 f., at retsplejelovens regler om teleoplysning, jf. § 780, stk. 1, nr. 3, giver hjemmel for indhentelse af teleoplysninger ikke blot om, hvilke telefoner mv., der har været sat i forbindelse med et bestemt telefonnummer, men også om, hvilke telefoner, der har været sat i forbindelse med telefoner på en nærmere angiven adresse, selv om numrene på telefonerne dér ikke på forhånd har kunnet angives. Derimod fandt Højesteret, at bestemmelsen ikke indeholder fornøden hjemmel til at indhente oplysninger om hvilke mobiltelefoner, der i en nærmere angiven periode havde været sat i forbindelse med hinanden via sendemaster inden for en radius af 1 km fra en nærmere angiven adresse. For den sidstnævnte type af oplysninger anvendes reglerne om udvidet teleoplysninger i § 780. stk. 1, nr. 4, jf. pkt. 7.1.2.

De almindelige betingelser for at foretage indgreb i meddelelseshemmeligheden, herunder i form af teleoplysning, findes i retsplejelovens § 781, stk. 1. Betingelserne er, at der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt (mistankekravet), og at indgrebet må antages at være af afgørende betydning for efterforskningen (indikationskravet), jf. retsplejelovens § 781, stk. 1, nr. 1 og 2.

Herudover er det en betingelse, at efterforskningen vedrører en af de lovovertrædelser, der er omfattet af § 781, stk. 1, nr. 3, stk. 2 og stk. 3 (kriminalitetskravet). Disse lovovertrædelser er dels afgrænset ved en generel henvisning til alle lovovertrædelser med en bestemt strafferamme dels specificeret ved henvisning til kapitler i straffeloven eller til lovbestemmelser.

Efter § 781, stk. 1, nr. 3, er det således en betingelse for at kunne foretage indgreb i meddelelseshemmeligheden, at efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitler 12 eller 13 eller en overtrædelse af straffelovens § 124, stk. 2 (befrielse af en anholdt eller fængslet mv), § 125 (hjælp til at unddrage nogen fra forfølgning for en forbrydelse mv.), § 127, stk. 1 (unddragelse af krigstjeneste mv.), § 233, stk. 1 (rufferi), § 235 (børnepornografi), § 266 (trusler), § 281 (afpresning) eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5 (forskellige former for forsætlig bistand til en udlænding med ulovlig indrejse, ophold eller lignende).

Kriminalitetskravet vedrørende forbrydelser, som efter loven kan medføre en straf på fængsel i 6 år eller derover blev i forarbejderne begrundet med, at lovovertrædelser, hvor strafferammen når op på fængsel i mindst 6 år, typisk er så alvorlige og af en sådan art, at det er både rimeligt og hensigtsmæssigt at give adgang til indgreb i meddelelseshemmeligheden, og at grænsen harmonerede med, at der i de senere år forud for lovforslaget var sket en nedsættelse af strafferammerne for visse forbrydelser og at dette også ville gøre sig gældende i fremtiden. Der henvises til pkt. 2.4.1 i de almindelige bemærkninger til lovforslag nr. L 164 A af 1. februar 1985, jf. Folketingstidende, 1984-85, Tillæg A, sp. 2971 f.

Retsplejelovens § 781, stk. 2 og 3, oplister herudover en række lovovertrædelser, der kan begrunde indgreb i meddelelseshemmeligheden, såfremt betingelserne i § 781, stk. 1, nr. 1 og 2, i øvrigt er opfyldt. Det drejer sig om følgende lovovertrædelser:

- Fredskrænkelser som omhandlet i straffelovens § 263, stk. 1. Denne bestemmelse vedrører den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem, jf. § 781, stk. 2.
- Krænkelser som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, jf. § 781, stk. 3, nr. 1. Denne bestemmelse

omfatter bl.a. krænkelser af en andens fred ved at forfølge eller genere den anden ved kontakt mv., hvilket omfatter at opsøge en anden ved personlig, mundtlig eller skriftlig henvendelse, herunder ved elektronisk kommunikation, eller på anden måde kontakte eller forfølge den anden, jf. § 1 i lov om tilhold, opholdsforbud og bortvisning.

- Overtrædelse af straffelovens § 279 a om databedrageri, eller § 293, stk. 1, om brugstyveri, begået ved anvendelse af en telekommunikationstjeneste, jf. § 781, stk. 3, nr. 2.
- Overtrædelse af artikel 14 eller 15 i Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014 om markedsmisbrug. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel og uretmæssig videregivelse af intern viden (artikel 14) samt forbud mod markedsmanipulation (artikel 15), jf. § 781, stk. 3, nr. 3.
- Overtrædelse af artikel 3, stk. 1, eller artikel 5 i Europa-Parlamentets og Rådets forordning (EU) nr. 1227/2011 af 25. oktober 2011 om integritet og gennemsigtighed på engrosenergimarkederne. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel (artikel 3, stk. 1) og forpligtelse til at offentliggøre intern viden (artikel 5), jf. § 781, stk. 3, nr. 4.
- Overtrædelse af artikel 38, stk. 1, artikel 39, artikel 40, jf. artikel 38, stk. 1, eller artikel 39, eller artikel 41 i Kommissionens forordning (EU) nr. 1031/2010 af 12. november 2010 om det tidsmæssige og administrative forløb af auktioner over kvoter for drivhusgasemissioner og andre aspekter i forbindelse med sådanne auktioner i medfør af Europa-Parlamentets og Rådets direktiv 2003/87/EF om en ordning for handel med kvoter for drivhusgasemissioner i Fællesskabet. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel (artikel 38, stk. 1, og artikel 40) og andre anvendelser af intern viden, som er forbudt (artikel 39), jf. § 781, stk. 3, nr. 5.

Teleoplysning må ligesom andre indgreb i meddelelseshemmeligheden ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb, jf. retsplejelovens § 782, stk. 1, der udtrykker det almindelige proportionalitetsprincip, der finder anvendelse ved straffeprocessuelle tvangsindgreb.

Henvisningen til "sagens betydning" i retsplejelovens § 782, stk. 1, indebærer, at der skal tages konkret stilling til alvoren af det forhold, der er under

efterforskning, uanset at lovovertrædelsen i øvrigt er omfattet af kriminalitetskravet i § 781.

Et indgreb i meddelelseshemmeligheden sker efter rettens kendelse, jf. retsplejelovens § 783, stk. 1. I kendelsen fastsættes det tidsrum, inden for hvilket indgrebet kan foretages, jf. stk. 3. Tidsrummet skal være så kort som muligt og må ikke overstige 4 uger. Tidsrummet kan forlænges, men højest med 4 uger ad gangen. Såfremt indgrebets øjemed ville forspildes, dersom retskendelse skulle afventes, kan politiet træffe beslutning om at foretage indgrebet, jf. § 783, stk. 4. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten.

Inden retten foretager indgreb i meddelelseshemmeligheden, skal der beskikkes en advokat for den, som indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig, jf. retsplejelovens § 784, stk. 1. Advokaten skal underrettes om alle retsmøder i sagen og er berettiget til at overvære disse samt til at gøre sig bekendt med det materiale, som politiet har tilvejebragt, jf. § 785, stk. 1.

Efter afslutningen af et indgreb i meddelelseshemmeligheden skal der gives underretning om indgrebet, jf. retsplejelovens § 788, stk. 1. Retten kan dog bestemme, at underretning skal undlades eller udsættes, hvis underretning vil være til skade for efterforskningen eller til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt taler imod underretning, jf. § 788, stk. 4, 1. pkt.

Efter retsplejelovens § 786, stk. 1, påhviler det bl.a. udbydere af telenet eller teletjenester at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at give de i § 780, stk. 1, nr. 3, nævnte oplysninger. Reglerne i lovens § 178 om vidnetvang finder tilsvarende anvendelse. Dette indebærer eksempelvis, at udbyderen kan idømmes en bøde, hvis udbyderen uden lovlig grund undlader at yde denne bistand, jf. § 178, stk. 1, nr. 1.

7.1.2. Særligt om retsplejelovens regler om udvidet teleoplysning

Efter retsplejelovens § 780, stk. 1, nr. 4, kan politiet indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning). Reglerne om udvidet teleoplysning blev indført ved lov nr. 465 af 7. juni 2001 om ændring af straffeloven og retsplejeloven (Hæleri og anden efterfølgende medvirken samt IT-efterforskning). Loven bygger bl.a. på betænkning nr. 1377/1999 fra Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet ("Brydensholt-udvalget").

Bestemmelsen i retsplejelovens § 780, stk. 1, nr. 4, om udvidet teleoplysning blev ifølge bemærkningerne til lovforslaget indsat på baggrund af den i pkt. 7.1.1 omtalte kendelse fra Højesteret fra 1997, gengivet i Ugeskrift for Retsvæsen, 1997, s. 1021 f., der fastslog, at der ikke i § 780, stk. 1, nr. 3, om teleoplysning var fornøden hjemmel til at indhente oplysninger om hvilke mobiltelefoner, der i en nærmere angiven periode havde været sat i forbindelse med hinanden via sendemaster inden for en radius af 1 km fra en nærmere angiven adresse, jf. pkt. 4.4.1, 4.4.2 og 4.4.3.1 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5707 ff.

Det fremgår af forarbejderne, at reglerne ikke specifikt vedrører masteoplysninger, men at bestemmelsen er formuleret, så den tager højde for den teknologiske udvikling og vedrører teleoplysninger, der ikke kan specificeres på kendelsestidspunktet, jf. pkt. 4.4.3.1 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5708 f.

For at kunne foretage udvidet teleoplysning, skal henholdsvis indikationskravet og kriminalitetskravet i retsplejelovens § 781, stk. 1, nr. 2 og 3, være opfyldt. Disse betingelser er omtalt i pkt. 7.1.1 ovenfor. Mistankekravet i § 781, stk. 1, nr. 1, skal ikke være opfyldt, men udvidet teleoplysning kan kun foretages, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller betydelige samfundsværdier, jf. § 781, stk. 5.

Reglerne om proportionalitet, retskendelse, advokatbeskikkelse, og bistandspligt fra teleselskaberne, gælder også for indgreb i meddelelseshemmeligheden i form af udvidet teleoplysninger. Der henvises til pkt. 7.1.1 ovenfor.

Efter afslutning af et indgreb i meddelelseshemmeligheden i form af udvidet teleoplysning efter § 780, stk. 1, nr. 4, skal der ikke gives underretning til indehaverne af de pågældende telefoner, jf. § 788, stk. 5. Denne fravigelse af udgangspunktet om underretning begrundes i bestemmelsens forarbejder med, at det vil medføre betydelige praktiske vanskeligheder at foretage sådan underretning, jf. pkt. 4.4.3.4 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5709 f.

7.1.3. Retsplejelovens regler om adgang til historiske masteoplysninger

I EU-Domstolens dom af 6. oktober 2020 i La Quadrature du Net-sagen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender.

I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata", som ikke er eller har været logningspligtig, og dermed ikke omfattet af EU-Domstolens dom i La Quadrature du Net-sagen.

Hvis oplysningerne ikke angår, hvilken bestemt telefon eller andet kommunikationsapparat som en telefon eller andet kommunikationsapparat har været sat i forbindelse med, men angår eksempelvis, hvilken sendemast eller lignende telefonen eller kommunikationsapparatet har været sat i forbindelse med, foreligger der ikke et indgreb i meddelelseshemmeligheden. Hvis et teleselskab er i besiddelse af sådanne oplysninger (historiske oplysninger), eksempelvis som følge af reglerne om logning, jf. retsplejelovens § 786, stk. 4, kan disse oplysninger udleveres efter reglerne om edition. Denne

retsstilling blev lagt til grund ved Højesterets kendelse af 22. juli 2009, gengivet i Ugeskrift for Retsvæsen, 2009, s. 2620 ff.

Efter retsplejelovens § 804, stk. 1, kan der som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning meddeles en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande (edition), hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskereres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

Ligesom for indgreb i meddelelseshemmeligheden gælder det, at et pålæg om edition ikke må meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre, jf. retsplejelovens § 805, stk. 1. Ifølge bestemmelsens forarbejder lovfæster den det almindelige proportionalitetsprincip, der antages at gælde ved alle straffeprocessuelle tvangsindgreb, herunder bl.a. reglen i § 782, stk. 1, jf. ovenfor i pkt. 7.1.1. Der henvises til bemærkningerne til § 805 i lovforslag nr. L 41 af 8. oktober 1998, jf. Folketingstidende 1998-99, tillæg A, s. 876.

Betingelserne for at kunne anvende retsplejelovens regler om edition er lempeligere end kravene for at kunne foretage indgreb i meddelelseshemmeligheden. For at kunne foretage edition kræves således alene, at der skal være tale om en lovovertrædelse, som er undergivet offentlig påtale, jf. retsplejelovens § 804, stk. 1.

Afgørelse om pålæg om edition træffes af retten efter politiets begæring, jf. retsplejelovens § 806, stk. 1 og 2. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om beslaglæggelse og om edition, jf. § 806, stk. 4. Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest muligt og senest inden 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes, jf. stk. 4, 2. punktum. Retsplejelovens § 806, stk. 8 og 9, indeholder regler om kontradiktion, for så vidt angår den, pålægget om edition retter sig imod. Men der er ingen pligt til at underrette den, der måtte være genstand for oplysningerne, eksempelvis ejeren af telefonen. Efter § 804, stk. 1, 2. pkt., jf. § 189, stk. 1, kan der meddeles en erhvervsvirksomhed pålæg om tavshedspligt med hensyn til viden om sagen, når hensynet til

fremmede magter, til statens sikkerhed eller til opklaring af alvorlige forbrydelser taler derfor.

Ud over de forpligtelser til udlevering af oplysninger, der følger af retsplejelovens regler om edition, er udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere efter § 13 i lov om elektroniske kommunikationsnet og -tjenester forpligtede til på begæring af politiet at udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

7.2. Relevante dele af La Quadrature du Net-dommen og H.K.-dommen

EU-Domstolens præmisser vedrørende logning af trafik- og lokaliseringsdata er omtalt ovenfor i afsnit 2.

For så vidt angår spørgsmålet om adgangen til lagret data, omtaler EU-Domstolen dette spørgsmål i La Quadrature du Net-dommen, præmis 166-167, hvoraf følgende fremgår:

> ”166. Det skal desuden tilføjes, således som det navnlig fremgår af denne doms præmis 115 og 133, at adgangen til de trafikdata og lokaliseringsdata, som udbyderne lagrer som følge af en foranstaltning, der er vedtaget i henhold til artikel 15, stk. 1, i direktiv 2002/58, i princippet kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring. Det følger navnlig heraf, at der under ingen omstændigheder kan gives adgang til sådanne data med henblik på at retsforfølge og straffe en almindelig strafbar handling, når lagringen heraf er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed. I overensstemmelse med proportionalitetsprincippet, således som dette er blevet præciseret i denne doms præmis 131, kan en adgang til data, der er lagret med henblik på bekæmpelse af grov kriminalitet, under forudsætning af, at de i den foregående præmis nævnte materielle og proceduremæssige betingelser, der gælder for at opnå en sådan adgang, overholdes, til gengæld begrundes i formålet om beskyttelse af den nationale sikkerhed.
>
> 167. I denne henseende står det medlemsstaterne frit for i deres lovgivning at fastsætte, at der under overholdelse af disse samme materielle og proceduremæssige betingelser kan gives adgang til trafikdata og lokaliseringsdata med henblik på bekæmpelsen af grov kriminalitet eller beskyttelsen af den nationale sikkerhed, når de nævnte data af en udbyder lagres på en måde, der er i overensstemmelse med artikel 5, 6 og 9 eller artikel 15, stk. 1, i direktiv 2002/58.”

Efter EU-Domstolens opfattelse må der således i princippet kun gives adgang til lagrede trafik- og lokaliseringsdata med henblik på at efterforske og retsforfølge en strafbar overtrædelse, hvis den strafbare overtrædelse vedrører det hensyn, der er baggrunden for, at teleudbyderne mv. er pålagt at lagre de pågældende data, idet der dog kan gives adgang til lagrede trafik- og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed, selv om lagringsforpligtelsen er pålagt med henblik på at bekæmpe grov kriminalitet.

Som det fremgår af den citerede præmis 166, finder EU-Domstolen, at hensynet til at efterforske og retsforfølge almindelig kriminalitet ikke vil kunne begrunde, at politi og anklagemyndighed kan få adgang til lagrede trafik- og lokaliseringsdata. EU-Domstolen tager derimod ikke eksplicit stilling til, om hensynet til at efterforske og retsforfølge grov kriminalitet vil kunne begrunde, at politi og anklagemyndighed kan få adgang til lagrede trafik- og lokaliseringsdata, der er lagret med henblik på at beskytte den nationale sikkerhed.

Domstolen henviser dog i præmis 166 til præmis 131, som lyder:

> ”131. Det fremgår nærmere bestemt af Domstolens praksis, at medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der navnlig er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, skal vurderes ved at bedømme alvoren af det indgreb, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 55 og den deri nævnte retspraksis).”

Når EU-Domstolen henviser til præmis 55 i Ministerio Fiscal-dommens opstillede proportionalitetskrav, må dette kunne tages til indtægt for den opfattelse, at Domstolen herved – fortsat – har den opfattelse, at et alvorligt indgreb (dvs. teleudbyderes pligt til at lagre trafik- og lokaliseringsdata og offentlige myndigheders adgang hertil) i de grundlæggende rettigheder kan begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser, der har til formål at bekæmpe kriminalitet, der på samme måde kan kvalificeres som ”grov”, jf. Ministerio Fiscal-dommens præmis 56.

Det vurderes således – dog under en væsentlig procesrisiko i lyset af præmis 166 i logningsdommen – at dommen ikke er til hinder for, at medlemsstaterne kan give politi og anklagemyndighed adgang til lagrede trafik- og lokaliseringsdata, der er lagret med henblik på at beskytte den nationale sikkerhed, i de tilfælde, hvor politi og anklagemyndighed bekæmper grov kriminalitet. I tilknytning hertil skal det dog bemærkes, at det må antages, at den grove kriminalitet skal være af en sådan alvorlig karakter, at det vil være i overensstemmelse med det EU-retlige proportionalitetskrav at give politi og anklagemyndighed adgang til sådanne lagrede trafik- og lokaliseringsdata.

EU-Domstolens dom af 2. marts 2021 i H.K.-sagen har ikke endeligt afgjort det rejste spørgsmål. På den ene side indeholder dommens præmis 31 en gengivelse af dele af den førnævnte præmis 166 i La Quadrature du Net-dommen, idet der udtales følgende:

> ”31. Hvad angår de formål, der kan begrunde de offentlige myndigheders adgang til de data, som udbydere af elektroniske kommunikationstjenester lagrer som følge af en foranstaltning, der er i overensstemmelse med disse bestemmelser, fremgår det af Domstolens praksis, at en sådan adgang kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse tjenesteudbydere er blevet pålagt at foretage denne lagring (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 166).”

På den anden side konstaterer EU-Domstolen følgende i præmis 33 i H.K.-sagen:

> ”33. Hvad angår det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager, der forfølges med den i hovedsagen omhandlede lovgivning, er det i overensstemmelse med proportionalitetsprincippet kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, såsom de indgreb, som lagring af trafikdata og lokaliseringsdata indebærer, **uanset om der er tale om generel og udifferentieret lagring eller målrettet lagring.** Det er således kun de indgreb i de nævnte grundlæggende rettigheder, der ikke er alvorlige, som kan begrundes i det formål, der forfølges med den i hovedsagen omhandlede lovgivning, om at foretage forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 140 og 146).” (fremhævet her)

Derudover bemærkes det, at EU-Domstolen ikke forholder sig generelt til, hvad der kan kvalificeres som henholdsvis "almindelig kriminalitet", "grov kriminalitet" og "beskyttelsen af den nationale sikkerhed". Det fremgår imidlertid af præmis 166, at adgangen til loggede data "i princippet kun kan begrundes i det mål af almen interesse med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring". Justitsministeriet forstår dette således, at der skal foretages en vurdering af kriminalitetens grovhed i forhold til, hvad der har begrundet lagringen af oplysningerne.

I præmis 154 omtales i forbindelse med spørgsmålet om lagring af IP-adresser, at IP-adressen, hvor en lovovertrædelse er begået online, kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået. Det hedder videre, at dette bl.a. kan "være tilfældet for særligt alvorlige lovovertrædelser på området for børnepornografi, såsom erhvervelse, udbredelse, transmission eller tilrådighedsstillelse online af børnepornografi som omhandlet i artikel 2, litra c), i Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi (…)".

7.3. Justitsministeriets overvejelser

7.3.1. Generelle overvejelser i forhold til dommens rækkevidde i forhold til adgang til loggede oplysninger

Adgangen til loggede teledata er et helt centralt efterforskningsmiddel for politiet i forbindelse med efterforskningen af alvorlig kriminalitet, ligesom det kan være afgørende i forhold til anklagemyndighedens strafforfølgning af tiltalte ved domstolene. Det gælder for såvel trafikdata (teleoplysninger) som historiske masteoplysninger.

Teledata defineres efter Justitsministeriets opfattelse som oplysninger, som teleudbyderne indsamler, registrerer og opbevarer (logger) samt bearbejder dels i forretningsøjemed, bl.a. til brug for taksering af ydelser, fakturering af kunder og fejlretning på netværket, dels for at efterleve kravene i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen.

Teledata indeholder oplysninger om kommunikation på telenetværket. F.eks. om hvilke telefoner der har været i kontakt med hinanden, og hvilke sendemaster de har været registreret på. Teledata indeholder, i modsætning til f.eks. telefonaflytning, ikke oplysninger om indholdet af kommunikationen.

Adgang til teledata vil typisk omfatte teleoplysning, herunder masteoplysninger, efter retsplejelovens § 780, stk. 1, nr. 3, jf. § 804, stk. 1, og udvidet teleoplysning (mastesug) efter reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens § 780, stk. 1, nr. 4, jf. § 804, stk. 1, mens udlevering af historiske masteoplysninger (som betegnes "lokaliseringsdata" i La Quadrature du Net-dommen) efter omstændighederne pålægges alene efter reglerne om edition i retsplejelovens § 804, stk. 1.

Politiet anvender loggede teledata på forskellige stadier af en efterforskning. I den indledende fase af en efterforskning kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikation og på den baggrund danne et overblik over personernes kommunikationsmønstre og færden. Herved er det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke personer fra efterforskningen, hvis de vurderes ikke at have relevans for sagen. Teledata kan være med til bl.a. at målrette politiets indsamling af andre beviser på et tidligt stadie af efterforskningen, herunder videoovervågning, f.eks. for hurtigt at finde og identificere en ellers ukendt gerningsmand. I tilfælde hvor den formodede gerningsmand er kendt af politiet, men forsvundet, kan teledata også bidrage til at opspore den mistænkte. En analyse af indhentede teledata kan også resultere i nye efterforskningsveje eller kaste lys over andre forhold, der gør det nødvendigt at indhente yderligere teledata. Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan teledata bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes teledata til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

Udvidet teleoplysning (mastesug) omfatter oplysninger om, hvilke telefoner der inden for et nærmere angivet område har været eller sættes i forbindelse med andre telefoner. Indhentelse af udvidede teleoplysninger (mastesug) anvendes til at identificere telefonnumre af interesse for politiets efterforskning, hvorefter efterforskningen kan målrettes indsamling af andre bevismidler, herunder historiske teleoplysninger. Et af områderne for anvendelse

af udvidede teleoplysninger er sager, hvor et antal ukendte personer, der mistænkes for at have begået en alvorlig forbrydelse, vurderes at have kommunikeret med hinanden umiddelbart før og efter den pågældende forbrydelse, muligvis via mobiltelefoner, og hvor den eneste efterforskningsmulighed er at få oplysninger fra den nærmeste sendemast i forhold til gerningsstedet og dermed se, hvilke telefoner der har kommunikeret via masten. Udvidede teleoplysninger kan have stor betydning i forbindelse med efterforskning af grov kriminalitet som f.eks. terror, drab, røveri mv. og i forbindelse med målrettede eftersøgninger i denne sammenhæng.

Pålæg om edition af historiske masteoplysninger, der viser, hvilke sendemaster telefonen har været registreret på i en given periode, og dermed kan vise et bevægelsesmønster for den pågældende telefon, kan derudover være et effektivt og afgørende efterforskningsskridt for politiet, ligesom det kan være afgørende i forhold til anklagemyndighedens strafforfølgning af tiltalte ved domstolene.

Det er derfor Justitsministeriets vurdering, at politiet og anklagemyndigheden i videst muligt omfang fortsat bør have adgang til loggede oplysninger inden for rammerne af EU-retten, herunder særligt La Quadrature du Net-dommen.

Justitsministeriet finder imidlertid i lyset af EU-Domstolens dom i La Quadrature du Net-sagen, navnlig præmis 166, som gennemgået ovenfor, at der er behov for at ændre reglerne om edition, sådan at det sikres, at der alene gives adgang til historiske masteoplysninger, når der er tale om efterforskning af grov kriminalitet. Justitsministeriet finder endvidere, at der er behov for at vurdere, om reglerne om adgang til loggede trafikdata ved indgreb i meddelelseshemmeligheden ligeledes bør ændres i lyset af EU-Domstolens dom, herunder om der i lyset af, at lagringen af data vil ske mere målrettet, er rum for at stille et lempeligere kriminalitetskrav for adgang til denne type oplysninger, end det nuværende.

Justitsministeriet overvejer konkrete modeller for, hvordan dette bedst sikres.

Det kan f.eks. være ved at sikre, at der gælder et tilstrækkeligt kriminalitetskrav for de pågældende indgreb, når de sker for at få udleveret loggede op-

lysninger. Et sådant kriminalitetskrav vil – som i dag for så vidt angår indgreb i meddelelseshemmeligheden – bl.a. kunne fastsættes i form af et krav til strafferammen for de lovovertrædelser, som efterforskes.

Domstolens præmisser giver imidlertid efter Justitsministeriets umiddelbare opfattelse ikke grundlag for at konkludere, at den for lovovertrædelsen foreskrevne strafferamme er det eneste kriterium, der vil kunne indgå ved vurderingen af, om en lovovertrædelse kan kvalificeres som henholdsvis "almindelig" eller "grov kriminalitet".

I denne vurdering må det efter Justitsministeriets opfattelse således også kunne indgå, om en alvorlig lovovertrædelse i praksis kun vanskeligt ville være mulig at efterforske, hvis ikke der var adgang til et bestemt tvangsindgreb, f.eks. indgreb i meddelelseshemmeligheden i form af teleoplysning, samt om lovovertrædelsen – uanset at den ikke måtte opfylde et strafferammekrav – kan karakteriseres som grov af andre årsager, f.eks. fordi der er tale om flere gentagelsestilfælde.

7.3.2. Retsplejelovens regler om adgang til loggede trafikdata

Justitsministeriet har overvejet, om La Quadrature du Net-dommen giver anledning til at ændre reglerne om indgreb i meddelelseshemmeligheden for så vidt angår adgang til teleoplysninger og udvidede teleoplysninger, som teleselskaberne pålægges at logge, i lyset af det strenge strafferammekrav, der allerede i dag som udgangspunkt gælder herfor. Justitsministeriet finder således, at et strafferammekrav på 6 års fængsel eller derover med sikkerhed må antages at opfylde betingelsen om, at indgrebet alene anvendes i relation til efterforskningen af grov kriminalitet.

Justitsministeriet finder derudover ikke, at nogen af de lovovertrædelser, der kan begrunde indgreb i meddelelseshemmeligheden efter kriminalitetskravet i § 781, på forhånd kan kvalificeres således, at de ikke vedrører grov kriminalitet. Dette vil dog skulle undersøges nærmere.

Det bemærkes i den forbindelse, at anvendelse af retsplejelovens regler om teleoplysning og udvidet teleoplysning, ligesom lovens regler om indgreb i meddelelseshemmeligheden i øvrigt, som udgangspunkt er betinget af forudgående retskendelse, hvor domstolene vurderer, om betingelserne for at foretage indgrebet er opfyldt. Som led i denne afgørelse vil domstolene vurdere, om indgrebet er proportionalt i forhold til den sag, der efterforskes, jf.

retsplejelovens § 782, stk. 1. Efter denne bestemmelse må et indgreb i meddelelseshemmeligheden ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være uforholdsmæssigt. Som beskrevet ovenfor i pkt. 7.1.1 indgår lovovertrædelsens grovhed i denne vurdering. Domstolene vil således også i dag skulle foretage en vurdering af betydningen af den sag, der forfølges, over for de oplysninger, der ønskes udleveret.

Politiet og anklagemyndigheden bør som anført sikres de bedst mulige rammer for at efterforske og retsforfølge grov kriminalitet. I forbindelse med ændringen af reglerne om teleudbydernes pligt til at logge data, vil der ske en indskrænkning i den data, som politi og anklagemyndighed vil have adgang til.

Justitsministeriet finder i den forbindelse, at det bør undersøges, om der – i lyset af at lagringen af data vil ske mere målrettet – er rum for at stille et lempeligere kriminalitetskrav end det nuværende.

7.3.3. Retsplejelovens regler om myndighedernes adgang til historiske masteoplysninger

Retsplejelovens regler om edition, jf. lovens § 804, giver politiet adgang til historiske masteoplysninger (betegnet "lokaliseringsdata" i dommen).

For så vidt angår editionspålæg, der kan give adgang til historiske masteoplysninger som omhandlet i dommen, gælder det ligesom for indgreb i meddelelseshemmeligheden, at det ikke på baggrund af dommen kan siges generelt hvilke former for lovovertrædelser, der kan kvalificeres som henholdsvis "almindelig kriminalitet", "grov kriminalitet" eller hvilke formål, der tjener til "beskyttelse af den nationale sikkerhed".

Retsplejelovens regler om edition omfatter på grund af det lempelige kriminalitetskrav (undergivet offentlig påtale eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning) en bred kategori af lovovertrædelser af meget forskellig karakter. Loggede data, f.eks. i form af historiske masteoplysninger, kan således pålægges udleveret som led i efterforskningen af en række lovovertrædelser, som det på forhånd kan være vanskeligt at kvalificere som "grov kriminalitet". Justitsministeriet vurderer på den baggrund, at der er et behov for at ændre reglerne om edition, sådan

at adgangen til historiske masteoplysninger, som teleudbyderne har været pålagt at logge, begrænses til at gælde i sager om grov kriminalitet. Dette kan bl.a. ske ved en ændring eller præcisering af kriminalitetskravet, idet et sådant krav dog ikke nødvendigvis vil kunne være eneste parameter for vurderingen af kriminalitetens grovhed, jf. ovenfor under pkt. 7.3.1. Dette vil blive undersøgt nærmere.

Justitsministeriet vil dog også i den forbindelse understrege, at der allerede i dag gælder et almindeligt proportionalitetsprincip, jf. retsplejelovens § 805, stk. 1. Domstolene vil derfor, før der meddeles pålæg om edition, skulle vurdere sagens betydning i forhold til det tab eller den ulempe, som indgrebet kan antages at medføre.

7.4. Forholdet til databeskyttelseslovgivningen

Databeskyttelsesforordningen og databeskyttelsesloven finder anvendelse for al behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Databeskyttelsesforordningen og databeskyttelsesloven finder dog ikke anvendelse i de tilfælde, der er nævnt i forordningens artikel 2, stk. 2, litra b-d, og lovens § 3. Forordningen og loven finder efter forordningens artikel 2, stk. 2, litra d, ikke anvendelse for retshåndhævende myndigheders behandling af personoplysninger til retshåndhævelsesformål, der i stedet er reguleret af bestemmelserne i retshåndhævelsesloven, som gennemfører det såkaldte retshåndhævelsesdirektiv. Endvidere finder databeskyttelsesforordningen og databeskyttelsesloven ikke anvendelse for behandling af personoplysninger, som udføres for eller af Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste, jf. databeskyttelseslovens § 3, stk. 2.

For behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet, finder reglerne i e-databeskyttelsesdirektivet anvendelse, jf. direktivets artikel 3, stk. 1. Efter direktivets artikel 1, stk. 2, specificerer og supplerer det databeskyttelsesforordningens bestemmelser på dette område. Det indebærer, at de danske regler om beskyttelse af personoplysninger, der gennemfører e-databeskyttelsesdirektivets bestemmelser, har forrang for reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Da spørgsmålet om, hvorvidt teleselskaberne må videregive trafik- og lokaliseringsdata til politiet, ikke er reguleret af e-databeskyttelsesdirektivet bestemmelser, skal regler herom fastsættes inden for rammerne af databeskyttelsesforordningen, herunder forordningens grundlæggende principper for behandling af personoplysninger og regler om, hvornår personoplysninger lovligt kan behandles.

De grundlæggende behandlingsprincipper følger af forordningens artikel 5, hvorefter personoplysninger bl.a. skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede. Endvidere skal personoplysninger indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. I forhold til dette princip om formålsbestemthed bemærkes det, at det efter forordningens artikel 6, stk. 4, og præambelbetragtning nr. 50 kan fastsættes i national ret, at der – uanset foreneligheden mellem formålene – kan ske behandling af oplysninger til et andet formål end det, de er indsamlet til. Det er en betingelse for fastsættelse af sådanne bestemmelser i national ret, at der er tale om en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er fastsat i forordningens artikel 23, stk. 1, herunder forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger.

Reglerne om, hvornår behandling af personoplysninger lovligt kan finde sted, følger af databeskyttelsesforordningens artikel 6, stk. 1, hvorefter behandling, herunder videregivelse, af ikke-følsomme personoplysninger som f.eks. trafik- og lokaliseringsdata lovligt kan finde sted, hvis det bl.a. er nødvendigt af hensyn til at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

For så vidt angår de nævnte scenarier under pkt. 7.2 ovenfor vil der efter Justitsministeriets vurdering inden for rammerne af databeskyttelsesforordningen, herunder forordningens artikel 5 og 6, stk. 1, litra c, og stk. 4, kunne fastsættes regler om politiets adgang til loggede oplysninger.

Politiets indhentning af sådanne oplysninger vil endvidere kunne ske inden for rammerne af retshåndhævelsesloven, hvorefter sådanne oplysninger kan behandles, når det bl.a. er nødvendigt for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger.

8. Perioden indtil et nyt regelsæt træder i kraft

Justitsministeriet har overvejet, om EU-Domstolens dom har betydning for, hvordan gældende regler kan administreres, indtil nye regler om revision af logningsreglerne mv. måtte træde i kraft.

Det bemærkes i den forbindelse, at forpligtelsen til at ændre national ret for at bringe den i overensstemmelse med EU-retten, som fortolket af EU-Domstolen i dommen, gælder så hurtigt som muligt. Der gælder derfor ikke en umiddelbar pligt til at ophæve eller suspendere de danske logningsregler. Tilsvarende gælder for så vidt angår reglerne om myndighedernes adgang til lagrede teledata.

Det bemærkes endvidere, at La Quadrature du Net-dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed, såfremt medlemsstaten står over for en sådan alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Som nævnt under afsnit 3.3.1, fremgår det af den seneste Vurdering af Terrortruslen mod Danmark, at CTA vurderer, at terrortruslen mod Danmark er alvorlig, altså det næsthøjeste niveau af fem niveauer. Det betyder i henhold til CTA's definitioner, at der er en erkendt trussel, og at der er kapacitet, hensigt og planlægning.

Det er i den forbindelse Justitsministeriets umiddelbare opfattelse, at Danmark på nuværende tidspunkt står over for en sådan alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, at en generel og udifferentieret logning vil kunne fastsættes i overensstemmelse med La Quadrature du Net-dommen.

For så vidt angår spørgsmålet om adgang til lagrede teledata, der er opnået ved hjælp af en generel og uddifferentieret logning, som måtte være uforenelig med EU-retten, har EU-Domstolen forholdt sig til dette i La Quadrature du Net-dommens præmis 228, hvoraf følgende fremgår:

> "228. […] artikel 15, stk. 1, som fortolket i lyset af effektivitetsprincippet, pålægger den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt

> mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder."

Det bemærkes i den forbindelse, at loggede oplysninger altid vil indgå som ét blandt flere beviser i en sag, og at betydningen af et bevis i form af teledata altid vil bero på en konkret vurdering af dels det enkelte bevis, dels sagens samlede omstændigheder i øvrigt. Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt et bevis i form af teledata skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse. Herudover vil der i overensstemmelse med det såkaldte "ligestillingsprincip" være adgang til kontradiktion samt fuld transparens i processen.

Det bemærkes derudover, at idet oplysningerne i overensstemmelse med EU-retten vil kunne være indhentet med henblik på beskyttelse mod en alvorlig trussel mod national sikkerhed, kan det ikke antages, at oplysningernes værdi kan betvivles, fordi de er indhentet på baggrund af en logningsforpligtelse, der ikke fuldt ud vil kunne opretholdes efter EU-retten. Endvidere må det antages, at lovligheden af logningsforpligtelsen ikke har haft betydning for bevisets værdi, uanset at oplysningerne ikke ville være indhentet, hvis der ikke var en sådan pligt til logning.

Samlet set er det således Justitsministeriet vurdering, at der ikke forud for indførelsen af ny lovgivning – som forventes at kunne træde i kraft 1. januar 2022 – er behov for en suspension af anvendelsen af loggede oplysninger, der er opnået ved en generel og udifferentieret lagring af trafik- og lokaliseringsdata. Efter Justitsministeriets vurdering kan loggede oplysninger således fortsat indhentes og anvendes efter de gældende regler i retsplejelovens kapitel 71 (indgreb i meddelelseshemmeligheden) og kapitel 74 (edition) til brug for efterforskningen, ligesom disse oplysninger også fortsat kan anvendes som bevis i straffesager. Det er endvidere Justitsministeriets vurdering, at databeskyttelsesforordningen ikke er til hinder for teleselskabernes fortsatte behandling af loggede teleoplysninger i overensstemmelse med logningsbekendtgørelsens bestemmelser.

9. Sammenfatning

Loggede oplysninger er centrale for politiets og efterretningstjenesternes arbejde, og dermed beskyttelsen af danske borgere mod trusler mod navnlig den nationale sikkerhed og grov kriminalitet.

Det er derfor afgørende for regeringen, at nationale myndigheders muligheder for logning sikres i videst muligt omfang inden for EU-rettens grænser.

På den baggrund foreslås en ordning, hvorefter justitsministeren, såfremt der foreligger en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, kan fastsætte en generel og udifferentieret forpligtelse for teleudbydere mv. til at foretage logning af teleoplysninger mv. for en afgrænset periode på op til 1 år. Det forventes, at Vurderingen af Terrortruslen mod Danmark kan indgå som et hovedmoment i en samlet vurdering, hvor også andre trusselsvurderinger kan indgå. Hvorvidt der foreligger en situation, som kan begrunde en sådan logningsforpligtelse, vil kunne prøves efterfølgende ved domstolene.

Der foreslås endvidere en ordning, hvorefter teleudbydere mv. kan pålægges personbestemt og geografisk målrettet logning for en afgrænset periode på op til 1 år af hensyn til bekæmpelse af grov kriminalitet mv. Det vil nærmere skulle vurderes, hvad der kan udgøre et tilstrækkeligt kriminalitetskrav for "grov kriminalitet".

For den personbestemte logning vil et pålæg kunne omfatte følgende kategorier af personer:

- Personer der inden for en nærmere bestemt årrække er dømt for grov kriminalitet mv.
- Personer der tidligere har været genstand for indgreb efter retsplejelovens kapitel 71 med henblik på bekæmpelse af grov kriminalitet mv.
- Personer der tidligere har været i kontakt med personer, som har været aflyttet med henblik på bekæmpelse af grov kriminalitet mv.
- Personer som retshåndhævende myndigheder har en konkret formodning om har forbindelse til grov kriminalitet mv.

For den geografisk målrettede logning vil et pålæg kunne fastsættes på baggrund af myndighedernes vurdering af – på grundlag af objektive og ikke-

diskriminerende forhold – en forhøjet risiko for, at der planlægges eller begås alvorlig kriminalitet i et givent område, herunder på følgende steder:

- Steder der er kendetegnet ved et højt antal tilfælde af grov kriminalitet.
- Steder der i særlig grad kan begås grov kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer.
- Strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

Endvidere foreslås en ordning, hvorefter der kan fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser for brugeres adgang til internettet for en periode på 1 år.

Den målrettede logning og logning af IP-adresser vil være begrænset til det strengt nødvendige samt ledsaget af processuelle garantier. Logningen forslås i overensstemmelse med La Quadrature du Net-dommen begrænset til bekæmpelse af grov kriminalitet, forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed. Det vil nærmere skulle vurderes, hvad der kan udgøre et tilstrækkeligt kriminalitetskrav for "grov kriminalitet".

Justitsministeriet finder endvidere, at der er behov for at ændre reglerne om edition, sådan at det sikres, at der alene gives adgang til historiske masteoplysninger ("lokaliseringsdata" i La Quadrature du Net-dommen), når der er tale om efterforskning af grov kriminalitet. Det vil ligeledes blive vurderet, om reglerne om adgang til loggede trafikdata ved indgreb i meddelelseshemmeligheden bør ændres i lyset af EU-Domstolens dom, herunder om der i lyset af, at lagringen af data vil ske mere målrettet, er rum for at stille et lempeligere kriminalitetskrav, for adgang til denne type oplysninger, end det nuværende.

For at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse, har Justitsministeriet fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til revision. Det forslås således, at der stilles krav om, at der fremadrettet ved salget af taletidskort er en forpligtelse til at registrere oplysninger om køberens civile identitet. Dette vil minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort

udgør i dag. Endelig forslås justering af ordningen om hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelse af den nationale sikkerhed.

De ovenstående overvejelser udgør de overordnede principper for, hvordan logning fremadrettet kan finde sted i Danmark. En lang række forhold vil skulle fastlægges nærmere i forbindelse med udformningen af det lovforslag, som regeringen forventer at fremsætte til efteråret 2021. Lovskitsen skal danne grundlag for drøftelser med branchen, interessenter mv., inden lovforslaget fremsættes.

Center for Terroranalyse CTA

VURDERING AF TERRORTRUSLEN MOD DANMARK

Marts 2021

Foto: Astrid Maria Rasmussen, Ritzau Scanpix

FORORD

Vurderingen af terrortruslen mod Danmark (VTD) udgør Center for Terroranalyses[1] (CTA's) samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet. Den er udarbejdet på baggrund af underliggende CTA-analyser, der strækker sig fra vurderinger af truslen mod konkrete personer, lokaliteter og begivenheder til bredere tendensanalyser og vurderinger af fænomener med betydning for terrortruslen mod Danmark og danske interesser i udlandet.

I forhold til den tidligere VTD har CTA valgt at justere betegnelsen for trusselsniveauskalaens laveste niveau fra "ingen" til "minimal" for at betegnelsen harmonerer med trusselsniveauets betydning. Herudover er formålet at kunne reflektere et trusselspotentiale på områder, hvor der ikke er erkendt kapacitet eller hensigt. På baggrund af denne præcisering indplaceres henholdsvis Grønland og Færøerne i trusselsniveauet "minimal" frem for "begrænset", uden at dette afspejler en ændring i truslens karakter.

Vurderingen af terrortruslen mod Danmark 2021 er udarbejdet i skyggen af en igangværende pandemi, som påvirker store dele af samfundet. Pandemien og dens afledte konsekvenser har også indflydelse på vurderingen af det aktuelle trusselsbillede, hvor der fortsat er usikkerhed om betydningen for den fremtidige udvikling.

Vurderingen beskriver terrortruslen fra militant islamisme, højreekstremisme, venstreekstremisme og andre trusler, der kan have karakter af terror. Afsnit 6 fokuserer på terrortruslen mod Grønland og Færøerne.

Vurderingen er baseret på efterretninger, der er blevet behandlet før den 15. marts 2021.

Med venlig hilsen

Michael Hamann
Chef for CTA

1. CTA er et fusionscenter, hvis medarbejdere stammer fra fem danske myndigheder (Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste, Udenrigsministeriet, Beredskabsstyrelsen og Rigspolitiets Nationale Efterforskningscenter).

Indhold

UDVALGTE BEGREBER OG SKALAER I VURDERINGEN

CTA anvender følgende sandsynlighedsgrader (fremhævet med *kursiv* i teksten):

Usandsynligt	*Mindre sandsynligt*	*Muligt*	*Sandsynligt*	*Meget sandsynligt*
<= 15%	*15-40%*	*40-60%*	*60-85%*	*>= 85%*

TERRORTRUSSELS-NIVEAU	DEFINITION
Meget alvorlig	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse.
Alvorlig	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.
Generel	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.
Begrænset	Der er en potentiel trussel. Der er begrænset kapacitet og/eller hensigt.
Minimal	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

BEGREBER	DEFINITION
Terrorisme	CTA definerer terrorisme jævnfør straffelovens § 114.
Vesten	Nordamerika, Australien, New Zealand og Europa, eksklusive Rusland, Hviderusland, Tyrkiet, Moldova og Kaukasus.
Udrejst	En privatperson, der er rejst til en konfliktzone med henblik på at støtte en af de stridende parter uden nødvendigvis at deltage i kamphandlinger.
Intention	Vilje til at bringe en given kapacitet i spil over for et givent mål eller en given målgruppe.
Kapacitet	Udtryk for en overensstemmelse mellem en persons tilgængelige midler og evnen (uddannelse, færdigheder, logistik osv.) til at anvende disse til et terrorangreb.
Ekstremisme	Vilje til at anvende vold eller andre ulovlige handlinger for at ændre eksisterende samfundsforhold.
Radikalisering	Dynamisk proces, hvor en person i stigende grad accepterer anvendelse af vold til at opnå politiske, religiøse eller ideologiske mål.
Soloterrorist	En person, der begår terrorangreb på egen hånd, mens planlægning, træning m.v. kan involvere andre personer.
Inspireret angreb	Gerningspersonen er inspireret af militant islamisme eller politisk ekstremisme og planlægger angreb på egen hånd.
Understøttet angreb	Gerningspersonen er i direkte kontakt med én eller flere personer, der vejleder eller på anden vis understøtter angrebsplaner.
Dirigeret angreb	Et angreb sanktioneres af og/eller planlægges med mandat fra en terrorgruppes ledelse.

Foto: Amager Torv, Strøget i København, Rune Johansen, Scanpix

1. OVERORDNET VURDERING AF TERRORTRUSLEN MOD DANMARK

CTA vurderer, at terrortruslen mod Danmark fortsat er alvorlig. Det betyder i henhold til PET's definitioner, at der er en erkendt trussel. Der er kapacitet, hensigt og planlægning[2].

PET iværksætter løbende operationer med henblik på at afdække og afværge mulige terrortrusler mod mål i Danmark. Siden 2019 har PET sammen med de respektive politikredse foretaget anholdelser i relation til fem separate terrorrelaterede sager. Senest anholdt PET i samarbejde med relevante politikredse 13 personer den 06. og 08. februar 2021 i Danmark, og yderligere én blev anholdt af tysk politi. Personerne er mistænkt for at planlægge et terrorangreb i Danmark eller udlandet med brug af skydevåben og hjemmelavede bomber.

Terrorangreb kan finde sted uden forudgående efterretningsmæssige indikationer, også selvom gerningspersonerne tidligere har været kendt for at nære sympati for militant islamisme eller politisk ekstremisme. En særlig bekymring knytter sig i den forbindelse til personer, der har gennemgået relativt kortvarige radikaliseringsforløb, og til personer, der ekskluderes fra eller afvises af ekstremistiske miljøer, eksempelvis på grund af særligt ekstreme holdninger eller opførsel.

Foto: Københavns Byret, Ida Guldbæk, Ritzau Scanpix

1.1 Militante islamister

Militante islamister udgør fortsat den væsentligste terrortrussel mod Danmark, og CTA vurderer, at denne trussel er i niveauet alvorlig. Det betyder i henhold til PET's definitioner, at der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.

Der er personer i Danmark og i udlandet med sympati for militant islamisme, som udgør en terrortrussel mod Danmark. CTA vurderer, at truslen udgår fra personer, der sympatiserer med og inspireres af udenlandske militant islamistiske terrorgrupper, særligt Islamisk Stat (IS) og al-Qaida (AQ). Det illustreres bl.a. af anholdelsen den 30. april 2020 af en dansk statsborger, mistænkt for at planlægge et terrorangreb på egen hånd med et eller flere skydevåben, og af anholdelserne den 06. februar 2021 af to syriske statsborgere i Danmark, mistænkt for at planlægge et terrorangreb i Danmark eller udlandet med brug af skydevåben og hjemmelavede bomber. I begge sager er der indikationer på, at de mistænkte var blevet inspireret af militant islamistisk propaganda.

I 2020 har hændelser i Danmark og udlandet, der er blevet opfattet som krænkelser af islam, vist, at krænkelsessager fortsat har et betydeligt potentiale som drivkraft for militante islamister. Reaktioner på krænkelsessager i udlandet og særligt i Frankrig har været med til at sætte fokus på både historiske og aktuelle krænkelsessager i Danmark. Både AQ og IS har i det seneste år omtalt Danmark i deres udgivelser, ligesom den AQ-affilierede gruppe al-Qaida på Den Arabiske Halvø (AQAP) i en propagandaudgivelse har opfordret til at angribe navngivne danske "krænkere". Et øget fokus på krænkelsessager generelt kan skærpe terrortruslen mod Danmark og danske interesser i udlandet. Eventuelle reaktioner vil kunne komme på kort sigt, men vil også kunne finde sted med en betydelig forsinkelse.

Der blev ikke gennemført militant islamistiske angreb i Danmark i 2020, men der blev i andre lande i Vesten gennemført 12 militant islamistiske angreb, mens der blev afværget otte angreb. Antallet af terrorangreb i Vesten var i 2020 væsentlig lavere end i perioden fra 2015 til 2017, om end der har været en stigning i antallet af gennemførte angreb i Vesten og særligt i Frankrig siden genoptrykningen af muhammedtegninger den 02. september 2020 i det franske satiremagasin Charlie Hebdo.

Det mest sandsynlige militant islamistiske terrorangreb i Danmark er et angreb, der udføres med let tilgængelige midler, skydevåben eller hjemmelavede bomber af en mindre gruppe eller en soloterrorist, der er inspireret af militant islamistisk propaganda. CTA vurderer, at truslen både udgår fra personer i danske militant islamistiske miljøer og fra andre radikaliserede personer i Danmark og udlandet. Internationale virtuelle fællesskaber, hvori der spredes propaganda og udveksles ekstremistiske synspunkter på tværs af landegrænser, spiller ofte en rolle i radikaliseringsforløb.

De mest sandsynlige mål for et militant islamistisk terrorangreb i Danmark er symbolmål eller ubeskyttede civile mål, såsom et offentligt befærdet sted. Symbolmål omfatter bl.a. personer, institutioner og begivenheder, der kan opfattes som islamkrænkende. Andre mulige symbolmål er jødiske mål, politi og militær – særligt i forbindelse med bevogtningsopgaver. Der kan også udgå en trussel mod andre myndighedsrepræsentanter og visse repræsentanter for politiske partier.

De militant islamistiske grupper IS og AQ er ledelsesmæssigt svækket, og deres kapacitet til at gennemføre komplekse, dirigerede terrorangreb i Vesten, herunder i Danmark, er fortsat reduceret. Gruppernes intention er dog uændret, og både IS og AQ opfordrer deres tilhængere til at udføre angreb mod mål i Vesten.

Aktuelt er knap halvdelen af de 160 voksne personer, der er udrejst fra Danmark til konfliktområderne i Syrien/Irak enten vendt tilbage til Danmark eller har taget ophold i et andet land i eller uden for Europa, mens omkring en tredjedel formodes omkommet i konfliktzonen. De resterende 32 formodes fortsat at opholde sig i konfliktzonen i Syrien/Irak eller i omkringliggende lande.

CTA vurderer, at truslen mod danske interesser i udlandet som udgangspunkt ikke adskiller sig fra truslen

2. Truslen mod Danmark kan fastholdes i "alvorlig" uden igangværende planlægning, da Danmark tidligere har været genstand for angrebsplanlægning, angrebsforsøg eller gennemførte angreb.

mod andre vestlige landes interesser. Danskere kan i lighed med andre vestlige personer blive tilfældige ofre for angreb, der rettes mod vestlige interesser, eller hvis danskere befinder sig i nærheden af lokale terrormål, såsom store menneskemængder, kirker eller visse myndighedsbygninger.

1.2 Højreekstremister

CTA vurderer, at terrortruslen fra højreekstremister mod Danmark er i niveauet generel. Det betyder i henhold til PET's definitioner, at der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.

Det mest sandsynlige højreekstremistiske terrorangreb i Danmark er et angreb med lettilgængelige midler eller skydevåben, der udføres af en soloterrorist eller en mindre gruppe. CTA vurderer, at truslen fra højreekstremister primært udgår fra personer og mindre grupper, der fortrinsvis mødes, radikaliseres og inspireres i højreekstremistiske virtuelle fællesskaber og netværk.

De mest sandsynlige mål for et højreekstremistisk terrorangreb i Danmark er muslimske mål, migrationsmål, jødiske mål, personer af anden etnisk oprindelse end dansk samt lokaliteter, hvor sådanne personer opfattes at samles. Andre mulige mål er politiske modstandere, især venstreekstremister og udvalgte politikere, der holdningsmæssigt står i et modsætningsforhold til højreekstremister. Herudover er visse myndigheder og LGBTQ+-personer også mulige mål.

Der har i 2020 været to gennemførte og syv afværgede højreekstremistiske terrorangreb i Vesten. Det er et markant fald i forhold til 2019, hvor særligt angrebet i marts 2019 i Christchurch, New Zealand, inspirerede andre højreekstremistiske angreb. Der var således i 2019 12 gennemførte og syv afværgede angreb.

1.3 Venstreekstremister

CTA vurderer, at terrortruslen fra venstreekstremister i Danmark er i niveauet begrænset. Det betyder i henhold til PET's definitioner, at der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt.

Det mest sandsynlige venstreekstremistiske terrorangreb i Danmark er et angreb med lettilgængelige midler, der udføres af en mindre gruppe personer, som er medlemmer af eller har kontakt til en dansk venstreekstremistisk gruppe.

De mest sandsynlige mål for et venstreekstremistisk terrorangreb er højreekstremistiske aktiviteter samt repræsentanter for myndigheder, først og fremmest politiet. Andre mulige mål er enkeltpersoner med opfattet sympati for højreekstremisme samt i mindre grad visse politikere og offentligt kendte personer, der opfattes som politiske modstandere, eksempelvis kunstnere og debattører.

1.4 Øvrige forhold

Der er en række andre forhold, der kan have betydning for terrortruslen i Danmark. Visse konspirationsteorier og bevægelser kan således indeholde et voldeligt trusselspotentiale, og disse forhold kan udvikle sig til handlinger, der efter en konkret juridisk vurdering kan have karakter af terror.

Herudover kan truende ytringer på bl.a. sociale medier påvirke visse psykisk uligevægtige eller meget påvirkelige personer til at begå vold, der kan have karakter af terror. Tilstedeværelsen af psykiske lidelser hos en gerningsperson kan gøre det vanskeligt for myndighederne at vurdere, hvorvidt personens voldelige handlinger udgør terror.

Endelig kan politiske, etniske og religiøse konflikter i udlandet føre til reaktioner fra personer eller grupper med tilknytning til de berørte grupper i Danmark, som kan udvikle sig til handlinger, der har karakter af terror. Sådanne handlinger kan involvere statslige aktører. De konkrete reaktioner, herunder voldelige protester, vil bl.a. kunne blive rettet mod politikere, myndighedsrepræsentanter, tilfældige borgere eller andre landes diplomatiske repræsentationer i Danmark.

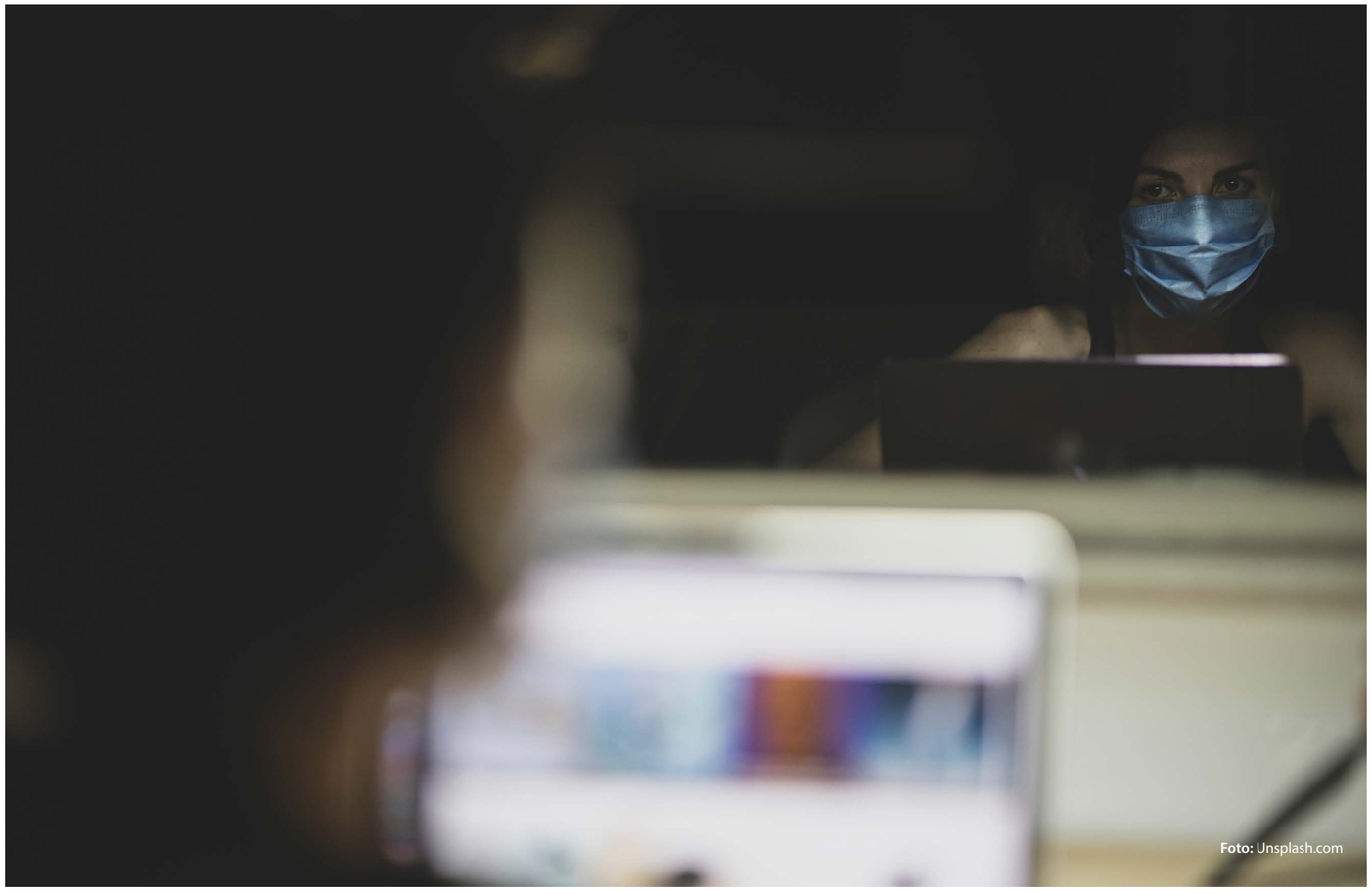


Foto: Unsplash.com

1.5 Betydningen af covid-19 for terrortruslen mod Danmark

CTA vurderer, at covid-19-pandemien ikke er en væsentlig drivkraft for terrorisme i Danmark og at pandemien og dens håndtering ikke i sig selv har ændret på militante islamisters eller politiske ekstremisters intention om og kapacitet til at begå terrorangreb i Danmark. Det er dog *sandsynligt*, at covid-19-pandemien har medvirket til at forstærke eksisterende antistatslige narrativer blandt højreekstremister i Danmark. CTA vurderer, at det øgede antistatslige fokus kan have betydning for danske højreekstremisters måludvælgelse. CTA vurderer endvidere, at modstand mod restriktio-

nerne eller vaccinationsprogrammer kan føre til trusler på livet, civil ulydighed, ildspåsættelse, hærværk og vold, der efter en konkret juridisk vurdering vil kunne have karakter af terror.

Virtuelle aktiviteter spiller ofte en rolle i personers radikaliseringsforløb, og det er *muligt*, at nedlukningen af samfundet under covid-19-pandemien i nogle tilfælde kan have øget forbruget af propaganda på internettet.

Begrænsninger af samfundsaktiviteten som følge af covid-19-restriktioner reducerer tilgængeligheden af ubeskyttede mål såsom forsamlinger i det offentlige rum. Dette kan afstedkomme, at en gerningsperson justerer sin angrebsplan og måludvælgelse.

CTA vurderer, at konspirationer om covid-19 kan appellere til og radikalisere personer, der ikke har eksisterende eller udprægede ekstremistiske synspunkter eller kontakt til ekstremistiske miljøer. En række konspirationsteorier, som udspringer af eller udbygges i relation til covid-19, indgår i et økosystem af konspirationsteorier online, der kan virke yderligere radikaliserende på allerede voldsparate personer og i visse tilfælde legitimere eller opfordre til voldelige handlinger. Det gælder særligt konspirationsteorier, der fremmer mistillid til myndigheder, som udbreder et forenklet sort-hvidt syn på verden, italesætter politikere og myndighedspersoner som fjender, og som legitimerer voldshandlinger ud fra hensyn til "folket".

Generelt har myndighedernes covid-19-restriktioner og vaccinationsprogrammer mødt modstand fra løst sammensatte grupper af covid-19-skeptikere og modstandere af covid-19-restriktioner. Modstanden har medført hård, antistatslig retorik på sociale medier, hvor der bl.a. ses trusler og personangreb mod udvalgte politikere samt repræsentanter fra myndigheder og sundhedsvæsen. Forhold relateret til vaccine kan tillige udnyttes af ekstremister og konspirationsteoretikere til misinformation og propaganda. Herudover har der været tilfælde af voldsanvendelse ved demonstrationer mod covid-19-restriktioner, eksempelvis ved demonstrationer i Aalborg og København i vinteren 2020/2021. CTA vurderer endvidere, at modstand mod restriktionerne eller vaccinationsprogrammer kan føre til trusler på livet, civil ulydighed, ildspåsættelse, hærværk og vold, der efter en konkret juridisk vurdering vil kunne have karakter af terror.

Vurdering af truslen fra covid-19-skeptikere og modstandere af covid-19-restriktioner er præget af en høj grad af usikkerhed. Der er tale om personer og grupper, der ikke har en velkendt og langvarig historik for så vidt angår voldelige protester eller andre reaktioner rettet mod politikere eller myndigheder, og informationsgrundlaget er følgelig begrænset.

CTA vurderer, at mængden af truende eller fjendtlige indlæg i virtuelle fora og ved demonstrationer med stor offentlig bevågenhed, kan øge risikoen for, at visse psykisk uligevægtige personer inspireres til at udføre en voldelig handling, der efter en konkret juridisk vurdering vil kunne have karakter af terror.

Det er *muligt*, at terrorgrupper i udlandet på længere sigt vil kunne drage fordel af pandemien og dens afledte virkninger, og at den generelle terrortrussel mod vestlige, herunder danske, interesser i de påvirkede lande og regioner på den baggrund vil blive forøget.

Militant islamisme

er en islamistisk ideologi, der legitimerer anvendelse af vold for at opnå politiske, religiøse eller ideologiske mål.

2. TERRORTRUSLEN MOD DANMARK FRA MILITANTE ISLAMISTER

Foto: Liselotte Sabroe, Ritzau Scanpix

Dette kapitel beskriver udviklingen på en række centrale områder, som CTA vurderer vil have betydning for terrortruslen mod Danmark fra militante islamister i det kommende år. Navnlig beskrives betydningen af opfattede krænkelser af islam, det globale trusselsbillede, virtuelle fællesskaber, militant islamistiske miljøer, forbindelser til bandemiljøer, radikaliserede løsladte fra fængslerne, udrejste og tilbagevendte fra konfliktzoner, asyl- og migrationsområdet samt personer, som kan rejse til Danmark for at begå terror. Til sidst vurderer CTA betydningen af terrorfinansiering fra Danmark og terrortruslen fra militante islamister mod danskere og danske interesser i udlandet.

CTA vurderer, at terrortruslen fra militante islamister mod Danmark er i niveauet alvorlig. Det betyder i henhold til PET's definitioner, at der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.

Det mest sandsynlige militant islamistiske terrorangreb i Danmark er et angreb, der udføres med lettilgængelige midler, skydevåben eller hjemmelavede bomber af en mindre gruppe eller en soloterrorist, der er inspireret af militant islamistisk propaganda. Angreb med lettilgængelige midler kan gennemføres spontant eller efter meget kort planlægning. CTA vurderer, at truslen både udgår fra personer i danske militant islamistiske miljøer og fra andre radikaliserede personer i Danmark og udlandet. Internationale, virtuelle fællesskaber, hvori der spredes propaganda og udveksles ekstremistiske synspunkter på tværs af landegrænser, spiller ofte en rolle i radikaliseringsforløb.

CTA vurderer, at covid-19-pandemien ikke er en oplagt drivkraft for militante islamister i Danmark, der traditionelt fokuserer på opfattede krænkelser af islam, opfattet undertrykkelse af muslimer samt vestlige militære interventioner i muslimske lande. Det er *muligt*, at personer i Danmark, som sympatiserer med militant islamisme, har brugt mere tid på internettet siden covid-19-pandemiens udbrud og indførelsen af restriktioner på samfundsaktiviteten. Personerne kan herved også være blevet eksponeret for mere ekstremistisk og voldsforherligende militant islamistisk propaganda og have forøget deres deltagelse i militant islamistiske virtuelle fællesskaber på internettet.

2.1 Betydningen af opfattede krænkelser for terrortruslen

Siden tegningesagen har sager om opfattede krænkelser af islam (herefter "krænkelsessager"), i nogle tilfælde relateret til debat om ytringsfrihed, været en faktor i terrortruslen mod Danmark. I 2020 har hændelser i Danmark og udlandet, der er blevet opfattet som krænkelser af islam, vist, at krænkelsessager i Danmark og udlandet fortsat har et betydeligt potentiale som drivkraft for militante islamister. Reaktioner på krænkelsessager i udlandet og særligt i Frankrig har været med til at sætte fokus på både historiske og aktuelle krænkelsessager i Danmark.

Det politiske parti Stram Kurs fortsatte i 2020 med at skænde koraner i forbindelse med en række demonstrationer i Danmark og enkelte demonstrationer i udlandet. Den internationale omtale af Stram Kurs og partiets formand tog til efter partiets afbrænding af en koran i Malmø, Sverige, den 28. august 2020.

Under en Stram Kurs-demonstration ved Gellerupparken i Aarhus, den 05. juni 2020, forcerede en person politiets afspærring og trak en kniv frem. Der foreligger indikationer på, at personen er psykisk uligevægtig. Gerningsmanden og en medtiltalt modtog i februar 2021 dom ved byretten for forsøg på vold af særlig farlig karakter, hvor den ene blev idømt fængsel i et år og tre måneder, mens den anden blev dømt til tidsubegrænset anbringelse og udvisning fra Danmark.

Det franske satiremagasin Charlie Hebdo genoptrykte den 02. september 2020 sin egen forsidetegning fra 2006 af en grædende Muhammed og samtlige 12 danske muhammedtegninger fra 2005. Anledningen var, at en retssag blev indledt den dag i Frankrig mod 14 personer tiltalt for at have forbindelse til terrorangrebet på Charlie Hebdo i januar 2015.

Genoptrykningen blev genstand for negative reaktioner i dele af den muslimske verden, ligesom en række militant islamistiske propagandamedier havde betydelig fokus på hævn over Frankrig. I ugerne efter genoptrykningen blev Danmark eller danskere i fire tilfælde

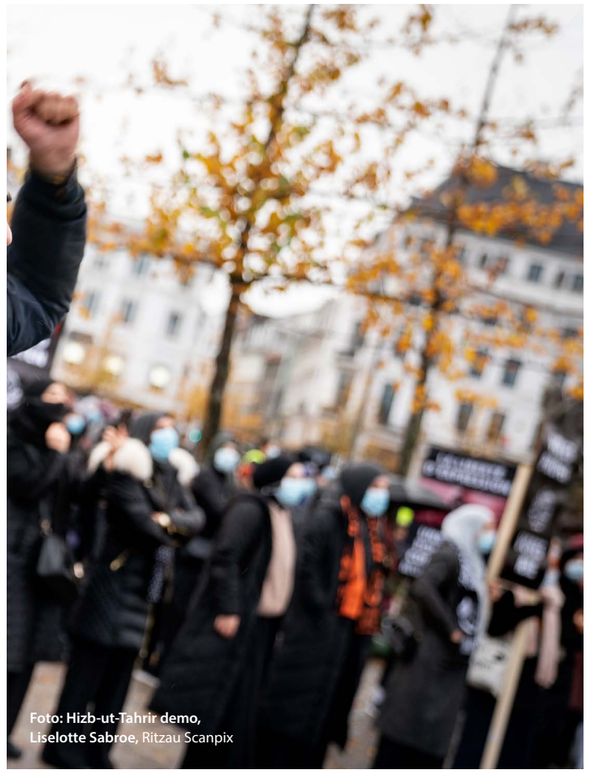


Foto: Hizb-ut-Tahrir demo, Liselotte Sabroe, Ritzau Scanpix

ker, at militante islamister også inden genoptrykningen i Charlie Hebdo havde fokus på Frankrig.

Genoptrykningen og særligt drabet på den franske skolelærer medførte tillige en debat om grænserne for ytringsfrihed i Danmark. Omfanget af hændelser i perioden gav også i Danmark anledning til betydelig bekymring i samfundet.

Omfanget af negative reaktioner på krænkelsessager i Vesten varierer fra sag til sag. Nogle sager opnår aldrig opmærksomhed, mens andre - som det var tilfældet i Frankrig i efteråret 2020 - opnår en betydelig negativ opmærksomhed, herunder planlægning og gennemførelse af militant islamistiske terrorangreb.

CTA vurderer, at Danmark blandt militante islamister siden tegningesagen i 2005 har haft et ry for at krænke islam. Når Danmark eller danskere nævnes eller fremhæves i militant islamistisk propaganda, kan Danmarks omdømme som "krænkelsesnation" atter få momentum.

CTA vurderer samlet, at markant militant islamistisk opmærksomhed på forhold og begivenheder i Danmark kan få betydning for terrortruslen rettet mod enkeltpersoner i Danmark, mod Danmark generelt og mod danske interesser i udlandet. CTA vurderer, at betydningen for terrortruslen i høj grad afhænger af den eksponering, de konkrete sager opnår i både nationale og internationale redaktionelle medier, på sociale medier og i den militant islamistiske propaganda, samt af reaktionen på disse sager i de militant islamistiske miljøer i Danmark og i udlandet. Eventuelle reaktioner vil kunne komme på kort sigt, men vil også kunne finde sted med en betydelig forsinkelse.

Endelig bemærker CTA, at militant islamistiske terrorangreb motiveret af sager om opfattede krænkelser af islam også kan medføre voldelige modreaktioner fra personer og grupper, der er motiveret af en højreekstremistisk antimuslimsk dagsorden.

omtalt direkte i militant islamistiske gruppers officielle propaganda. Danmark blev hovedsageligt brugt som historisk reference til den straf og de sanktioner, der tidligere har ramt lande, som bliver opfattet som krænkende over for islam.

I månederne efter genoptrykningen gennemførte militante islamister i Frankrig uafhængigt af hinanden tre terrorangreb rettet mod henholdsvis tilfældige personer ved Charlie Hebdos tidligere lokaler (den 25. september i Paris), en fransk skolelærer (den 16. oktober i Paris) og tilfældige personer i en kirke (29. oktober i Nice). Ved angrebene blev i alt fire personer dræbt, mens to blev hårdt såret. Det er *meget sandsynligt,* at alle tre angreb var motiveret af genoptrykningen af tegningerne i det franske satiremagasin. CTA bemær-

2.2 Udviklingen i det globale trusselsbillede for militant islamisme[3]

De militant islamistiske grupper IS og AQ står ledelsesmæssigt svækket, og deres kapacitet til at gennemføre komplekse, dirigerede terrorangreb i Vesten, herunder i Danmark, har været reduceret i de seneste år. Gruppernes intention er dog uændret, og både IS og AQ opfordrer deres tilhængere til at udføre angreb mod vestlige mål. Dette understreges ikke mindst af IS' indsats for at opbygge angrebsstrukturer uden for Syrien/Irak, der både kan agere lokalt og være i stand til at ramme mål i Vesten. Både IS og AQ har i 2020 udnyttet opfattede krænkelser af islam og covid-19-pandemien i deres propaganda.

Siden IS i marts 2019 mistede de sidste landområder, som gruppen kontrollerede i Syrien/Irak, har IS etableret sig som lokal terror- og oprørsgruppe i de to lande. Det er *sandsynligt*, at IS i Syrien/Irak primært er fokuseret på at angribe lokale mål.

IS ser Vesten som sin fjende og udgør sammen med IS-affilierede grupper og sympatisører fortsat en terrortrussel i Danmark og mod danske interesser i udlandet. Det er *sandsynligt*, at den overordnede strategi for IS er uændret, og at det langsigtede mål fortsat er at etablere et såkaldt kalifat. IS har også i 2020 opfordret sympatisører til på egen hånd at udføre angreb i deres hjemlande, herunder i Vesten.

AQ anser islam for at være under angreb fra Vesten, både militært, økonomisk, socialt og kulturelt. AQ og AQ-affilierede grupper udgør en trussel, selv om gruppens kapacitet til at dirigere komplekse angreb i Vesten fortsat er begrænset. Flere AQ-ledere døde i 2020, og det er *sandsynligt*, at disse tab vil forsinke, men ikke i sig selv forhindre, gruppens planer om at udføre terrorangreb mod vestlige mål.

Det er *sandsynligt*, at den primære trussel fra AQ mod Vesten udspringer fra mindre AQ-netværk, der opererer uafhængigt af hinanden. Netværkene er typisk enten tilknyttet AQ's øverste ledelse eller regionale undergrupper. Netværkene har intention om at ramme symbolske mål, og planlægningen strækker sig typisk over flere år. AQ har også i 2020 opfordret sympatisører til på egen hånd at udføre angreb i deres hjemlande, herunder i Vesten.

AQ's regionale undergrupper spiller en helt central rolle i gruppens organisation og globale tilstedeværelse. Undergrupperne er i dag til stede i store dele af Afrika, Mellemøsten og Asien. De fokuserer som udgangspunkt på egne, lokale interesser, men følger ofte den øverste ledelses vejledning.

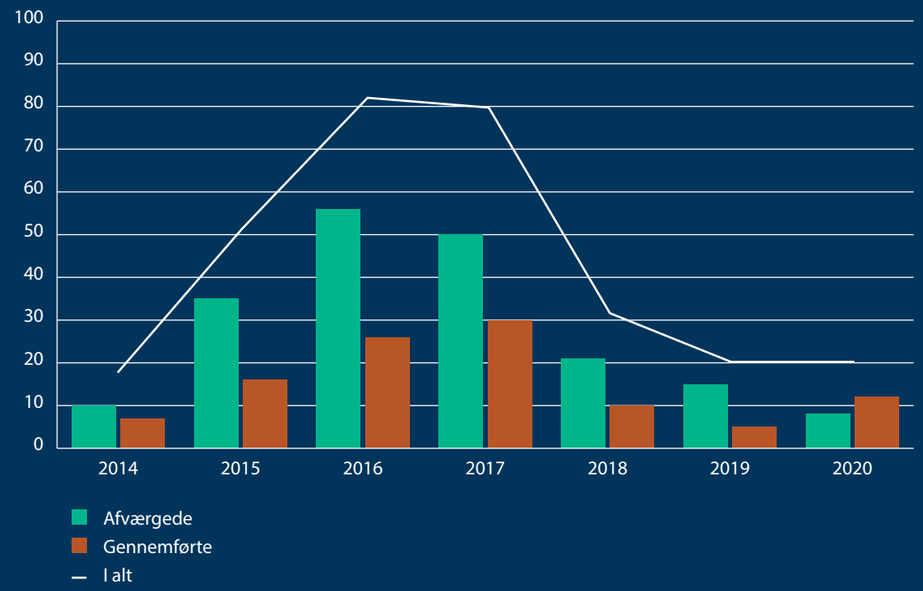
CTA vurderer, at IS- og AQ-sympatisører kan blive inspireret af gruppernes propaganda til at begå angreb i Danmark eller mod danske mål i udlandet. Både kvantiteten og kvaliteten af den officielle IS- og AQ-propaganda er fortsat markant reduceret sammenlignet med for få år siden, hvor særligt IS havde en omfattende propagandaproduktion. Der findes dog fortsat en stor mængde propaganda på internettet, herunder ekstrem voldelig IS-propaganda, der kan have betydning for radikalisering samt for udpegning af mål, ligesom den kan bidrage med konkret vejledning ved angrebsplanlægning.

IS, AQ, deres affilierede grupper og sympatisører har i en række tilfælde omtalt covid-19 i deres propaganda. IS har blandt andet haft fokus på, hvordan pandemien svækker vestlige landes økonomier og øger deres sårbarhed over for militant islamistiske angreb. Fokus på covid-19 var dog primært fremtrædende i starten af pandemien og er aftaget i takt med smittens globale spredning.

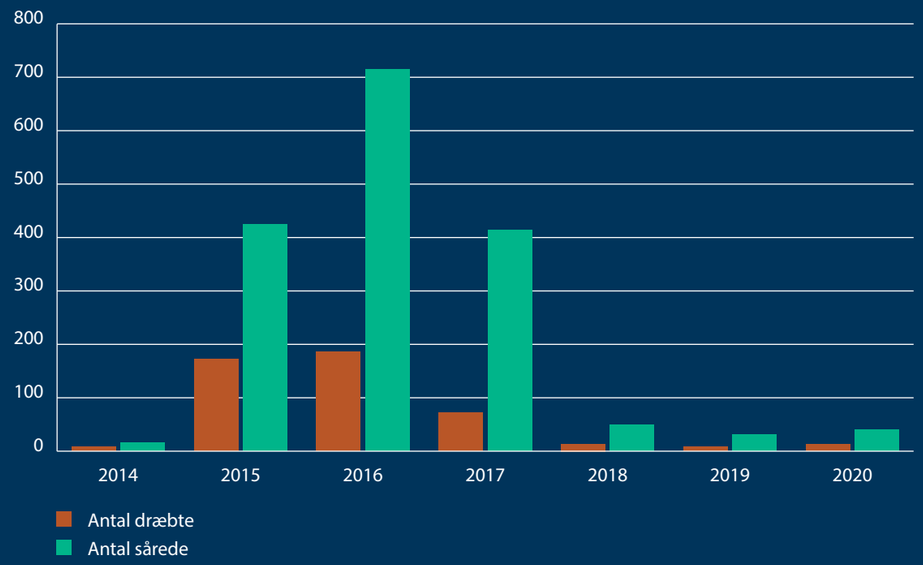
IS har siden september 2020 som noget nyt haft fokus på opfattede krænkelser af islam i sin officielle propaganda. Både IS, AQ, deres affilierede grupper og sympatisører har flere gange i efteråret og vinteren 2020 opfordret til hævn over opfattede krænkelser af islam samt til vareboykot.

3. CTA henviser til FE's Efterretningsmæssige Risikovurdering 2020 for yderligere detaljer.

Figur 1: Antal afværgede og gennemførte militant islamistiske terrorangreb i Vesten fra 2014 til og med 2020[4]



Figur 2: Antal sårede og dræbte ved militant islamistiske terrorangreb i Vesten fra 2014 til og med 2020



4. Det skal bemærkes, at opgørelser over antallet af afværgede og gennemførte militant islamistiske terrorangreb i Vesten kan variere afhængigt af opgørelsesmetode og tilgængelige oplysninger.

Definitioner på militant islamistiske måltyper

CTA vurderer, at der for militante islamisters måludvælgelse kan skelnes mellem symbolmål og civile mål.

Symbolmål

***Myndighedsmål**: Myndigheder, herunder visse ministerier, politi, militær, redningsberedskab, andre offentlige institutioner samt repræsentanter for sådanne myndigheder. Myndighedsmål kan også omfatte diplomatiske repræsentationer.*

***Politiske repræsentanter**: Folkevalgte, ministre og andre personer, begivenheder og lokaliteter med tilknytning til politiske partier og bevægelser.*

***Krænkelsesmål**: Grupper, personer, lokaliteter og arrangementer, der er udpeget i kraft af udtalelser, handlinger eller tematikker, som en gerningsperson opfatter som krænkende over for islam.*

***Jødiske mål**: Synagoger, jødiske tilholdssteder og institutioner, som fx skoler, samt andre mål, hvis tilknytning til jødedommen er identificerbar. Jødiske mål omfatter tillige israelske interesser i Danmark, herunder diplomatiske repræsentationer, virksomheder og turister.*

***Andre religiøse mål**: Kristne symbolmål som kirker og kristne skoler, muslimske symbolmål, herunder shiamuslimske moskéer, samt andre trosretninger.*

Civile mål

Andre personer, som ikke udgør et symbolmål. Eksempelvis forsamlinger af tilfældige personer på en offentlig plads, ved et arrangement eller et andet befærdet sted.

2.3 Terrormål og fremgangsmåder i Danmark for militante islamister

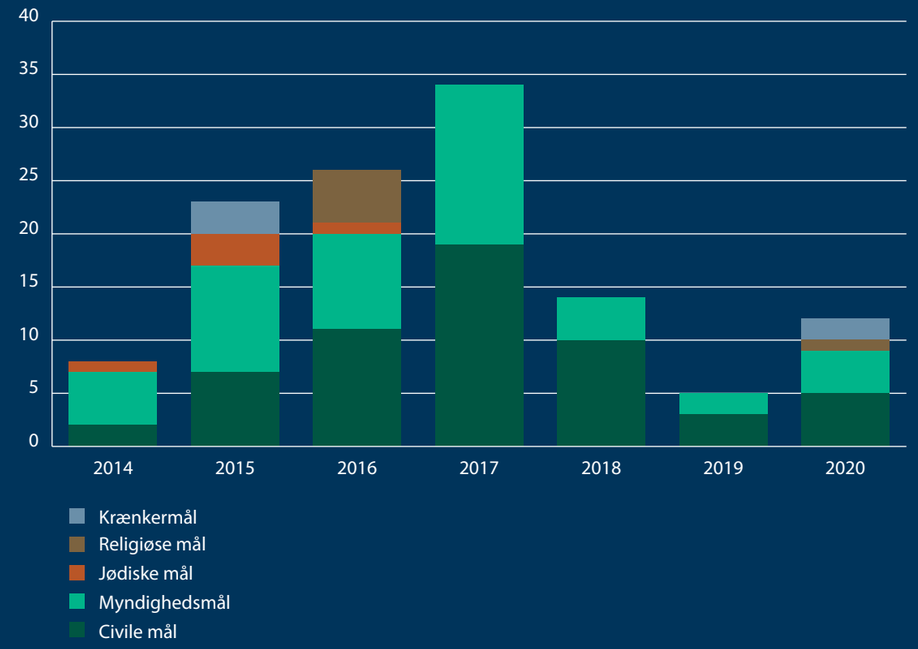
2.3.1 Mål

Militante islamisters måludpegning følger ikke et ensartet og forudsigeligt forløb og kan ændre sig i løbet af planlægningsfasen. Måludpegningen kan påvirkes af opfordringer i militant islamistisk propaganda, aktuelle dagsordner, personlige netværk og præferencer samt angrebsplanlæggerens kapacitet. Herudover kan allerede gennemførte terrorangreb i Vesten virke som inspiration for andre – en såkaldt copycat-effekt.

De mest sandsynlige mål for et militant islamistisk terrorangreb i Danmark er symbolmål eller ubeskyttede civile mål, såsom et offentligt befærdet sted. Truslen mod symbolmål retter sig i første række mod personer, institutioner og begivenheder, der kan opfattes som islamkrænkende. Andre mulige symbolmål er jødiske mål, politi og militær – særligt i forbindelse med bevogtningsopgaver. Der kan også udgå en trussel mod andre myndighedsmål og visse politiske repræsentanter[5]. Militante islamister har fortsat intention om at ramme transportinfrastrukturen.

Generelt måludpeges andre religiøse mål sjældent af militante islamister. IS har dog flere gange i sin propaganda opfordret til at angribe religiøse mål. I oktober 2020 var der et militant islamistisk terrorangreb mod besøgende i en kirke i Frankrig.

Figur 3: Måltyper for gennemførte militant islamistiske angreb i Vesten fra 2014 til og med 2020 (et angreb kan have flere mål)



5. Måltypen 'politiske repræsentanter' var tidligere inkluderet i måltypen 'myndighedsmål'. I nærværende VTD er kategorien udskilt som en selvstændig måltype. Etablering af en selvstændig måltype for politiske repræsentanter understøtter en mere detaljeret målbeskrivelse og er ikke i sig selv udtryk for ændringer i truslen.

Jødiske personer, begivenheder og lokaliteter har fortsat en fremtrædende plads i militant islamistisk propaganda, og militante islamister anser sådanne mål for at være legitime terrormål. Det seneste militant islamistiske angreb på et jødisk mål i Europa blev gennemført i januar 2016 i Frankrig.

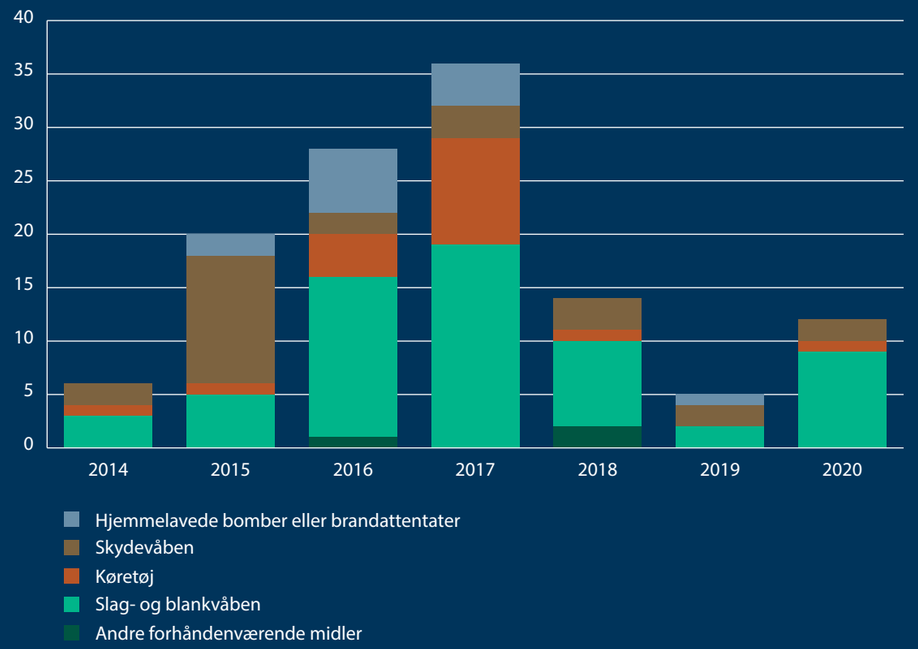
2.3.2 Fremgangsmåde[6]

CTA vurderer, at terrorangreb med lettilgængelige midler, skydevåben eller hjemmelavede bomber er den mest sandsynlige militant islamistiske angrebsform i Danmark. Angreb med lettilgængelige midler kan gennemføres spontant eller efter meget kort planlægning, mens angreb med skydevåben primært er forbeholdt personer med lovlig adgang til våben eller med kriminelle kontakter, der kan bistå med at skaffe våben. I en dansk kontekst udgør lettilgængelige midler hovedsageligt knive, slagvåben, ildspåsættelser eller køretøjer.

Anholdelserne i Danmark den 11. december 2019, den 30. april 2020 og den 06. februar 2021 understreger en vedholdende interesse for fortsat at gennemføre angreb med skydevåben i Danmark. De planlagde alle angiveligt at gennemføre terrorangreb på egen hånd med brug af bl.a. et eller flere skydevåben.

Det hyppigst anvendte middel ved militant islamistiske angreb i Vesten siden 2014 er slag- og blankvåben, der er blevet anvendt ved 50 procent af angrebene og forårsagede 11 procent af alle dræbte ved terrorangreb siden 2014.

Figur 4: Våben anvendt ved gennemførte militant islamistiske angreb i Vesten fra 2014 til og med 2020 (et angreb kan involvere flere våbentyper)



6. For yderligere uddybning af kapaciteten til terrorisme i Danmark, se bilag.

Terrorangreb med hjemmelavede bomber fremhæves løbende i militant islamistisk propaganda. Det seneste blev gennemført i 2019 i Lyon, Frankrig. I henholdsvis december 2019 og februar 2021 anholdt PET i samarbejde med relevante politikredse et antal personer, som blev sigtet for forberedelse til fremstilling af en eller flere bomber til brug ved en terrorhandling.

Angreb med droner eller kemiske, biologiske og radiologiske midler omtales løbende i militant islamistisk propaganda, og risikoen for angreb med sådanne midler nævnes også lejlighedsvist i åbne medier. Det er CTA's vurdering, at angreb med sådanne midler er *mindre sandsynligt*.

2.4 Fokusområder for truslen fra militant islamisme

2.4.1 Militante islamisters virtuelle fællesskaber og brug af internettet

Militante islamister i Danmark og udlandet anvender en række forskellige virtuelle fællesskaber til kommunikation med ligesindede, spredning af propaganda, radikalisering, rekruttering samt udveksling af informationer om våben og lignende, herunder bombe- og angrebsmanualer, der kan tjene til gensidig inspiration og kapacitetsopbygning.

Der hersker en betydelig grad af sikkerhedsbevidsthed i danske militante islamisters virtuelle fællesskaber. CTA har kendskab til, at militant islamistisk propaganda produceret af IS og AQ fortsat deles i danske onlinenetværk på sociale medier. På de større sociale medier deles propagandaen ofte i subtil form, hvor logoer og andre kendetegn associeret med terrorgrupperne er fjernet, så kun personer, der kender gruppernes symbolunivers og persongalleri, vil opfange, hvor propagandaen kommer fra, og forstå dens reelle betydning.

Det er *sandsynligt*, at militante islamister i Danmark og udlandet i det kommende år vil fortsætte og øge benyttelsen af virtuelle fællesskaber, idet de gør det muligt hurtigt og relativt nemt at sprede militant islamistiske budskaber og propaganda til et stort publikum på tværs af lande.

2.4.2 Militant islamistiske miljøer i Danmark

Mange militante islamister bevæger sig ind og ud af forskellige miljøer og gruppekonstellationer, hvor der deles ekstremistisk materiale og propaganda og pågår aktiviteter af social og religiøs karakter, der kan have en radikaliserende indvirkning på de deltagende personer. Særligt mere lukkede grupper kan fungere som ekkokamre, hvor deltagerne uimodsagt kan opbygge og bekræfte hinanden i et militant islamistisk verdenssyn. Militante islamister ses, ud over religiøse emner, optaget af især danske sager, som de opfatter som krænkende.

Der hersker en betydelig grad af sikkerhedsbevidsthed i danske militant islamistiske grupper. Billigelse af volds- og terrorhandlinger eller opbakning til fx IS og AQ sker som regel i mere lukkede forsamlinger eller indirekte gennem brug af indforståede referencer.

De fysiske militant islamistiske miljøer findes hovedsageligt i og omkring København, Aarhus og Aalborg samt på Fyn. Der er typisk tale om multietniske sunnimuslimske miljøer bestående af mindre grupper af mænd i 20'erne overvejende med baggrund i arabisktalende lande.

2.4.3 Forbindelser mellem militante islamister og danske bandemiljøer

CTA vurderer, at personer i bandemiljøet i Danmark først og fremmest er motiveret af pengeindtjening og personlig status. Der er dog flere eksempler på relationer mellem militante islamister og personer fra kriminelle miljøer. Disse relationer skyldes i de fleste tilfælde, at der er et geografisk og relationelt overlap i de miljøer, hvor bandemedlemmer og personer med sympati for militant islamisme færdes. Der er også eksempler på, at personer fra de militant islamistiske miljøer bedriver muslimsk mission (*dawa*) i kriminelle miljøer, ligesom imamer eller personer med høj agtelse i islamistiske kredse flere gange er blevet brugt til at forhandle fred mellem bandegrupperinger i konflikt.

CTA vurderer, at der i de danske bandemiljøer findes enkeltpersoner med sympati for militant islamisme, herunder også personer, som har været udrejst til Syrien/Irak. CTA vurderer, at personer, der påvirkes af militant islamistisk propaganda og som samtidig er tilknyttet kriminelle miljøer med en høj grad af voldsparathed og adgang til våben, kan udgøre en terrortrussel mod Danmark. Herudover kan vedvarende relationer mellem personer fra bandemiljøet og militant islamistiske miljøer øge militante islamisters kapacitet til at udføre terrorangreb i Danmark med skydevåben og sprængstoffer.

2.4.4 Radikaliserede løsladte fra fængslerne

CTA vurderer, at radikaliserede indsatte i fængslerne kan udgøre en terrortrussel under afsoning og efter løsladelse. Denne trussel kan udgå fra personer, der er dømt eller sigtet i terrorrelaterede sager, samt fra andre voldsparate personer, der påbegynder eller fortsætter en radikaliseringsproces under varetægtsfængsling eller domsafsoning. Radikalisering i fængslerne kommer desuden til udtryk ved udbredelse af ekstremistiske netværk og ideologisk påvirkning af andre.

CTA har kendskab til, at syv gerningspersoner i Europa siden 2015 har begået et terrorangreb under udgang eller inden for de første seks måneder efter deres løsladelse. En af disse gerningspersoner var danske Omar Abdel Hamid El-Hussein, der gennemførte et terrorangreb i København i februar 2015 ca. tre uger efter sin løsladelse. Senest begik en 20-årig mand med asylstatus den 04. oktober 2020 et terrorangreb med knive i Dresden, Tyskland, knap to uger efter, han blev løsladt. Dette var ét af tre angreb i 2020, som fandt sted inden for to uger efter gerningspersonernes løsladelse.

CTA modtager løbende oplysninger om bekymring for radikalisering og mulige trusler blandt indsatte i danske fængsler. CTA vurderer, at det kan skærpe truslen fra radikalisering blandt indsatte i danske fængsler, såfremt yderligere udrejste til Syrien/Irak returnerer til Danmark og bliver retsforfulgt. Dette gælder både for mænd og kvinder.

Foto: Storstrøm Fængsel, Asger Ladefogde, Ritzau Scanpix

CTA har kendskab til enkelte tilfælde, hvor personer dømt for militant islamistiske terrorrelaterede forbrydelser har interageret med hinanden under afsoning og har forsøgt at påvirke andre indsatte.

CTA vurderer, at der kan udgå en terrortrussel fra radikaliserede indsatte mod personale i fængsler og arresthuse. Siden 2014 har CTA kendskab til tre gennemførte terrorangreb i andre europæiske lande mod fængselspersonale motiveret af militant islamisme.

2.4.5 Truslen fra udrejste og tilbagevendte fra konfliktzonen i Syrien/Irak

CTA vurderer, at personer, der er eller har været udrejst fra Danmark til konfliktzonen i Syrien/Irak, kan udgøre en trussel mod Danmark eller mod danske interesser i udlandet. Det gælder både mænd og kvinder og uanset om personerne opholder sig i konfliktzonen, er returneret til Danmark eller opholder sig i et andet land i eller uden for Europa. Den mulige trussel er ikke begrænset til eventuel angrebsplanlægning, men vedrører også radikalisering af andre personer, propagandavirksomhed, logistisk støtte, terrorfinansiering og anden terrorrelateret virksomhed.

Også personer udrejst fra andre lande end Danmark, herunder fra andre europæiske lande, kan udgøre en trussel mod Danmark og danske interesser i udlandet. Truslen fra andre landes udrejste udgår i første række – men ikke udelukkende – fra personer, der opholder sig i lande, som grænser op til Danmark.

En persons udrejse til en konfliktzone for at støtte en militant islamistisk dagsorden betyder dog ikke nødvendigvis, at personen udgør en terrortrussel mod Danmark eller danske interesser i udlandet. Terrortruslen beror på en konkret vurdering af den enkeltes hensigt og kapacitet til at angribe danske mål. Blandt relevante faktorer er den udrejste persons fortsatte sympati for militant islamisme og tilknytning til militant islamistiske grupper samt personens eventuelle våbentræning og deltagelse i kamphandlinger. Ifølge CTA's oplysninger har syv procent af alle gennemførte og afværgede angreb i Vesten siden 2014 involveret gerningspersoner, der har været udrejst til Syrien/Irak.

CTA vurderer, at der siden sommeren 2012 er mindst 160 personer, der er eller har været udrejst fra Danmark til Syrien/Irak for at tilslutte sig militant islamistiske grupper. Af disse er knap halvdelen på nuværende tidspunkt vendt tilbage til Danmark eller har taget ophold i primært andre europæiske lande.

Knap en tredjedel af det samlede antal udrejste er ifølge PET's oplysninger omkommet i konfliktzonen. 32 voksne personer udrejst fra Danmark befinder sig fortsat i Syrien/Irak, eller i omkringliggende lande. Lidt under halvdelen af dem er kvinder. Af de 32 voksne personer, der fortsat opholder sig i konfliktzonen eller i omkringliggende lande, har 11 alene haft opholdstilladelse i Danmark, og af disse har foreløbig 10 fået deres opholdstilladelse inddraget. Herudover har 10 fået frataget deres danske statsborgerskab administrativt. De resterende 11 voksne personer er danske statsborgere. Af disse 11 personer er fem ifølge PET's oplysninger fængslet eller tilbageholdt, hovedsageligt i kurdisk-kontrollerede lejre i det nordøstlige Syrien, mens de resterende seks formodes fortsat at opholde sig på fri fod i eller omkring konfliktzonen eller i omkringliggende lande.

Foto: Unsplash.com

Det er ifølge PET's oplysninger ikke lykkedes personer at udrejse fra Danmark til konfliktzonen i Syrien/Irak for at tilslutte sig militant islamistiske grupper siden 2016. Tre voksne udrejste personer er blevet udleveret til Danmark siden 2016, heraf to i 2020. Alle tre er aktuelt fængslet. CTA har ikke kendskab til yderligere personer, som er returneret til Danmark siden 2016. Alle resterende 32 voksne udrejste fra Danmark har været i konfliktzonen eller i omkringliggende lande i mere end fire år.

CTA vurderer, at kun få af de personer, der er eller har været udrejst fra Danmark til Syrien/Irak, og som aktuelt befinder sig i konfliktzonen, vil være i stand til at vende tilbage til Danmark på kort sigt uden bistand fra danske eller andre landes myndigheder. Størstedelen af de tilbageværende voksne danske udrejste vil blive retsforfulgt, hvis de indrejser i Danmark.

Det er CTA's vurdering, at forholdene i lejre og fængsler i det nordøstlige Syrien kan bidrage til at øge radikaliseringen af tilbageholdte personer, herunder også tilbageholdte personer udrejst fra Danmark.

I 2020 er det lykkedes et stigende antal kvinder fra især europæiske, men også andre lande at flygte fra lejre i det nordøstlige Syrien – nogle af dem ledsaget af børn. CTA vurderer, at det også fremover vil kunne lykkes kvinder med eller uden børn at flygte fra lejre i det nordøstlige Syrien, herunder potentielt også kvinder med tilknytning til Danmark.

Der er flere rapporter om fangeoprør i de overfyldte kurdisk-kontrollerede fængsler i det nordøstlige Syrien, hvor omkring 2.000 udrejste mænd med tilknytning til IS er tilbageholdt, ligesom der det seneste år har været tilfælde af indsatte med tilknytning til IS, der har formået at flygte. Det er *sandsynligt*, at der også det kommende år vil være mænd, der formår at flygte fra fængsler i det nordøstlige Syrien. CTA vurderer dog, at det også fremover vil være væsentligt mere vanskeligt at flygte fra fængsler end fra lejre.

De udrejstes børn

Der er flere af personerne udrejst fra Danmark, der medbragte børn til konfliktzonen, og nogle har fået børn under deres ophold i konfliktzonen. Ifølge PET's oplysninger opholder der sig ca. 45 børn i og omkring konfliktzonen med mindst én forælder, som var dansk statsborger ved barnets fødsel. PET har herudover oplysninger om, at ca. 10 børn af personer, som tidligere har haft opholdstilladelse i Danmark, også opholder sig i eller omkring konfliktzonen. Af de i alt ca. 60 børn af personer udrejst fra Danmark opholder mindst 25 sig i det nordøstlige Syrien, primært i lejrene al-Roj og al-Hawl. De øvrige opholder sig ifølge PET's oplysninger blandt andet i det nordvestlige Syrien og i Tyrkiet.

Det er efter CTA's vurdering *usandsynligt*, at der udgår en aktuel terrortrussel fra børn af personer udrejst fra Danmark til konfliktzonen. Det hænger først og fremmest sammen med børnenes nuværende lave alder. Det er CTA's generelle vurdering, at større børn, der indrejser i Danmark fra konfliktzonen eller fra lejre, kan udgøre en terrortrussel på grund af indoktrinering eller anden påvirkning i konfliktzonen. Det er i den forbindelse også CTA's vurdering, at risikoen for indoktrinering og påvirkning som udgangspunkt forøges, jo længere tid børnene opholder sig i et radikaliseret miljø, herunder i lejrene i det nordøstlige Syrien.

Truslen fra udrejste fra Danmark, herunder fra de udrejstes børn, der kommer til Danmark, vil blandt andet kunne påvirkes af, hvorledes de modtages af de hjemlige myndigheder, herunder om de tilbydes støtte med henblik på eventuel afradikalisering og reintegration.

2.4.6 Truslen fra asylansøgere, flygtninge, migranter og personer på tålt ophold

CTA vurderer, at asylansøgere, afviste asylansøgere, anerkendte flygtninge og migranter, der opholder sig i eller ankommer til Danmark, kan udgøre en terrortrussel, såfremt de er radikaliserede. Denne trussel kan udgå fra personer, der er tilrejst med flygtningestrømmen med forsæt om at begå terrorangreb i Europa, eller fra andre personer, der påbegynder eller fortsætter en radikaliseringsproces efter ankomsten til Danmark. CTA vurderer dog, at det kun er en meget lille andel af de personer, der ankommer til Europa og Danmark som flygtninge og migranter, der har sympati for militant islamisme, og som kan anses for at udgøre en terrortrussel.

Det er fortsat *muligt*, at militant islamistiske grupper vil forsøge at udnytte flygtninge- og migrantruter til at begå terrorangreb i Europa, herunder i Danmark. CTA har ikke kendskab til, at personer udsendt af en militant islamistisk terrorgruppe via flygtningestrømmen har begået terrorangreb i Europa det seneste år.

CTA vurderer endvidere, at asylansøgere, afviste asylansøgere og migranter kan være særligt modtagelige over for radikalisering og påvirkning fra militant islamistiske dagsordner. Det gør sig især gældende for yngre personer, der rejser alene. En øget modtagelighed kan bl.a. skyldes frustration over egen situation, en følelse af eksklusion, fravær af familie samt psykisk ustabilitet.

Siden november 2015 har asylansøgere, afviste asylansøgere, anerkendte flygtninge og/eller migranter været involveret i flere gennemførte og afværgede angreb i Europa. Fem af de gennemførte angreb har fundet sted det seneste år, senest den 29. oktober 2020 i Frankrig. Angrebet blev udført af en 21-årig tunesisk statsborger, som havde søgt asyl i Italien mindre end en måned før angrebet. CTA bemærker herudover, at anholdelsesaktionerne i Danmark i februar 2021 omfatter personer med asylbaggrund.

CTA vurderer, at der kan udgå en terrortrussel fra udlændinge på tålt ophold i Danmark, der sympatiserer med militant islamisme. Det er *sandsynligt*, at nogle terrordømte personer på tålt ophold vil etablere nye netværk eller styrke eksisterende netværk med ligesindede med militant islamistiske sympatier.

2.4.7 Militante islamister bosat i andre lande

Der udgår også en terrortrussel mod Danmark fra radikaliserede enkeltpersoner og mindre grupper bosat i andre lande, i første række Danmarks nabolande. Angreb planlagt af personer i ét land rettet mod mål i et andet kan være særligt vanskelige for myndighederne at afdække og afværge.

CTA vurderer, at der kan udgå en trussel fra personer med eller uden tilknytning til Danmark, som er udrejst til konfliktzonen i Syrien/Irak og returneret til andre lande end Danmark, og fra radikaliserede løsladte i udlandet. Der løslades i de kommende år et stort antal terrordømte i andre europæiske lande, som efter løsladelse vil være i stand til at rejse til Danmark. CTA vurderer, at den væsentligste faktor for angrebsplanlægning mod mål i Danmark fra personer bosat i udlandet er eksponering af aktuelle og historiske sager i Danmark om opfattede krænkelser af islam, og særligt når sådanne sager eksponeres i væsentlig grad i militant islamistisk propaganda og i militant islamistiske virtuelle fællesskaber.

CTA har kendskab til fem sager i de seneste ti år – senest en sag fra 2016 – hvor personer bosat i Vesten er rejst til Danmark for at forberede og gennemføre terrorangreb. I fire af sagerne ville gerningspersonerne angribe mål med relation til den danske tegningesag, mens angrebsmålet er ukendt i den såkaldte tændstikssag fra 2016. Antallet af denne type sager i Danmark er højere end i andre europæiske lande, hvilket CTA vurderer, primært skyldes tegningesagen og tilstedeværelsen af mål i Danmark, som har haft en central rolle i sagen.

2.4.8 Finansiering i Danmark af militant islamistiske terrorgrupper i udlandet

Terrorfinansiering er med til at opretholde terrorgrupper og fremme deres virke. Tilførsel af finansielle ressourcer forbedrer terrorgruppers mulighed for at udføre operationer og rekruttere og fastholde medlemmer.

CTA vurderer, at terrorfinansiering fra personer i Danmark til militant islamistiske terrorgrupper primært tilgår grupper i Syrien, Irak, Somalia, Libanon, Afghanistan samt Palæstina.

Det er CTA's vurdering, at intentionen blandt personer i Danmark om at yde finansiering til militant islamistiske grupper ikke er aftaget. Samtidig er viden om metoder til at anskaffe penge ved økonomisk kriminalitet og måder at overføre penge eller andre formuegoder til terrorgrupper fortsat udbredt i specifikke islamistiske netværk i Danmark. Netværkenes vidt forgrenede karakter øger sandsynligheden for, at omfanget af terrorfinansiering i fremtiden kan stige.

Der er i 2020 faldet dom i landsretten i den såkaldte dronesag, hvor tre tiltalte fik fængselsstraffe på henholdsvis otte år, fire år og seks måneder samt tre år. For den ene tiltaltes vedkommende fandt landsretten, at indkøb og facilitering af termiske kameraer til IS udgjorde medvirken til terror. Sagen er ikke en typisk terrorfinansieringssag, men illustrerer det forhold, at ikke kun penge, men også anskaffelse, facilitering og overdragelse af andre formuegoder, kan bruges af sympatisører til at understøtte terrorgrupper i udlandet.

2.5 Terrortruslen fra militante islamister mod danskere og danske interesser i udlandet

CTA vurderer overordnet, at militant islamistiske grupper i en række lande fortsat har intention om at angribe vestlige personer og mål – herunder danske – uden for Vesten.

CTA har ikke kendskab til, at der i 2020 er gennemført eller forsøgt gennemført terrorangreb mod danskere eller mod danske interesser i lande uden for Vesten. CTA har i 2020 kendskab til mindst fire gennemførte militant islamistiske terrorangreb mod vestlige civile personer eller interesser i lande uden for Vesten.

Vestlige personer og mål er generelt godt beskyttede og dermed svært tilgængelige mål i lande med et højt terrortrusselsniveau. Det relativt begrænsede antal angreb mod vestlige personer i 2020 kan tillige være påvirket af, at covid-19-pandemien medførte lavere global rejseaktivitet og dermed mindre tilstedeværelse af vestlige personer i lande uden for Vesten.

Terrortruslen retter sig både mod beskyttede mål, såsom diplomatiske repræsentationer, og ubeskyttede

mål, såsom virksomheder, NGO'er og turister. Danskere kan i lighed med andre vestlige personer blive tilfældige ofre for angreb, der rettes mod vestlige interesser. Danskere i udlandet risikerer herudover at blive ofre for angreb, hvis de befinder sig i nærheden af lokale terrormål, såsom store menneskemængder, kirker eller visse myndighedsbygninger.

CTA vurderer generelt, at danske diplomatiske repræsentationer og anden dansk tilstedeværelse i udlandet, herunder ansatte i danske virksomheder, vil kunne blive opfattet som symbolmål, der giver mulighed for at ramme Danmark uden at foretage angreb i Danmark. Det er muligt, at danske diplomatiske repræsentationer kan blive mål for terrorangreb, hvis de opfattes som mindre sikrede end andre vestlige landes repræsentationer.

CTA vurderer, at det generelle terrortrusselsniveau er højest i lande og regioner, hvor AQ og IS har afdelinger og netværk, og hvor de kan træne og planlægge angreb. Dette gælder især i Syrien og Irak samt i Afghanistan, men også i lande i det vestlige og østlige Afrika, hvor militant islamistiske terrorgrupper i 2020 jævnligt har udført angreb mod lokalbefolkning og myndigheder. I Sydasien og Sydøstasien har der i 2020 være indikationer på fortsat stigende tilslutning til militant islamisme. CTA vurderer, at øget tilslutning til IS i Sydasien og Sydøstasien vil kunne medføre, at lokale militant islamistiske grupper i de enkelte lande i stigende grad får fokus på også at angribe vestlige personer og interesser.

CTA vurderer, at truslen fra militant islamistisk bortførelse er størst i konfliktzoner og disses nærområder. CTA vurderer tillige, at danskere som udgangspunkt ikke er mere udsatte for bortførelse end andre vestlige personer[7].

Tegningesagen er ikke glemt i militant islamistiske kredse, og Danmarks ry som krænkelsesnation kan hurtigt blive bragt op internationalt, hvorved truslen mod danskere og danske interesser i udlandet vil kunne udvikle sig i negativ retning. I efteråret 2020 medførte partiet Stram Kurs' koranafbrændinger i Sverige og andre lande således en vis international omtale. Det internationale fokus på opfattede krænkelser tog for alvor til i omfang efter Charlie Hebdos genoptrykning af egne og danske muhammedtegninger i september 2020. Langt størstedelen af omtalen var rettet mod Frankrig.

Hændelserne i Sverige og især i Frankrig førte også til, at Danmark blev omtalt i militant islamistisk propaganda. CTA vurderer, at omtalen af Danmark i militant islamistisk propaganda vil kunne skærpe lokale militant islamistiske gruppers fokus på Danmark som et legitimt mål, og at dette kan øge truslen mod danskere og danske interesser i konkrete lande og regioner.

CTA vurderer, at covid-19-pandemien ikke har ændret militante islamisters intention om og kapacitet til at begå terror mod danske interesser i udlandet. CTA vurderer, at covid-19-pandemien formentlig har gjort det vanskeligere for militant islamistiske grupper at angribe danskere og danske interesser i udlandet.

CTA vurderer, at nogle terrorgrupper i udlandet på længere sigt vil kunne drage fordel af pandemien og dens afledte økonomiske og sociale virkninger, og at den generelle terrortrussel mod vestlige, herunder danske, interesser på den baggrund kan blive forøget. Fx vil covid-19-pandemien kunne svække og destabilisere en række lande i Mellemøsten, Afrika og Asien, hvilket kan føre til en nedprioritering af forebyggelse og bekæmpelse af terrorisme.

7. Det er muligt at holde sig orienteret om særlige landerisici i Udenrigsministeriets rejsevejledning på www.um.dk

Højreekstremisme

er en fællesbetegnelse for forskellige politiske holdninger, der ligger yderst til højre i det politiske spektrum, og som kendetegnes ved kombinationer af nationalistiske, autoritære, anarkistiske, antiparlamentariske, racistiske, xenofobiske og antisemitiske standpunkter. Det ideologiske grundlag for højreekstremisme kan stamme fra nazisme, fascisme såvel som nationalkonservatisme. Højreekstremister sætter spørgsmålstegn ved eller afviser demokrati og anser anvendelse af vold som et legitimt middel til at opnå politiske mål.

3. TERRORTRUSLEN MOD DANMARK FRA HØJREEKSTREMISTER

CTA vurderer, at terrortruslen fra højreekstremister mod Danmark er i niveauet generel. Det betyder i henhold til PET's definitioner, at der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.

CTA vurderer, at det mest sandsynlige højreekstremistiske terrorangreb i Danmark er et angreb, der udføres af en soloterrorist eller en mindre gruppe, der befinder sig i periferien af eller uden for et højreekstremistisk miljø. I forlængelse heraf vurderer CTA, at der kan udgå en trussel fra bl.a. sårbare personer, der finder identitet, inspiration og fællesskab i højreekstremistiske virtuelle miljøer. Det er *mindre sandsynligt,* at en højreekstremistisk terrortrussel i Danmark vil udgå direkte fra de organiserede fysiske grupper og organisationer. CTA bemærker dog, at danske højreekstremistiske gruppers aktioner, som ikke har karakter af terror, kan virke utryghedsskabende. Eksempelvis har der i de senere år været en række antisemitiske aktioner i Danmark, bl.a. begik højreekstremister i november 2019 groft hærværk og gravskænding af jødiske symboler og grave[8].

CTA vurderer, at nedlukningen af samfundet under covid-19-pandemien og den deraf følgende isolation i nogle tilfælde kan have øget forbruget af højreekstremistisk propaganda på internettet, ligesom den kan have styrket eksisterende konspirationsteorier og antistatslige narrativer. Det er CTA's vurdering, at covid-19 overordnet set ikke har påvirket trusselsniveauet fra højreekstremister i Danmark. Det er *muligt*, at covid-19 vil kunne få betydning for det højreekstremistiske trusselsbillede inden for det kommende år.

3.1 Udviklingen i truslen og narrativer

3.1.1 Udviklingen i det globale trusselsbillede for højreekstremisme

En række myndigheder i Vesten har de seneste år vurderet, at truslen fra højreekstremister er øget. Dette skyldes bl.a. en række voldsomme højreekstremistiske angreb i 2019, herunder et angreb på to moskéer i Christchurch, New Zealand, i marts 2019. I 2020 har CTA registreret et fald i antallet af gennemførte og afværgede højreekstremistiske angreb i Vesten sammenlignet med 2019. CTA registrerede 12 gennemførte og syv afværgede højreekstremistiske angreb i Vesten i 2019, mens de tilsvarende tal for 2020 er to gennemførte og syv afværgede angreb[9]. Det er sandsynligt, at nedgangen i antallet af angreb i Vesten i 2020 skyldes et større fokus på højreekstremisme fra myndighedernes side, men den generelle nedlukning af samfundet i forbindelse med covid-19 kan også have virket dæmpende på det højreekstremistiske aktivitetsniveau i det fysiske rum i 2020, herunder planlægning og gennemførelse af angreb. CTA vurderer, at angrebet i Christchurch i 2019 blev katalysator for flere efterfølgende copycat-angreb samme år. Der har i 2020 ikke været højreekstremistiske angreb, der på tilsvarende måde har kunnet anspore højreekstremister til at udføre lignende inspirerede angreb.

Truslen fra højreekstremister i Vesten udgår fra et bredt spektrum af organisationer, grupper og individer, der henter inspiration fra forskellige politiske og ideologiske dagsordner, herunder konspirationsteorier. Det ideologiske grundlag for højreekstremisme kan stamme fra eksempelvis nazisme, fascisme eller nationalkonservatisme, men forskellige konspirationsteorier ses som stadig mere fremtrædende drivkræfter blandt højreekstremister i Vesten.

Mens militante islamister ofte inspireres af internationale organisationer som AQ og IS, findes der ikke fysiske højreekstremistiske organisationer, der på tilsvarende måde evner at samle og inspirere internationalt på tværs af nationale og kulturelle skel.

CTA vurderer, at truslen fra højreekstremister i første række ikke udspringer fra de etablerede fysiske organisationer, men derimod fra soloterrorister eller mindre grupper af højreekstremister. Ifølge CTA's oversigt over højreekstremistiske angreb i Vesten blev 12 ud af de 14 gennemførte højreekstremistiske angreb i 2019 og 2020 udført af soloterrorister. Ingen af disse angreb var

8. To danske højreekstremister blev dømt i sagen.
9. Det skal bemærkes, at opgørelser over antallet af afværgede og gennemførte højreekstremistiske terrorangreb i Vesten kan variere afhængigt af opgørelsesmetode og tilgængelige oplysninger.

dirigeret af en terrorgruppe, og ingen af gerningspersonerne var på angrebstidspunktet tilknyttet fysiske højreekstremistiske organisationer eller grupper.

CTA vurderer, at truslen fra højreekstremister i Vesten i det kommende år i særlig grad udgår fra personer og mindre grupper, der fortrinsvis mødes, radikaliseres og inspireres i højreekstremistiske virtuelle fællesskaber og netværk. I de vestlige lande ses en stigende tendens til internationalisering af højreekstremistiske narrativer gennem deling og forbrug af højreekstremistisk propaganda samt gennem transatlantiske og europæiske virtuelle fællesskaber. CTA vurderer, at denne øgede internationale udveksling af propaganda og ekstremistiske synspunkter kan øge truslen fra højreekstremisme i Danmark.

3.1.2 Supranationale narrativer

Blandt højreekstremister både internationalt og i Danmark findes der supranationale narrativer, der understøtter, fastholder og i nogle tilfælde kan udgøre hele fundamentet for deres højreekstremistiske ideologi og verdensbillede. Der er forskel på, i hvilken grad højreekstremistiske narrativer baserer sig på en højreekstrem opfattelse af verificerbare oplysninger, fx om indvandring og islam, eller på stærkt tvivlsomme eller ikke-verificerbare oplysninger, hvorved de antager karakter af konspirationsteorier.

Et af de mest udbredte og centrale højreekstremistiske narrativer er teorien om "Den Store Udskiftning". Narrativet angiver, at Europas oprindelige befolkning bliver udskiftet med indvandrere fra ikke-vestlige lande, hvilket primært skyldes indvandring som følge af opfattet lempelig asyl- og indvandringspolitik, indvandreres højere fødselsrate samt europæiske befolkningers tilsvarende lave reproduktion. Narrativet findes også i en konspirationsteoretisk form, hvor en politisk og økonomisk elite, bestående af eksempelvis indvandringsvenlige politiske partier, EU, FN og store virksomheder, anses for at arbejde intentionelt og målrettet for befolkningsudskiftningen via tilskyndet massiv indvandring. Den Store Udskiftning er både titlen på og det bærende budskab i det manifest, som gerningsmanden bag angrebet i Christchurch udsendte kort tid inden sit angreb i 2019. CTA vurderer, at Den Store Udskiftning er et af de mest fremherskende narrativer blandt højreekstremister globalt, og at det er udbredt blandt både danske højreradikale og højreekstremister.

Et narrativ med betydelig lighed med "Den Store Udskiftning" er konspirationsteorien "White Genocide" (Hvidt Folkemord), der angiver, at hvide befolkninger i Vesten mindskes og uddør som følge af indvandring, lav fødselsrate samt vold mod og mord på hvide personer begået af indvandrere. Narrativet adskiller sig imidlertid ved oftest at være antisemitisk i sit udgangspunkt, idet det hævder, at en jødisk sammensværgelse står bag og kontrollerer udviklingen med henblik på at udrydde den hvide race. Dette narrativ har i sagens natur størst tilslutning blandt antisemitiske højreekstremister og promoveres bl.a. eksplicit af Nordisk Modstandsbevægelse (NMB) i Danmark.

Beslægtet med Hvidt Folkemord er den antisemitiske konspirationsteori ZOG, der er en forkortelse for "Zionist Occupied Government" (zionistisk- eller jødisk-besat regering), der hævder, at jøder kontrollerer vestlige regeringer, bl.a. via deres påståede ejerskab af og totale kontrol med bankerne og det finansielle system.

CTA vurderer, at højreekstremistiske narrativer kan være med til både at styrke eksisterende samt skabe nye højreekstremistiske fjendebilleder og derfor kan have betydning for, hvilke mål den højreekstremistiske terrortrussel retter sig imod. Herudover kan de have en både mobiliserende og samlende effekt i højreekstremistiske miljøer, herunder også i Danmark. CTA vurderer ydermere, at højreekstremistiske narrativer fortsat er meget udbredte og aktuelt når et stort publikum via distribution i virtuelle fællesskaber og på sociale medier.

3.1.3 Højreekstremisters virtuelle fællesskaber og brug af internettet

Danske højreekstremister og højreekstremistiske grupper internationalt anvender en række forskellige virtuelle fællesskaber til at kommunikere med ligesindede,

spredning af propaganda, opbygning af kapacitet samt radikalisering og rekruttering. Alt imens store, kommercielle virtuelle platforme som Facebook, Twitter, YouTube og Reddit samt dedikerede højreekstremistiske hjemmesider og fora stadigvæk benyttes til disse formål, har øget opmærksomhed på ekstremistisk indhold fra udbydere og myndigheder gjort sådanne aktiviteter vanskeligere.

Foto: Patrick Hertzog, AFP, Ritzau Scanpix

Grundet denne opmærksomhed migrerer en del højreekstremister til, hvad de anser som mere sikre platforme, eksempelvis image boards som 4chan og 8kun, der er yndede samlingssteder for højreekstremister på grund af deres begrænsede moderation, og fordi de tilbyder brugerne en høj grad af anonymitet. Herudover anvendes også sociale medier med begrænset moderation, eksempelvis det russiske VK, videotjenesten BitChute samt de amerikanske Twitter-kloner GAB og Parler. Krypterede, internetbaserede kommunikationsplatforme har ligeledes vundet indpas som eksempelvis Telegram, der har opnået stor popularitet blandt højreekstremister, mens gaming-platforme som de digitale distributions- og chattjenester Discord og Steam og live streamingtjenesten Twitch ligeledes benyttes.

Det er *sandsynligt*, at højreekstremister internationalt og i Danmark vil fortsætte og øge brugen af virtuelle fællesskaber, idet disse tillader, at man særdeles hurtigt og med få ressourcer kan dele højreekstremistiske budskaber og propaganda med et meget stort publikum på tværs af grænser.

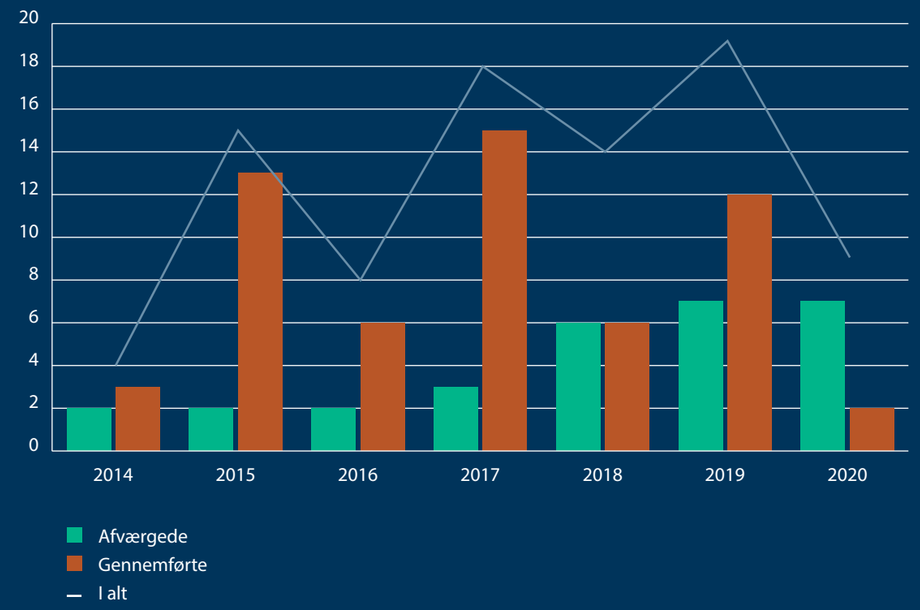
Højreekstremisters anvendelse af virtuelle fællesskaber har udviklet sig til at inkludere en række nye platforme. Det er *meget sandsynligt*, at især yngre og teknologisk kyndige højreekstremister fortsat vil søge og benytte sådanne nye platforme, og at denne udvikling vil fortsætte, også blandt højreekstremister i Danmark.

3.1.4 Danske højreekstremisters internationale kontakter

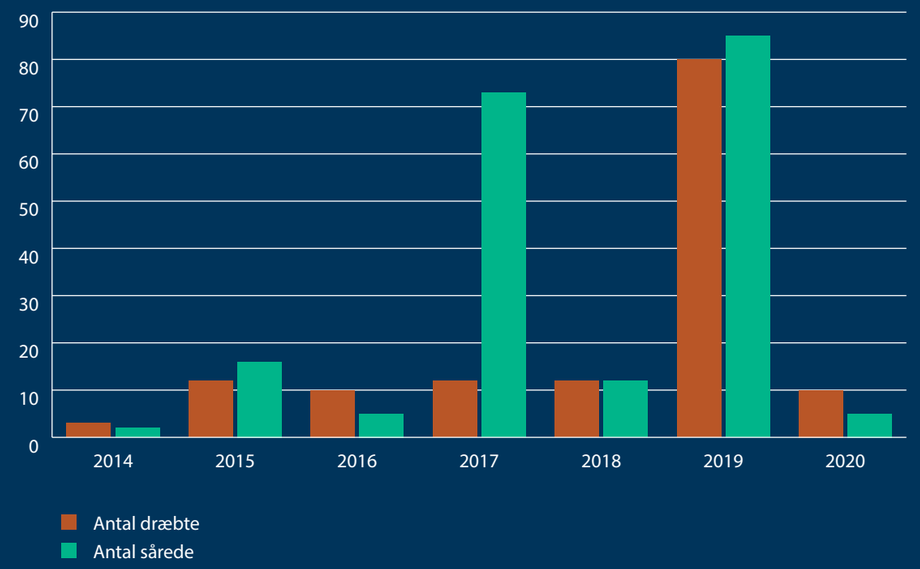
CTA vurderer, at danske højreekstremisters internationale kontakter kan medvirke til at skabe og opretholde netværk, der kan være medvirkende til at radikalisere danske højreekstremister og mobilisere til deltagelse i højreekstremistiske aktiviteter. De udenlandske kontakter kan påvirke og udvikle fjendebilleder og narrativer og kan desuden styrke kapacitetsopbygningen blandt danske højreekstremister.

CTA vurderer, at covid-19-pandemien har begrænset den fysiske mødeaktivitet for højreekstremister på tværs af landegrænser, men de internationale kontakter er vedligeholdt og styrket i det virtuelle rum.

Figur 5: Antallet af afværgede og gennemførte højreekstremistiske terrorangreb i Vesten fra 2014 til og med 2020



Figur 6: Antal dræbte og sårede ved højreekstremistiske terrorangreb i Vesten fra 2014 til og med 2020



Definitioner på højreekstremistiske måltyper

CTA vurderer, at der for højreekstremisters måludvælgelse kan skelnes mellem symbolmål og civile mål.

Symbolmål

***Muslimske mål**: Moskéer og andre muslimske samlingssteder samt arrangementer på muslimske fest- og helligdage, muslimske skoler, klubber og butikker, der frekventeres af muslimer.*

***Migrationsmål**: Asylansøgere, asylcentre, anerkendte flygtninge, migranter og andre personer, der grundet etniske og kulturelle markører som hudfarve og sprog kan opfattes som værende migranter.*

***Jødiske mål**: Synagoger, jødiske tilholdssteder og institutioner, som fx skoler, samt andre mål, hvis tilknytning til jødedommen er identificerbar, samt arrangementer på jødiske fest- og helligdage. Jødiske mål omfatter tillige personer, der opfattes som jøder, israelske interesser i Danmark, herunder diplomatiske repræsentationer, virksomheder og turister.*

***Racistiske mål**: Personer, der ud fra etniske markører, fx hudfarve, udpeges som et terrormål.*

***Myndighedsmål**: Myndigheder, herunder visse ministerier, politi, militær, redningsberedskab, andre offentlige institutioner samt repræsentanter for sådanne myndigheder. Myndighedsmål kan også omfatte diplomatiske repræsentationer.*

***Politiske repræsentanter**: Folkevalgte, ministre og andre personer, begivenheder og lokaliteter med tilknytning til visse politiske partier og bevægelser.*

***Andre opfattede politiske modstandere**: Personer, begivenheder og lokaliteter, der opfattes som eller repræsenterer politiske modstandere, og som ikke er myndighedsmål eller politiske repræsentanter.*

***LGBTQ+-mål**: Personer, der erklærer sig eller kan opfattes som bl.a. homoseksuelle, queer, biseksuelle og transpersoner.*

Civile mål

Andre personer, som ikke udgør et symbolmål. Eksempelvis forsamlinger af tilfældige personer på en offentlig plads, ved et arrangement eller et andet befærdet sted.

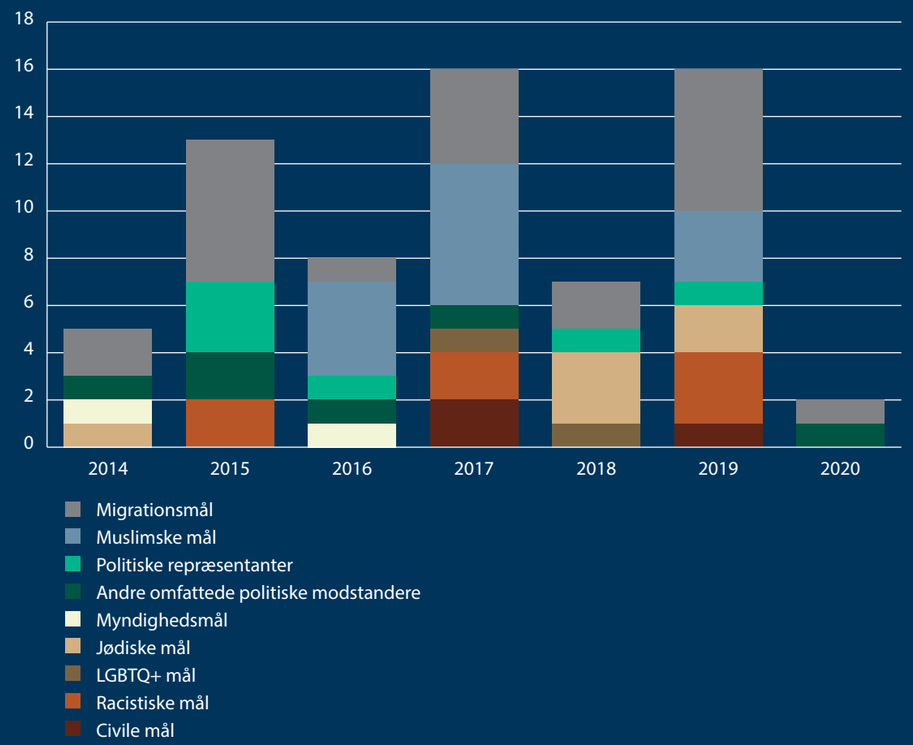
3.2 Terrormål og fremgangsmåder i Danmark for højreekstremister

3.2.1 Mål

De mest sandsynlige mål for et højreekstremistisk terrorangreb i Danmark er muslimske mål, migrationsmål, jødiske mål, personer af anden etnisk oprindelse end dansk samt lokaliteter, hvor sådanne personer opfattes at samles. Andre mulige mål er visse opfattede politiske modstandere. Herudover er myndigheder og LGBTQ+-personer også mulige mål.

CTA vurderer, at antistatslig retorik har vundet større indpas blandt danske højreekstremister i 2020. Det er *sandsynligt*, at covid-19-pandemien har medvirket til at forstærke eksisterende antistatslige narrativer blandt højreekstremister i Danmark, ligesom det er muligt, at danske højreekstremister er blevet inspireret af amerikanske eller tyske højreekstremister, der ofte udviser og deler stærke antistatslige holdninger. CTA vurderer samtidig, at det øgede antistatslige fokus kan have betydning for danske højreekstremisters måludvælgelse.

Figur 7: Terrormål ved højreekstremistiske angreb i Vesten fra 2014 til og med 2020 (et angreb kan have flere mål)

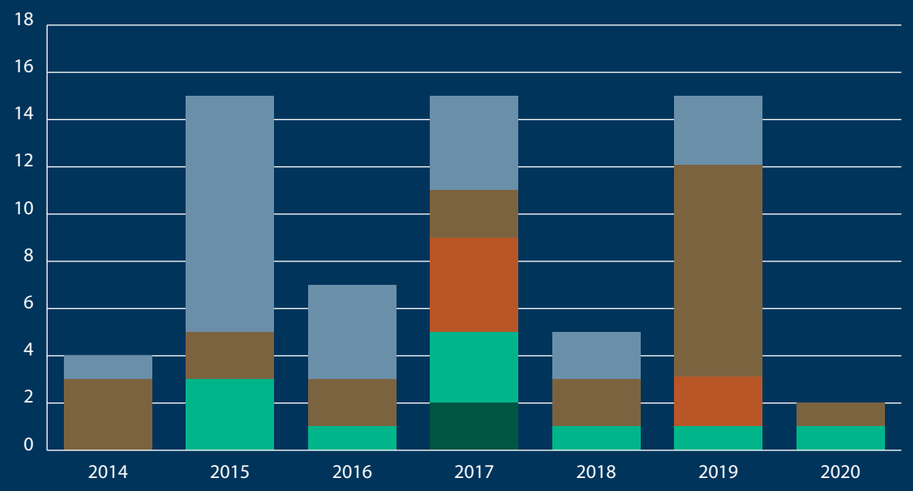


CTA vurderer, at konspiratoriske forestillinger ses vinde indpas i højreekstremistiske kredse i Danmark. Til de højreekstremistiske konspiratoriske narrativer knytter sig ofte antisemitiske budskaber, hvilket kan skyldes, at de toneangivende og mest aktive højreekstremister i Danmark har en nationalsocialistisk ideologi. CTA vurderer, at konspiratoriske narrativer blandt danske højreekstremister kan forstærke eksisterende fjendebilleder.

3.2.2 Fremgangsmåde[10]

De mest sandsynlige våben ved et højreekstremistisk terrorangreb i Danmark er blank- eller stikvåben og lette skydevåben, herunder særligt jagtrifler, haglgeværer, pistoler og hjemmelavede skydevåben. Andre mulige våben inkluderer ildspåsættelse, hjemmelavede bomber og køretøjer. CTA vurderer ydermere, at højreekstremister kan opbygge kapacitet til at anvende våben, herunder skydevåben og sprængstoffer via deling af viden i virtuelle fællesskaber samt instruktioner på hjemmesider, særligt videoer på YouTube.

Figur 8. : Våben anvendt ved højreekstremistiske terrorangreb i Vesten fra 2014 til og med 2020 (et angreb kan involvere flere våbentyper)



10. For yderligere uddybning af kapaciteten til terrorisme i Danmark, se bilag.

4. TERRORTRUSLEN MOD DANMARK FRA VENSTREEKSTREMISTER

CTA vurderer, at terrortruslen fra venstreekstremister i Danmark er i niveauet begrænset. Det betyder i henhold til PET's definitioner, at der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. CTA vurderer, at danske venstreekstremister er voldsparate og samtidigt besidder en begrænset, men dog eksisterende, kapacitet til at begå terror. Samtidig har deres intention om at begå politisk motiveret vold, som kan have karakter af terrorisme, været nedadgående og er aktuelt meget lav.

Danske venstreekstremisters primære mål er at eksponere, imødegå og bekæmpe opfattet racisme og fascisme, særligt som det kommer til udtryk hos højreradikale og højreekstremistiske grupper. CTA vurderer, at det mest sandsynlige mål for et venstreekstremistisk terrorangreb er højreekstremistiske aktiviteter samt repræsentanter for myndigheder, først og fremmest politiet. CTA vurderer dog, at truslen mod politiet i høj grad er situationsbestemt og primært er forbundet med sammenstød med venstreekstremister i forbindelse med aktioner, demonstrationer og husbesættelser. Andre mulige mål er enkeltpersoner med opfattet sympati for højreekstremisme samt i mindre grad visse politikere og offentligt kendte personer, der opfattes som politiske modstandere, eksempelvis kunstnere og debattører.

CTA vurderer, at højreekstremistiske angreb i Danmark kan inspirere en voldelig modreaktion fra danske venstreekstremister.

Det mest sandsynlige venstreekstremistiske terrorangreb i Danmark er et angreb, der udføres af en mindre gruppe, som er medlemmer af eller har kontakt til en dansk venstreekstremistisk gruppe.

De mest sandsynlige våben, der kan tages i anvendelse ved et venstreekstremistisk terrorangreb i Danmark er slag- og blankvåben, brandstiftende anordninger som molotovcocktails samt fyrværkeri, herunder kraftige kanonslag, krysantemumbomber, bomberør og raketter. Herudover er ildspåsættelse et andet muligt våben, der især kan tages i brug i forbindelse med demonstrationer og aktioner. CTA vurderer det som *mindre sandsynligt*, at danske venstreekstremister vil anvende hjemmelavede bomber, samt usandsynligt, at de vil anvende skydevåben[11].

Der findes en række virtuelle fællesskaber, hvor danske venstreekstremister kommunikerer og deler information. Via disse virtuelle fællesskaber er danske venstreekstremister i stand til relativt hurtigt at mobilisere støtter til eksempelvis deltagelse i venstreekstremistiske arrangementer og begivenheder, herunder personer, der ellers kun har begrænset kontakt til de venstreekstremistiske miljøer.

Danske venstreekstremistiske grupper indgår i samarbejde med ligesindede internationale organisationer og grupper. Det er *sandsynligt*, at samarbejde med internationale venstreekstremistiske organisationer og grupper kan opbygge kapacitet hos danske venstreekstremister, herunder konkret taktisk viden, der kan anvendes i forbindelse med voldsanvendelse. CTA vurderer herudover, at samarbejde med meget voldsparate internationale venstreekstremistiske miljøer kan øge radikalisering og voldsparathed hos danske venstreekstremister. Ydermere kan samarbejdet give mulighed for at skabe kontakt til og mobilisere voldsparate udenlandske venstreekstremister til deltagelse i venstreekstremistiske begivenheder i Danmark, hvilket kan øge terrortruslen.

11. For yderligere uddybning af kapaciteten til terrorisme i Danmark se bilag.

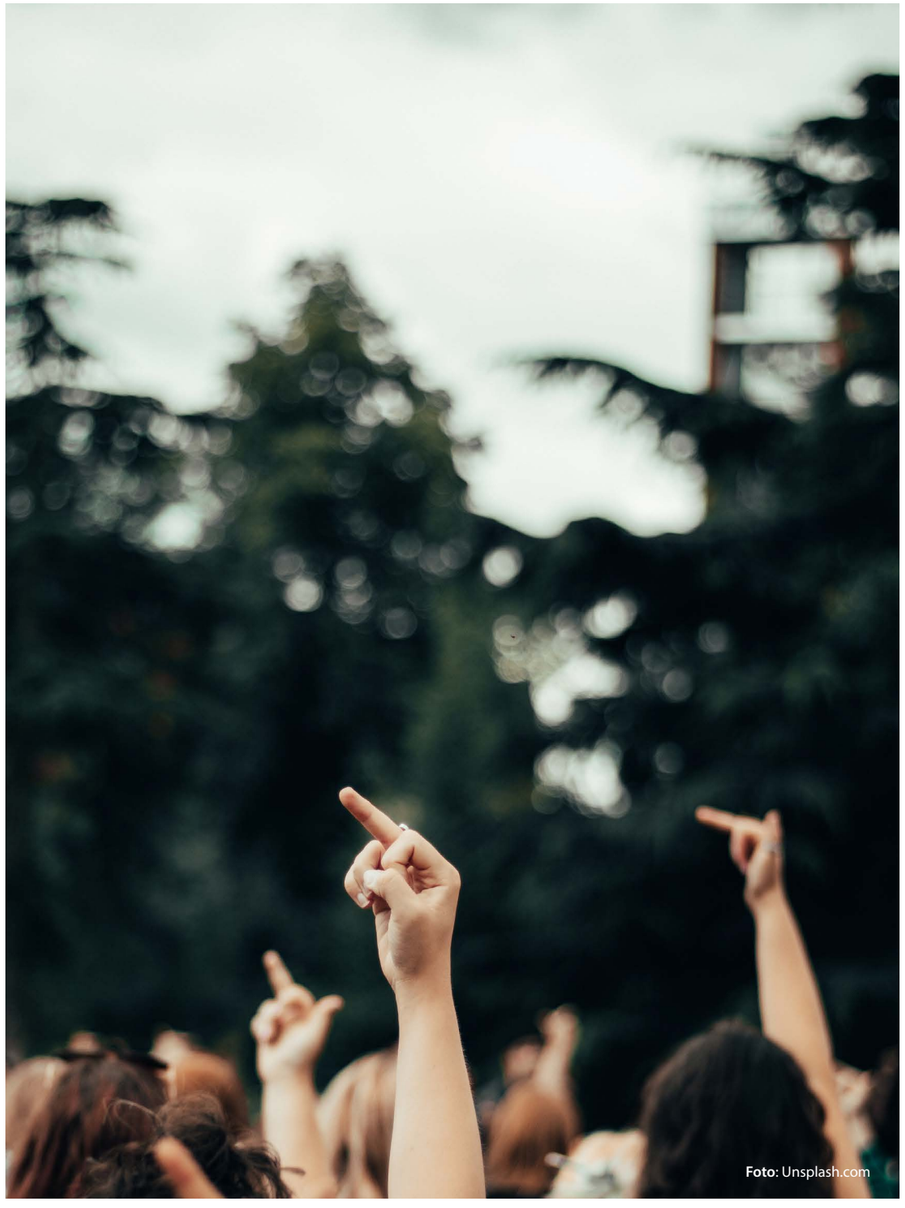


Foto: Unsplash.com

5. ANDRE TRUSLER, DER KAN HAVE KARAKTER AF TERRORISME

Dette kapitel beskriver udviklingen inden for andre fænomener end militant islamisme, højreekstremisme og venstreekstremisme, som CTA vurderer kan have betydning for terrortruslen mod Danmark. Kapitlet beskriver visse konspirationsteorier, incels, klimaekstremisme, suverænitetsbevægelser samt personer med psykiske problemstillinger, som kan inspirere til handlinger, der efter en konkret juridisk vurdering kan have karakter af terrorisme. Det skal understreges, at sådanne forhold alene har PET's interesse såfremt personer legitimerer anvendelse af vold for at opnå politiske, religiøse eller ideologiske mål.

Herudover kan politiske, etniske og religiøse konflikter i udlandet føre til reaktioner fra personer eller grupper med tilknytning til de berørte grupper i Danmark, som kan udvikle sig til handlinger, der har karakter af terror. Sådanne handlinger kan involvere statslige aktører. De konkrete reaktioner, herunder voldelige protester, vil bl.a. kunne blive rettet mod politikere, myndighedsrepræsentanter, tilfældige borgere eller andre landes diplomatiske repræsentationer i Danmark.

Foto: Anthon Unger, Ritzau Scanpix

5.1 Konspirationsteorier

Konspirationsteorier er forsøg på at forklare begivenheder og omstændigheder med grundløse påstande om bagvedliggende hemmelige sammensværgelser mellem magtfulde aktører. De, der tror på konspirationsteorier, vil ofte bestride betegnelsen, idet den har en nedsættende klang.

CTA vurderer, at en eventuel øget udbredelse af visse konspirationsteorier bl.a. kan føre til fremsættelse af trusler mod politikere og myndighedsrepræsentanter.

Konspirationsteorier har en relativ snæver appel i Danmark, bl.a. på grund af danskernes generelt høje tillid til myndighederne. Der har dog været en stigende interesse for konspirationsteorier i forbindelse med covid-19-pandemien. Det gælder særligt konspirationsteorier, der tager afsæt i pandemien, fx om myndighedernes håndtering og sundhedsråd eller om 5G-mobilnetværkets opfattede skadelige effekt.

Personer, som er kendt af de danske myndigheder for aktiviteter i de islamistiske miljøer, de politisk ekstremistiske miljøer eller i danske suverænitetsbevægelser, kan også være tilhængere af konspirationsteorier.

Tilhængere af konspirationsteorier mødes primært virtuelt i fora på internettet, herunder eksempelvis på Facebook, Instagram og andre sociale medier. Visse influencere (dvs. personer med mange følgere på deres sociale medier) går forrest i forhold til at fortolke og udbrede budskaberne.

Der er en tendens til, at personer ikke blot interesserer sig for en enkelt konspirationsteori, men oftest for en hel gruppe af overlappende eller undertiden direkte modstridende konspirationsteorier, alternative tanker og ideologier.

Tilhængere af konspirationsteorier er generelt præget af mistillid til politikere, medier og videnskab samt af en frygt for at miste grundlæggende frihedsrettigheder. Visse konspirationsteorier, som fx QAnon[12], har et kernebudskab om en korrupt og moralsk anløben politisk elite, som skal bekæmpes, og dette kan efter CTA's vurdering vække genklang hos personer, der har en dyb mistillid til staten, og som eventuelt har eller har haft uoverensstemmelser med danske myndigheder. En række konspirationsteorier har desuden et tydeligt antisemitisk og/eller islamofobisk islæt.

I flere europæiske lande, herunder Storbritannien og Nederlandene, har 5G-modstandere, der er inspireret af konspirationsteorier om 5G, begået alvorligt hærværk mod 5G-master eller master og anlæg, som opfattes som 5G. I USA har der været flere sager, hvor personer inspireret af QAnon har handlet voldeligt eller planlagt voldelige handlinger, herunder mod myndigheder eller private firmaer og privatpersoner, som har været mistænkeliggjort i forbindelse med konspirationsteorien.

CTA vurderer, at en eventuel øget udbredelse af visse konspirationsteorier, der skærper opfattelsen af politikere og myndighedsrepræsentanter som bl.a. landsforrædere og fjender, kan føre til en stigning i antallet af trusler og en skærpelse af retorikken i disse. Langt de fleste af de trusler, som fremsættes, manifesterer sig ikke i vold eller andre fysiske manifestationer. CTA vurderer dog, at i tilfælde af sådanne handlinger, kan konspirationsteorier have påvirket motivation og måludvælgelse.

12. QAnon er en konspirationsteori, hvor kernefortællingen er, at den tidligere amerikanske præsident Donald Trump i det skjulte bekæmper en international sammensværgelse, som bl.a. tæller fremtrædende politikere og styres af en jødisk elite.

CTA vurderer, at konspirationsteoriernes potentielle indflydelse på terrortruslen primært relaterer sig til personer med tilknytning til politisk ekstremistiske miljøer, herunder særligt højreekstremistiske miljøer.

CTA vurderer, at såfremt konspirationsteorier får større forankring blandt personer i de ekstremistiske miljøer, vil det kunne virke yderligere radikaliserende på personer i ekstremistiske miljøer. Det gælder særligt konspirationsteorier, der fremmer mistillid til myndighederne og udbreder et forenklet sort-hvidt syn på verden, italesætter politikere og myndighedsrepræsentanter som fjender, og som legitimerer voldshandlinger ud fra hensyn til "folket". Sådanne voldelige hændelser kan eksempelvis ske i form af personoverfald, som efter en konkret juridisk vurdering kan have karakter af terror.

5.2 Incels

Incel(s) er et begreb, der er en sammentrækning af forbogstaverne i de engelske ord "involuntary celibate", hvilket betyder en person i ufrivilligt cølibat. Begrebet dækker over personer, i langt overvejende grad mænd, der er frustrerede over ikke at være i stand til at opnå romantiske eller seksuelle forhold til kvinder. De finder ligesindede i en virtuel subkultur, der er repræsenteret på en række forskellige virtuelle platforme, eksempelvis 4chan og 8kun, samt på en række dedikerede hjemmesider og undergrupper på sociale medier. Nogle radikaliserede incels giver på disse platforme udtryk for et markant kvindehad samt had til mænd, der opfattes som havende succes med kvinder.

Mange incels færdes i internationale, virtuelle fællesskaber, der tilbyder brugerne en høj grad af anonymitet. Dette gør det vanskeligt at estimere det samlede antal af radikaliserede brugere.

Særligt kvindehadet har været drivkraft i en række angreb begået af incels i USA og Canada i perioden 2014 til 2020, hvor mange personer er blevet dræbt og såret. CTA vurderer, at det kan være særdeles svært for myndigheder at forudsige hvem og hvor, incels vil angribe. Dette skyldes, at incels har en bred måludvælgelse og vil kunne angribe både kvinder og mænd.

5.3 Klimaekstremister

Klimaekstremister betegner enkeltpersoner og grupper, der er villige til at anvende vold i kampen for en eller flere sager, hvor hensynet til miljøet og det globale klima indgår som et centralt element. Disse grupper står i modsætning til klimaaktivister, der alene gør brug af ikkevoldelige midler, herunder civil ulydighed. Blandt klimaekstremister findes der også personer med sympati for højreekstremisme, herunder de såkaldte økofascister. Der er også en mulighed for, at enkeltpersoner med sympati for venstreekstremisme kan agere voldeligt eksempelvis ved deltagelse i klimaaktioner.

CTA vurderer, at der ikke aktuelt findes klimaekstremistiske grupper i Danmark, som er villige til at anvende vold i kampen for klimaet og miljøet.

Det er *mindre sandsynligt*, at enkeltpersoner eller mindre grupper af personer, der er aktive i klimaaktivistiske grupper og er utilfredse med den ikkevoldelige aktivistiske linje, vil vælge at bryde ud af grupperne for at udøve klimaekstremisme.

5.4 Suverænitetsbevægelser

Suverænitetsbevægelser er bevægelser, der udgøres af løst tilknyttede grupper af varierende størrelse og af enkeltpersoner, og hvis bærende ideologiske fællestræk er, at de ikke anerkender statens og myndighedernes legitimitet og autoritet. Personer, der er en del af suverænitetsbevægelser, er ydermere af den overbevisning, at en person ved at erklære sig suveræn kan melde sig ud og gøre sig uafhængig af det eksisterende samfund og herefter ikke længere er forpligtet til at overholde dets gældende love og regler.

Grundet suverænitetsbevægelsers antistatslige ideologi kan de udgøre en trussel mod myndighederne, herunder særligt politiet. Denne trussel kan særligt komme til udtryk, når personer, der er en del af suverænitetsbevægelser, med vold modsætter sig bl.a. anholdelser.

Suverænitetsbevægelsers ideologi kan virke appellerende for eksempelvis kriminelle eller andre personer, der har eller har haft uoverensstemmelser med myndighederne, særligt politiet. Sådanne personer kan have en øget voldsparathed samt have lettere adgang til våben, hvilket kan øge truslen særligt i forbindelse med konfrontationer med politifolk.

CTA vurderer, at såfremt suverænitetsbevægelsers ideologi får større forankring blandt personer i Danmark, kan det øge sandsynligheden for, at suverænitetsbevægelser vil kunne komme til at udgøre en terrortrussel.

5.5 Personer med psykiske problemstillinger

Tilstedeværelsen af psykiske lidelser hos en gerningsperson kan gøre det vanskeligt for myndighederne at vurdere, hvorvidt personens voldelige handlinger udgør terror. Der kan i visse situationer være grund til at rette særlig opmærksomhed mod personer med psykiske lidelser, der udviser tegn på radikalisering og som tidligere har udvist voldelig adfærd eller impulsive handlinger. En psykisk lidelse er ikke nødvendigvis udslagsgivende for en persons evne og vilje til at begå terror, men alene én af flere faktorer, der skal inddrages i en vurdering af den terrortrussel, der eventuelt udgår fra den pågældende person. Det skal bemærkes, at psykiske lidelser typisk forekommer i samspil med andre risikofaktorer, såsom social isolation, marginalisering, arbejdsløshed og signifikante livsændringer. CTA vurderer, at en persons mentale tilstand, herunder psykiske lidelser, kan have stor betydning for dennes adfærd og motivation til at handle, herunder også i forbindelse med terror.

CTA's oplysninger indikerer en tendens til, at gerningspersoner med en psykiatrisk diagnose eller symptomer på en ikke-diagnosticeret psykisk lidelse ofte begår terrorangreb på egen hånd frem for i en gruppe.

Sociale medier anvendes i stigende grad til at fremsætte truende ytringer, bl.a. imod offentlige personer, og til at sprede rygter og falske nyheder. Mens langt størstedelen af disse ytringer ikke fører til konkret angrebsplanlægning, vurderer CTA, at sådanne tilkendegivelser kan påvirke visse psykisk uligevægtige eller meget påvirkelige personer til at begå ideologisk motiveret vold, der kan have karakter af terror.

6. TERRORTRUSLEN MOD GRØNLAND OG FÆRØERNE

CTA har ændret betegnelsen for terrortrusselsniveauskalaens laveste niveau fra "ingen" til "minimal". På baggrund af denne præcisering indplaceres henholdsvis Grønland og Færøerne i trusselsniveauet "minimal" frem for "begrænset", uden at dette afspejler en ændring i truslens karakter.

Foto: Færøerne, Unsplash.com

6.1. Særligt vedrørende terrortruslen mod Grønland

Terrortruslen mod Grønland er minimal. Det betyder i henhold til PET's definitioner, at der ikke er nogen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

CTA vurderer, at militant islamisme er mindre udbredt i Grønland end i Danmark.

Militant islamistisk eller politisk ekstremistisk propaganda kan dog også påvirke personer i Grønland til at begå voldelige handlinger. Socialt marginaliserede og sårbare unge kan være særligt modtagelige over for radikalisering.

CTA vurderer, at den nemmere adgang til våben og sprængstoffer i Grønland sammenlignet med det øvrige rigsfællesskab vil kunne øge muligheden for at gennemføre angreb med stor skadevoldende effekt.

6.2. Særligt vedrørende terrortruslen mod Færøerne

Terrortruslen mod Færøerne er minimal. Det betyder i henhold til PET's definitioner, at der ikke er nogen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

Som i Grønland er militant islamisme mindre udbredt på Færøerne end i Danmark.

Militant islamistisk eller politisk ekstremistisk propaganda kan påvirke personer på Færøerne eller tilrejsende til at begå voldelige handlinger. Dette kan være udløst af politiske enkeltsager som fx dyrevelfærd. Socialt marginaliserede og sårbare unge kan være særligt modtagelige over for radikalisering.

BILAG: FREMGANGSMÅDER VED TERRORANGREB I DANMARK

Valg af fremgangsmåde ved et terrorangreb er ofte en afspejling af den kapacitet, der er til stede hos en gerningsperson. Fremgangsmåder kan ligeledes have en indvirkning på antal sårede og dræbte og i forhold til den propagandaeffekt, som et angreb medfører. I det følgende gennemgås den overordnede kapacitet, som potentielle gerningspersoner i Danmark vurderes at kunne anvende. Inden for de enkelte kategorier af potentielle gerningspersoner kan der være forskelle i forhold til kapacitet, fokus og præferencer, hvilket har betydning for valget af fremgangsmåde[13].

CTA vurderer, at valget af fremgangsmåde påvirkes af en række forhold, herunder fokus i propaganda og på virtuelle platforme, den enkeltes evner og adgang til ressourcer, adgangen til det påtænkte mål samt inspiration fra andre angreb.

Terrortruslen i Vesten udspringer i stigende grad fra personer uden fysisk tilknytning til etablerede grupper. Dette gør sig gældende for både militante islamister og højreekstremister. I Danmark kan kapaciteten hos mulige gerningspersoner bl.a. øges via virtuelle netværk, hvor ressourcepersoner deler instruktioner og giver specifik rådgivning om konkrete fremgangsmåder.

Kapaciteten kan ligeledes øges ved rekruttering eller radikalisering af nøglepersoner, der har legal adgang til faciliteter, ressourcer eller information. Sådanne insidere kan have forskellige funktioner og adgange, der kan gøre dem i stand til at bidrage til gennemførelsen af et terrorangreb eller på anden måde forvolde skade.

Angreb med lettilgængelige midler, skydevåben og bomber

Terrorangreb med lettilgængelige midler kan gennemføres spontant eller efter meget kort planlægning. Angreb med lettilgængelige midler kan have stor skadevirkning, hvilket særligt angreb med køretøjer har illustreret. Samtidig har flere knivangreb i Frankrig i 2020 vist, at angreb med kniv kan medføre stor propagandaeffekt. Brug af køretøjer i forbindelse med terrorangreb i Vesten har primært været med henblik på at ramme større folkemængder.

CTA vurderer, at der i Danmark findes personer, der har kapacitet til at anvende skydevåben til at gennemføre terrorangreb. Erhvervelsen af sådanne våben er dog primært forbeholdt personer med lovlig adgang til våben eller med kriminelle kontakter, der kan bistå med at skaffe våben.

Der er efter CTA's vurdering personer i Danmark, der har kapacitet til at fremstille og gennemføre angreb med mindre, hjemmelavede bomber. På internettet findes der vejledninger og manualer til brug for fremstilling af forskellige sprængstoffer og hjemmelavede bomber, der vil kunne benyttes af personer uden særlige forkundskaber. Effekten af de fremstillede bomber kan dog variere betydeligt.

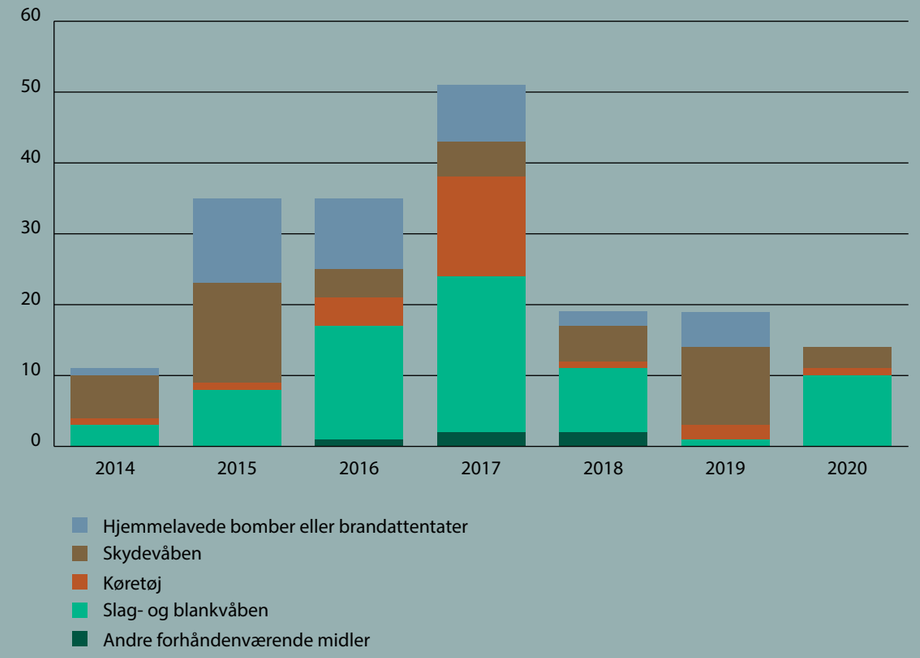
Der er en række barrierer for at producere hjemmelavet sprængstof, herunder den generelle bevågenhed omkring salg af stoffer som fx brintoverilte. Trods nationale og internationale tiltag er det dog stadig forholdsvis nemt at anskaffe ingredienser til brug for fremstilling af simple bomber, fx ved at samle krudt fra fyrværkeri eller pyroteknik.

Der er enkelte kriminelle miljøer i Danmark, der har kontakter, som muliggør erhvervelsen af fabriksfremstillet sprængstof, herunder særligt dynamit. En øget tilgængelighed af sådanne sprængstoffer kan lette fremstillingen af hjemmelavede bomber, som potentielt kan bruges til terror.

CTA vurderer, at radikaliserede personer, der har gennemgået våbentræning i en konfliktzone, såsom i Syrien/Irak, eller som har våbenkendskab fra fx afvikling af militærtjeneste, skydeklubber, kriminelle miljøer eller lignende, vil være i stand til at gennemføre angreb med særlig stor effekt. Dette omfatter også serieangreb, hvor personer eller grupper foretager flere angreb i forlængelse af hinanden.

13. Sådanne specifikke forhold er beskrevet under hhv. militant islamisme (kapitel 2), højreekstremisme (kapitel 3) og venstreekstremisme (kapitel 4).

Figur 9: Våben anvendt ved gennemførte militant islamistiske og højreekstremistiske terrorangreb i Vesten fra 2014 til og med 2020 (et angreb kan involvere flere våbentyper)



Angreb med droner
Der er i Danmark kapacitet til at anvende droner til rekognoscering, simple angreb og til at skræmme, men kapaciteten til at bruge droner til mere komplekse angreb er lav. Militante grupper har demonstreret en betydelig evne til at anvende droner til bl.a. angreb i og omkring konfliktzoner i bl.a. Syrien/Irak og Ukraine, men den opbyggede kapacitet er endnu ikke set i Vesten. Udfordringerne ved at anvende droner som angrebsvåben i Danmark er efter CTA's vurdering fortsat meget store i forhold til den skade, som et sådant våben ville kunne forvolde.

Angreb med kemiske midler
CTA vurderer, at kapaciteten i Danmark til at gennemføre kemiske angreb med andet end uforarbejdede midler er lav.

Forskellige propagandaudgivelser har lejlighedsvis fokus på anvendelsen af kemiske virkemidler. Trods opfordringer om at bruge ætsende væsker og kemiske virkemidler til at forgifte bl.a. fødevarer er sådanne midler ifølge CTA's oplysninger endnu ikke blevet benyttet til terrorangreb i Vesten.

Giftige, industrielle kemikalier og egentlige kampstoffer (primært sennepsgas) er blevet anvendt af væbnede grupper i konfliktzoner, men evnen til at overføre denne kapacitet til personer eller grupper i Vesten er efter CTA's vurdering meget lav.

Angreb med biologiske midler
CTA vurderer, at kapaciteten til at våbengøre biologiske virkemidler, såsom miltbrand, er meget lav i Danmark.

Det skyldes, at håndtering af vira og bakterier kræver helt særlige forudsætninger, herunder adgang til laboratoriefaciliteter.

CTA vurderer, at der er personer i Danmark, der vil være i stand til at fremstille enkelte toksiner i en kvalitet og mængde, der vil kunne anvendes til et simpelt biologisk angreb. Gennemførelse af et angreb vil dog også kræve kendskab til effektive metoder til udlægning eller spredning af stoffet. CTA har ikke oplysninger om angreb med biologiske midler i Vesten i 2020.

Angreb med pulverbreve
Der er kun meget få eksempler på gennemførte terrorangreb med pulverbreve i Vesten og CTA har ikke kendskab til angreb med pulverbreve i Vesten i 2020.

Angreb med radiologiske og nukleare midler
CTA vurderer, at kapaciteten til at gennemføre terrorangreb med radiologiske virkemidler hos personer i Danmark er meget lav. CTA har ikke kendskab til angrebsplanlægning med sådanne midler i Vesten.

CTA vurderer, at personer i Danmark ikke har kapacitet til at begå terror ved hjælp af nukleare midler.

Angreb med cyber-relaterede midler[14]
CTA vurderer, at kapaciteten til at gennemføre terror ved cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk national infrastruktur eller lignende mål, er lav i Danmark[15].

Angreb ved hjælp af nye teknologier
CTA følger løbende den teknologiske udvikling med henblik på at vurdere nye teknologiers indvirkning på terrortruslen i Danmark. Trods et muligt potentiale vurderer CTA, at ingen af de nye teknologier, såsom kunstig intelligens, 3D-printning og syntesebiologi[16], på nuværende tidspunkt er velegnede eller tilstrækkelig tilgængelige til at have en selvstændig indvirkning på terrortruslen.

14. "Angreb" henviser her til en aktivitet, der søger at have en skadelig effekt, og derfor ikke terroristers brug af computere til finansiering, propaganda eller lignende.
15. Se CFCS' vurdering af Cybertruslen mod Danmark.
16. Med syntesebiologi designes og konstrueres nye biologiske systemer, som ikke findes i naturen.

POLITIETS EFTERRETNINGSTJENESTE
CENTER FOR TERRORANALYSE
Klausdalsbrovej 1
2860 Søborg
45 15 90 07 • pet@pet.dk • www.pet.dk