

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.....	3
2.	INDLEDENDE BEMÆRKNINGER.....	3
3.	SUPPLERENDE SAGSFREMSTILLING	4
3.1	Præjudiciel dom C-520/18, C-511/18, C-512/18: Ordre des Barreaux, m.fl.	4
3.2	Logningsbekendtgørelsen opretholdes og håndhæves fortsat af Sagsøgte.....	13
3.3	Teledataskandalerne er eksempler på risikoen for misbrug af data lagret i medfør af Logningsbekendtgørelsen	17
4.	BESVARELSE AF UDVALGTE FORHOLD FRA SAGSØGTES SVARSKRIFT	21
4.1	EMRK art. 8 (Retten til privatliv)	21
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)	22
4.3	Underretning af berørte personer	23

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 lagring.

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 bestemmelers 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 rettidigt 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 meddelelshemmeligheden 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 vil 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 lovforslaget 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 godkendelse.

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 hørings svar, 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. Hørings svarene 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 Sagsøgte 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 telesekskaberne.

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 suspendede 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-retten 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.

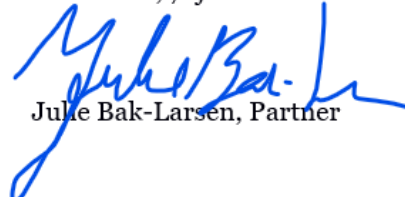
Sagsøgte redegør for reglerne i Retsplejeloven § 788, stk. 1 om, at der efter afslutning af et indgreb i meddelelseshemmeligheden skal ske underretning til de berørte personer. Sagsøgte henviser også til, at Retsplejeloven § 788, stk. 4 angiver, at sådan underretning undtagelsesvist ikke sker, hvis det 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. Rigspolitiets 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