



EU-note

Europaudvalget, Retsudvalget

EU-konsulenten

Til: Udvalgenes medlemmer
Dato: 13. januar 2017

Kontaktperson:

Julia Ballaschk (3655)

Christine Sidenius (3356)

EU-note: EU-Domstolen bekræfter i ny dom, at generel logning af elektronisk kommunikation skal respektere retten til privatliv og beskyttelse af persondata

EU-Domstolen har afsagt dom i to sager, som omhandler databeskyttelsesdirektivet vedrørende elektronisk kommunikation (e-databeskyttelsesdirektivet) [2002/58/EF](#). Dommen omhandler to sager om logningslovgivning i Sverige og Storbritannien, og om hvorvidt lovgivningen i tilstrækkelig grad beskytter følsomme personoplysninger og respekterer retten til respekt for privatliv, som det fremgår af charteret.

Sagerne er de første to sager, hvor Domstolen bekræfter sin linje efter [Digital Rights Irland-dommen](#), der annullerede logningsdirektivet fra 2006, og de første to store sager efter Snowden-sagen, om omfattende logning af kommunikationsdata i USA.

Denne note ser nærmere på domstolens afgørelse, og på mulige konsekvenser for Danmark, der på lige fod med Sverige og Storbritannien har gennemført nationale regler for logning, der gælder al elektronisk kommunikation.

Baggrund

Direktivet om databeskyttelse inden for elektronisk kommunikation (e-databeskyttelsesdirektivet) skal beskytte fortroligheden af den elektroniske kommunikation. Art. 15 i direktivet giver dog medlemslandene mulighed for at indskrænke rettighederne i direktivet og kræve teleudbydere at lagre data for at beskytte statens sikkerhed eller bekæmpe grov kriminalitet.

Fordi medlemslandene fortolkede denne bestemmelse vidt forskelligt, vedtog man et nyt logningsdirektiv 2006/24. Dette direktiv blev dog erklæret ugyldigt af EU-Domstolen i [Digital Rights Irland-sagen](#). Centralt i dommen stod at generel logning ikke må undergrave grundlæggende rettigheder om privatliv og

beskyttelse af persondata. Dommen er gennemgået i [EU-note](#) om sagen. Artikel 15 i e-databeskyttelsesdirektivet er dermed den eneste bestemmelse, der giver mulighed for at fravige direktivets øvrige bestemmelser f.eks. gennem logning, men der er opstået tvivl om, i hvor høj grad stater mulighed for at indføre generel logning er foreneligt med EU's charter om grundlæggende rettigheder.

Sverige har implementeret det nu ugyldige direktiv 2006/24 i forskellige love, der påbyder kommunikationsvirksomheder at lagre al metadata fra alle abonnenter i seks måneder og gøre dem tilgængelige for politiet og sikkerhedstjenester, for at myndighederne kan efterforske kriminalitet og bekæmpe sikkerhedsstrusler. Efter at direktivet blev erklæret ugyldig, vurderede det svenske justitsministerium, at svensk lovgivning ikke var i strid med EU-retten eller Den Europæiske Menneskerettighedskonvention (EMRK). Den svenske televirksomhed Tele2 Sverige nægtede alligevel at lagre og udlevere data til politiet og klagede ved den svenske forvaltningsdomstol.

Storbritannien havde også vedtaget forskellige love, der påbød telekommunikationsvirksomheder at lagre al telekommunikation og stille data til rådighed for politi og myndigheder. Flere borgerrettighedsorganisationer lagde sag an, fordi de mente, at disse love var i strid med EU's charter om grundlæggende rettigheder og med EMRK.

Det er på baggrund af disse sager, at der nu er ført sag og faldet afgørelse ved EU-Domstolen.

Selve dommen

Dommen er afsagt samlet i relation til to sager: Tele2 Sverige AB (sag C-203/15) mod Post og Telestyrelsen, og Secretary of State for the Home department (sag C-698/15) mod Tom Watson, Peter Brice og Geoffrey Lewis. Dommen fokuserer særligt på to aspekter, rejst i de to sager, direktivets anvendelsesområde og datalagring (logning).

Direktivets Anvendelsesområde

Domstolen har taget stilling til, om logning af data med henblik på at bekæmpe kriminalitet overhovedet falder inden for anvendelsesområdet af EU-retten.

Generelt gælder e-databeskyttelsesdirektivet ikke for dataindsamling og databehandling i forbindelse med politiarbejde eller i forbindelse med statens sikkerhed, der er reguleret af andre direktiver. Alligevel tillader art. 15 i direktivet lagring af data i en begrænset periode for bl.a. at kunne efterforske eller retsforfølge straffesager eller beskytte statens sikkerhed.

Domstolen fastslår, at retsfor skrifter om datalagring for netop disse formål ligger inden for direktivets anvendelsesområde, fordi det ellers ikke vil give me-

ning at inkludere artiklen i direktivet. Selvom formålet med de svenske og britiske love er at sikre adgangen til oplysninger for statslige politi- og sikkerhedsmyndigheder, pålægger de samtidig kommunikationsvirksomhederne en forpligtelse. Dermed er disse love omfattet af direktivets anvendelsesområde.

Datalagring (logning)

Selvom art. 15 af direktivet tillader begrænset brug af logning, konkluderer Domstolen, at denne undtagelsesbestemmelse ikke giver adgang til at indføre en generel regel om logning (Præmis 89 i dommen). Derudover skal logningen være forenelig med generelle EU-retlige principper og med EU Charteret.

Dommen medfører ikke, et totalt forbud mod regler om logning og datalagring, men i dommen stiller EU-Domstolen specifikke krav til logningsregler. Domstolen fremhæver, at logningen skal være proportional og streng nødvendig. Selvom logningsdata er vigtig for bekæmpelsen af organiseret kriminalitet og terrorisme, er dette altså ikke begrundelse nok til at indføre en generel regel om logning af data.

Dommen bekræfter de kriterier, der blev udviklet i *Digital Rights Ireland*-dommen, som kræver en direkte sammenhæng mellem data, der bliver lagret, og sikkerhedstruslen. Det betyder, at den nationale lovgivning skal definere:

- De personkategorier, hvor der er sandsynlighed for, at de er involveret i groft kriminalitet og hvis data kan blive lagret og/eller
- Den tidsperiode, hvor data kan blive lagret og/eller
- Det geografiske område, hvorfra data kan blive lagret (§106)

Domstolen anerkender ikke, at generel og udifferentieret datalogning er en nødvendig og proportional metode til at bekæmpe kriminalitet eller terrorisme.

I sin begrundelse henviser Domstolen til de konsekvenser, generel og vilkårlig datalogning kan have for demokratiet. Domstolen advarer om, at det kunne føre til at borgere føler sig konstant overvåget og dermed indskrænker deres brug af elektroniske kommunikationsmidler. Ultimativt kunne det føre til selv-censur (præmis 100 og 101).

Dommen set i sammenhæng med dansk logningslovgivning

Danmark har gennemført national lovgivning, der regulerer lagring af data og logning, og som på flere områder minder om den svenske lovgivning.

Lovhjemlen til de danske logningsregler er retsplejelovens § 786, stk. 4. Den indeholder en forpligtelse for tele- og kommunikationsvirksomheder til at registrere både tele- og internetkommunikation.

Forpligtelsen bliver konkretiseret i [logningsbekendtgørelsen](#). Logningsbekendtgørelsens § 4 er en generel regel, der gælder for alle telefonkunder. Ifølge § 4 skal teleudbydere registrere en række oplysninger om danske telekunder, såkaldte metadata. Bl.a. hvem de har ringet eller skrevet en sms til, tidspunktet for kommunikationen, og hvor de befandt sig.

Logningsbekendtgørelsen pålægger virksomhederne derudover at registrere en række oplysninger om deres kunders internetbrug, det såkaldte sessionslogning. Ifølge § 5 og § 6 skal teleudbydere bl.a. registrere adresser på deres abonnenter, tidspunkter for internetkommunikationen, den præcise geografiske placering af et trådløst internetnetværk og afsenderens og modtageres e-mailadresser. Alle disse oplysninger skal opbevares i et år.

Derudover henviser den danske [udbudsbekendtgørelse](#) til logningsreglerne i retsplejeloven. Udbudsbekendtgørelsen fastlægger, hvilke kriterier teleselskaberne skal opfylde forud for lagring af oplysninger om elektronisk kommunikation. Bekendtgørelsens § 23 indeholder en undtagelse fra forpligtelsen til at slette trafik- og lokaliseringsdata, hvis de skal stilles til rådighed for politiet til brug for efterforskning.

De danske logningsregler går videre end det nu ugyldige EU-logningsdirektiv. Men de danske regler indeholder samtidig en del betingelser, som den nye dom forudsætter for logning og for politiets adgang til logningsdata. Disse betingelser er listet i retsplejelovens § 781 - §784:

- det er alene politiet, der må få telelogningsdata udleveret
- der må være en mistænkt, der får eller sender meddelelserne
- logningsdata må være af afgørende betydning for efterforskningen og
- der skal foreligge en retskendelse

Politiet må kræve adgang til logningsdata i forbindelse med efterforskningen af grov kriminalitet eller terrorisme, men også i forbindelse med en række lovovertrædelser med lavere strafferammer end 6 år, som f.eks. overtrædelser af udlændingeloven.

Opsummering

Dommen har allerede fået flere medlemslande til at trække deres logningslovgivning tilbage med ønsket om at afvente nye EU-regler. Domstolens udtalelse om, at generelle logningsregler på nationalt niveau er problematiske, har allerede fået flere eksperter¹ til at udtale at de danske logningsregler bør ændres. Danske logningslovgivning om fortsat generel lagring af metadata, som

¹ https://www.version2.dk/artikel/jurist-lognings-dom-danske-logningsregler-klar-strid-med-eu-domstolen-1071375?utm_medium=email&utm_source=www.version2.dk&utm_campaign=tipen-ven

den i dag pålægger teleudbyderne i Danmark, skal derfor måske revideres for at imødekomme de krav som dommen fremhæver. Samtidig er der et fortsat ønske fra politiets side om udvidet adgang til lagret data.

Regeringen har i sit lovprogram for 2017 allerede annonceret et udkast til ny logningslovgivning, og regeringen har da også understreget at man vil tage højde for Domstolens dom.

https://www.version2.dk/artikel/bombe-under-ti-aars-dansk-telelogning-klart-ulovlig-skal-skrottes-1071891?utm_medium=email&utm_source=www.version2.dk&utm_campaign=tipenven