Rådet for
Den Europæiske Union

PUBLIC

Bruxelles, den 23. november 2018
(OR. en)

14319/18

LIMITE

COPEN 394
CYBER 277
DAPIX 349
ENFOPOL 561

NOTE

fra:	formandskabet
til:	De Faste Repræsentanters Komité/Rådet
Tidl. dok. nr.:	13826/18
Vedr.:	Datalagring - Status

I. Indledning

En fælles refleksionsproces om datalagring med henblik på forebyggelse og retsforfølgning af kriminalitet i lyset af Domstolens domme i *Digital Rights Ireland*[1]- og *Tele2*[2]-sagerne blev indledt under det maltesiske formandskab og blev fortsat af de estiske og bulgarske formandskaber.

På samlingen i december 2017 besluttede Rådet for Retlige og Indre Anliggender at fokusere på tre centrale elementer i det fremtidige arbejde: sikring af tilgængeligheden af data (sammenhæng med forordningen om e-databeskyttelse), etablering af garantier for adgang og begrænsning af anvendelsesområdet for reglerne for datalagring under hensyntagen til den seneste retspraksis[3].

1 C-293/12.
2 C-203/15.
3 14480/1/17.

For så vidt angår sammenhæng med udkastet til forordningen om e-databeskyttelse er reformen af reglerne om e-databeskyttelse relevant i forbindelse med debatten om datalagring. Med henblik herpå holdt DAPIX/Gruppen af Formandskabets Venner fælles møder med Gruppen vedrørende Telekommunikation den 12. februar og 17. maj 2018. I denne forbindelse er behovet for at bevare fleksibilitet i den nye e-databeskyttelsesforordning blevet anerkendt som et afgørende element for at tillade fremtidig udvikling enten via Domstolens retspraksis eller via lovgivningsmæssige reformer på nationalt eller europæisk plan.

For yderligere at underbygge begrebet begrænset datalagring (første indgrebsniveau) blev visse spørgsmål, såsom begrænsning af datakategorier, begrænsning af datalagringsperioderne, lagring på Unionens område og lagring i krypteret form eller pseudonymisering, specificeret i rapporten til Rådet med henblik på nærmere undersøgelse. For så vidt angår begrebet målrettet adgang til lagrede data (andet indgrebsniveau) blev der fremsat forskellige forslag til materielle og processuelle retlige krav. Det bemærkes indledningsvis, at der hersker fælles forståelse mellem medlemsstaterne om, at Domstolens afgørelse i *Digital Rights Ireland*- og *Tele 2*-sagerne ikke finder anvendelse på abonnentdata, men kun trafik- og lokaliseringsdata.

Det bulgarske formandskab indledte drøftelser i om indgrebsniveau 1 (**begrænset datalagring**) i arbejdsgruppen om datalagring under DAPIX/Gruppen af Formandskabets Venner. Den 18. april aflagde Europol rapport om resultaterne af datamatrixworkshoppen, og delegationerne diskuterede den eventuelle opfølgning. Der blev også set nærmere på begrebet lagringskendelser, der kan forlænges. Den 17. maj blev der indledt drøftelser om datalagringsperioderne, som blev fortsat under det østrigske formandskab den 10. juli. Dermed var gennemgangen af elementerne på indgrebsniveau 1 afsluttet. Den 11. september gennemgik arbejdsgruppen de materielle og processuelle retlige krav, hvilket afsluttede drøftelserne på indgrebsniveau 2 (**målrettet adgang til lagrede data**).

I dette dokument gør det østrigske formandskab status over drøftelserne i DAPIX/Gruppen af Formandskabets Venner (datalagring), inklusive de skriftlige bidrag, om første og andet indgrebsniveau, sammen med de mest relevante passager fra Domstolens retspraksis i *Digital Rights Ireland*- og *Tele 2*-sagerne. Den 21. november gennemgik CATS denne status med henblik på at forberede drøftelserne i De Faste Repræsentanters Komité den 28. november og i RIA-Rådet den 6.-7. december.

II. Indgrebsniveau 1: begrænset datalagring

Domstolen fastslår i *Tele 2*:

"(...) Artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel

52, stk. 1, er derimod ikke 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."*[4]

Nedenstående punkter behandler forskellige muligheder for begrænset datalagring (indgrebsniveau 1):

1. Begrænsning af datakategorier - arbejde på en "datamatrix" koordineret af Europol

Begrebet **begrænsning af datakategorier** har til formål at undersøge, om data[…], der ikke er strengt eller objektivt nødvendige til forebyggelse eller retsforfølgning af kriminalitet og sikring af den offentlige sikkerhed[…], på forhånd kan udelukkes fra reglerne om datalagring. Som et middel til at begrænse datakategorier blev der iværksat arbejde [...] på en "datamatrix". I den forbindelse opfordrede Rådet Europol til at lette det forberedende arbejde[...] til en sådan datamatrix på teknisk plan i tæt samarbejde med eksperter fra medlemsstaterne med henblik på yderligere gennemgang i DAPIX - Gruppen af Formandskabets Venner[5]. Der blev i marts og maj 2018 afholdt to workshops med nationale eksperter i cyberkriminalitet i Europols hovedkvarter i Haag.

---

4 *Tele 2*, præmis 108.
5 14480/1/17 REV 1.

En vigtig konklusion fra de to workshops var, at de relevante ETSI-standarder, som tjener som udgangspunkt for drøftelserne, allerede har filtreret de datasæt, der er teknisk tilgængelige. Dette betyder, at datakategorier[…], der ikke skønnes nødvendige for efterforskningen og retsforfølgelsen af kriminalitet[…], allerede er udelukket fra listen på forhånd. Som følge heraf mente eksperterne, at kun meget få yderligere datakategorier kunne udelukkes fra listen som værende ikke nødvendige for efterforskningen og retsforfølgningen af kriminalitet. Dette skyldes bl.a., at forskellig efterforskning af kriminalitet og forskellige efterforskningsteknikker kræver forskellige datakategorier, der skal anvendes af medlemsstaterne. Disse resultater, blandt andre, blev sammenfattet af Europol i to dokumenter og forelagt for DAPIX/Gruppen af Formandskabets Venner[6].

For så vidt angår spørgsmålet om begrænsning af datakategorier kan det derfor konkluderes, at det ville være meget vanskeligt, hvis ikke umuligt, på forhånd at undtage et væsentligt antal datakategorier fra oplagring. Årsagen er, at de relevante ETSI-standarder allerede har "filtreret" de bredere datasæt, der er teknisk tilgængelige, fordi de er blevet specifikt udviklet med henblik på retshåndhævelse. En yderligere reduktion af kategorier af lagrede data ville derfor være til skade for effektiviteten af de retshåndhævende myndigheders efterforskninger. Desuden kræver forskellig efterforskning af kriminalitet og forskellige efterforskningsteknikker i medlemsstaterne forskellige datakategorier. Eftersom de datakategorier, som ikke er nødvendige til retshåndhævelse, allerede er udelukket, sker der ingen generel og udifferentieret lagring af data som omhandlet Domstolens dom i *Tele 2*.

---

6 For nærmere oplysninger se dok.: WK 4507/2018 INIT (Resultater af 1. workshop), WK 5900/2018 INIT (Resultater af 2. workshop).

2. Lagringskendelser, der kan forlænges

I arbejdsdokument WK 3974/2018 INIT præsenterede det bulgarske formandskab begrebet lagringskendelser, der kan forlænges. Selv om Domstolen ikke havde rejst dette spørgsmål i sine domme, mente man, at det var værd at se nærmere på dette begreb. Med henblik på drøftelserne blev en lagringskendelse, der kan forlænges, defineret som en

"kendelse udstedt af en kompetent national myndighed rettet til (en) elektronisk(e) tjenesteudbyder(e), der opererer på en medlemsstats område, der anmoder tjenesteudbyderen om at lagre (visse kategorier af) data, og som er gældende i en specifik periode, i løbet af hvilken den kan fornys, hvis den opfylder de særlige betingelser, som den nationale lovgivning foreskriver for dens fornyelse, herunder at dens proportionalitet og nødvendighed er berettiget i en forudgående og bekræftet i en efterfølgende trusselsvurdering."[7]

En lagringskendelse, der kan forlænges, ville begrænse omfanget af lagrede data på grund af dens faste gyldighedsperiode, dens begrænsning til visse elektroniske tjenesteudbydere (f.eks. er mindre elektroniske tjenesteudbydere ikke omfattet) og/eller muligheden for at begrænse rækkevidden af lagringskendelser, der kan forlænges, til visse datakategorier. Endvidere ville kravet om, at en lagringskendelse, der kan forlænges, skal godkendes af en dommer, behovet for at forlænge lagringskendelsen efter udløbet af gyldighedsperioden og/eller andre retssikkerhedsgarantier sikre en regelmæssig gennemgang af foranstaltningen.

Under drøftelserne på mødet den 18. april 2018 i DAPIX /Gruppen af Formandskabets Venner om datalagring udtrykte langt størstedelen af medlemsstaterne imidlertid forbehold med hensyn til at acceptere idéen om lagringskendelser, der kan forlænges, for at begrænse omfanget af lagret data[8]. Kun én medlemsstat, som anvender et lignende system, støttede idéen. De vigtigste argumenter fra de medlemsstater, der var imod lagringskendelsen, var, at denne tilgang i deres nationale kontekst ville være for kompleks og ineffektiv, og at den slet ikke ville passe ind i deres nationale strafferetlige systemer og navnlig deres love om strafferetspleje.

I betragtning af de fleste medlemsstaters forbehold over for lagringskendelser, der kan forlænges, og det forhold, at begrebet under alle omstændigheder ikke blev bragt op af Domstolen, forekommer det ikke relevant at foretage yderligere undersøgelser.

---

7 WK 3974/2018, side 1.

8 Der var allerede udtrykt forbehold over for begrebet **på** [...] mødet den 6. november 2017, hvor idéen om lagringskendelsen blev fremlagt af det estiske formandskab sammen med mange andre forslag til det fremtidige arbejde i dok. 13845/17.

3. Begrænsede lagringsperioder

3.1. Lagringsperiodens længde

På mødet den 17. maj 2018 bad det bulgarske formandskab delegationerne om at give oplysninger om lagringsperiodens længde i deres medlemsstater. Skønt perioderne strakte sig fra nogle få uger til tre år, ligger lagringsperioden i størstedelen af medlemsstaterne (der allerede har en datalagringsordning) på enten seks eller tolv måneder).

På mødet den 10. juli 2018 bad det østrigske formandskab de medlemsstater, hvor den nationale datalagringsordning havde været indbragt for forfatningsdomstolen eller en anden ret i sidste instans, om at give oplysninger om afgørelserne med særlig henvisning til lagringsperioderne. Det blev konstateret, at i alle medlemsstater på nær én, der kommenterede dette spørgsmål, og uanset om datalagringsordningen blev opretholdt eller erklæret ugyldig af den pågældende nationale ret, var lagringsperiodens længde enten ikke afgørende i rettens overvejelser eller slet ikke relevant. Kun i én medlemsstat blev lagringsperioden, efter at sagen var indbragt for den nationale forfatningsdomstol, skåret ned fra tolv til seks måneder, mens lagringsperioden i en anden medlemsstat blev afkortet efter et forslag fra dens nationale forfatningsudvalg.

Domstolen begrænser sig i sine bemærkninger vedrørende lagringsperiodernes varighed i *Tele 2* til at fastslå, at den fastsatte varighed af lagringen skal begrænses til det strengt nødvendige[9]. Flere medlemsstater understregede, at en lagringsperiode på mindst 12 måneder efter deres opfattelse vil være absolut nødvendig af hensyn til en effektiv retshåndhævelse.

Det kan derfor konkluderes, at lagringsperiodens varighed ser ud til at være et mindre kritisk spørgsmål i Domstolens retspraksis, selv om det er afgørende, at data er tilgængelige i et passende tidsrum af hensyn til retshåndhævelsen.

9 *Tele 2*, præmis 108.

3.2. Sondring mellem datakategorier i forhold til lagring

På mødet den 10. juli 2018 spurgte det østrigske formandskab delegationerne, om der i deres nationale system gælder forskellige lagringsperioder for forskellige datakategorier. Flertallet af medlemsstater svarede, at de ikke skelnede mellem forskellige datakategorier i forhold til lagring, mens et fåtal svarede, at der i deres nationale lovgivning[…] var eller i fremtiden ville blive fastsat bestemmelser om en sondring. Domstolen udtaler sig ikke udtrykkeligt om forskellige lagringsperioder for forskellige typer datakategorier, men nævner kun muligheden for at skelne mellem forskellige kategorier af data[10]. Det følger derfor ikke nødvendigvis heraf, at sondringen skal vedrøre […] forskellige længder af perioder for forskellige datakategorier.

En anden mulighed end at skelne mellem datakategorier i forhold til lagring ville være at have forskellige perioder i forhold til adgang (jf. nedenfor).

3.3. Sletning af data ved udløbet af lagringsperioden

I *Digital Rights Ireland* kritiserer Domstolen, at "*direktiv 2006/24 [datalagringsdirektivet, der ved Digital Rights Ireland-dommen erklæres ugyldigt] ikke sikrer en irreversibel destruktion af dataene ved udløbet af lagringsperioden.*"[11] Derfor forekommer en konkret bestemmelse om sletning af data ved udløbet af lagringsperioden at være nødvendig i en ordning for lagring af data.

På mødet den 10. juli 2018 angav alle de medlemsstater, der deltog i drøftelsen, at de har **specifikke bestemmelser om sletning (eller i visse tilfælde pseudonymisering) af data ved udløbet af lagringsperioden**. Et antal medlemsstater bemærkede derudover, at lagring af data efter udløbet af den obligatoriske lagringsperiode i henhold til deres nationale lovgivning er lovlig, hvis den er nødvendig for udbyderen af forretningsmæssige hensyn. Retshåndhævelsesmyndighederne har adgang til sådanne data, så længe de respektive strafferetsplejeregler overholdes.

10 Jf. fodnote 2 (*Tele 2*, præmis 108).
11 Se også *Tele 2*, præmis 122.

4. Krav til databeskyttelse – lagring på Unionens område og lagring i krypteret form/pseudonymisering

4.1. Datalagring på Den Europæiske Unions område

Domstolen fastslår i *Tele 2*, at

"[h]enset til mængden af lagrede data, den følsomme karakter af disse data og risikoen for ulovlig adgang til disse skal udbyderne af elektroniske kommunikationstjenester med henblik på at sikre de pågældende datas fulde integritet og fortrolighed sikre et særligt højt niveau for beskyttelse og sikkerhed gennem passende tekniske og organisatoriske foranstaltninger. ***Særligt skal den nationale lovgivning foreskrive en lagring på EU's område*** *og en irreversibel destruktion af disse data ved udløbet af lagringsperioden."*[12]

På mødet den 10. juli 2018 (arbejdsdokument WK 7875/2018 INIT) spurgte det østrigske formandskab medlemsstaterne, om deres nationale datalagringssystem åbnede mulighed for obligatorisk datalagring på Den Europæiske Unions område. Af de medlemsstater, der bidrog til drøftelsen, angav et lille flertal af delegationerne, at lagring i EU (eller i EØS i et tilfælde) var obligatorisk. I halvdelen af disse tilfælde skulle dataene endda lagres i medlemsstaten selv. Blandt de medlemsstater, der ikke havde noget juridisk krav om at lagre data i EU, udtrykte nogle betænkeligheder ved en sådan forpligtelse, da den kunne medføre forskelle i behandlingen af indenlandske og udenlandske udbydere.

Medlemsstaternes holdninger og de nationale datalagringssystemer er således forskellige, hvad angår obligatorisk lagring af data i EU.

4.2. Datalagring i krypteret form/pseudonymisering

Forslaget om at lagre data i krypteret form eller beskytte dem ved pseudonymisering er ikke direkte afledt af *Digital Rights Ireland* eller *Tele 2*, men var et af de forslag til drøftelse, som blev fremsat af det estiske formandskab for at opfylde Domstolens fordring om, at der opstilles mindstekrav[13].

12 *Tele 2*, præmis 122.
13 Jf. WK 13845/17, s. 6.

Kun et meget lille antal medlemsstater angav under drøftelserne den 10. juli 2018, at de havde erfaring med databeskyttelsesforanstaltninger som lagring i krypteret form eller pseudonymisering. Flertallet af de medlemsstater, der bidrog til drøftelsen, forklarede, at der i deres nationale lovgivning ikke var fastsat bestemmelser om detaljerede eller deskriptive beskyttelsesforanstaltninger. Nogle af dem tilføjede, at de så kritisk på sådanne foranstaltninger, mens andre nævnte, at de allerede havde evalueret foranstaltninger som kryptering eller pseudonymisering af data eller i øjeblikket var inde i en evalueringsproces.

Som svar på et mere generelt spørgsmål om tekniske foranstaltninger til databeskyttelse angav de fleste medlemsstater, at deres nationale love om datalagring ikke omfattede specifikke bestemmelser om sikker lagring af data, men at generelle bestemmelser fandt anvendelse. Nogle medlemsstater giver udbyderne en skønsbeføjelse til at indføre passende beskyttelsesforanstaltninger. Kun et lille antal medlemsstater angav, at deres lovgivning og/eller tekniske forskrifter vedrørende sikker lagring af data i deres nationale datalagringssystem fastsatte specifikke krav.

Spørgsmålet om databeskyttelse er generelt et aktuelt og vigtigt emne for medlemsstaterne. Under hensyntagen til synspunktet hos mange medlemsstater og det forhold, at Domstolen ikke udtrykkeligt nævner datalagring i krypteret form eller pseudonymisering[14] […] **som et specifikt krav, forekommer datalagring i krypteret form/pseudonymisering imidlertid ikke at være et spørgsmål, der rangerer blandt de højest prioriterede i forbindelse med kortlægningen af de specifikke krav til en datalagringsordning.**

4.3. En uafhængig myndigheds tilsyn med beskyttelsesforanstaltninger mod misbrug af data

Kravet om, at en uafhængig myndighed fører tilsyn med overholdelsen af beskyttelsesforanstaltningerne, nævnes udtrykkeligt af Domstolen i *Tele 2*[15].

14 Domstolen omtaler kun beskyttelsesforanstaltninger i generelle vendinger som et uomgængeligt krav til en fremtidig datalagringsordning, jf. *Tele 2*, præmis 122.

15 *Tele 2*, præmis 123.

Under drøftelsen den 10. juli 2018 anførte alle deltagende medlemsstater, at en national myndighed havde beføjelse til at føre tilsyn med udbydernes beskyttelsesforanstaltninger med hensyn til datalagring. Nogle medlemsstater støttede udtrykkeligt det synspunkt, at et sådant tilsyn med beskyttelsesforanstaltninger ved en uafhængig myndighed kunne bruges som argument til støtte for national lovgivning om datalagring. **En datalagringsordning i henhold til EU-retten bør derfor omfatte en bestemmelse om en national uafhængig myndigheds tilsyn med overholdelsen af beskyttelsesforanstaltningerne.**

III. Indgrebsniveau II: Adgang

I *Digital Rights Ireland* fastslår Domstolen følgende:

"Ud over dette generelle fravær af grænser fastsætter direktiv 2006/24 ikke noget objektivt kriterium, som gør det muligt at ***afgrænse de kompetente nationale myndigheders adgang til dataene og den efterfølgende anvendelse heraf med henblik på forebyggelse, afsløring eller strafferetlig forfølgning vedrørende kriminalitet, der*** *henset til rækkevidden og alvoren af indgrebet i de rettigheder, som er fastslået i chartrets artikel 7 og 8,* ***kan anses for tilstrækkeligt grov til at begrunde et sådant indgreb****. Direktiv 2006/24 begrænser sig derimod til i artikel 1, stk. 1, at henvise generelt til grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning."*[16]

Domstolen gav imidlertid ikke nogen specifikke svar på spørgsmålet om, hvorvidt der skal foretages en sondring mellem de forskellige datakategorier.

1. Sondring mellem datakategorier i forhold til adgang

Holdningerne til den tekniske gennemførlighed af en sondring i forhold til adgang og dens værdi med hensyn til at opfylde Domstolens krav til en datalagringsordning var mangeartede. Nogle medlemsstater gik ind for forskellige adgangsperioder og anså dem for teknisk gennemførlige, mens andre medlemsstater modsatte sig tanken af forskellige grunde. Navnlig blev det vurderet som for dyrt og teknisk kompliceret at foretage en sondring mellem de forskellige kategorier i forhold til adgang.

16 *Digital Rights Ireland*, præmis 60.

2. Materialretlige krav til adgang til lagrede data

Drøftelsen berørte forskellige aspekter, elementer og valgmuligheder for så vidt angår **de materialretlige krav** til adgang til og brug af lagrede data. Et af de vigtigste spørgsmål, som rejses af Domstolen i *Digital Rights Ireland- og Tele2*-dommene, er manglen på objektive regler og kriterier for kriminalitet, som der kan gives adgang til data om, og for deres efterfølgende anvendelse med henblik på forebyggelse, afsløring eller strafferetlig forfølgning vedrørende kriminalitet[17].

Under den generelle drøftelse lagde medlemsstaterne klart vægt på sondringen mellem kriminalitetstyper og deres grovhed som vigtige aspekter.

2.1. Grov kriminalitet/organiseret kriminalitet/terrorisme

Domstolen fastslår i *Digital Rights Ireland*, at bekæmpelsen af "grov kriminalitet" er et mål af almen interesse, som i teorien kan begrunde datalagringsforanstaltninger. Den objektive almene interesse i at **bekæmpe grov kriminalitet kan imidlertid ikke alene begrunde en generel og vilkårlig datalagringsordning[18]**, især ikke, når direktivet kun henviser til det vage begreb "grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning"[19].

Domstolen anfører dette argument i *Tele 2* og går et skridt videre ved at fastslå, at kun bekæmpelsen af grov kriminalitet kan begrunde en foranstaltning som de anfægtede nationale datalagringsordninger.

Hvad angår **organiseret kriminalitet** og **terrorisme, anførte de bidragydende medlemsstater, at disse kriminalitetsformer utvetydigt (men ikke udelukkende) betragtes som grove, og at adgang til lagrede data derfor anses for nødvendig**.

---

17 Jf. ovenfor, *Digital Rights Ireland*, præmis 60.
18 *Digital Rights Ireland*, præmis 60.
19 Artikel 1, stk. 1, i direktiv 2006/24.

Desuden viste drøftelsen mellem medlemsstaterne, at de i deres nationale lovgivning havde indført specifikke bestemmelser om de materielle betingelser, på hvilke det er muligt at få adgang til lagrede data. For eksempel har nogle medlemsstater udarbejdet et katalog over kriminalitet, der giver adgang til lagrede data, mens andre har fastsat en tærskel ved en bestemt minimumsstraf eller kræver, at der kan idømmes varetægtsfængsling for den pågældende forbrydelse. Selv om medlemsstaterne var enige i, at adgangen til lagrede data ikke kun bør være mulig i sager om organiseret kriminalitet og terrorisme, men også med henblik på efterforskning og retsforfølgelse af alle andre former for grov kriminalitet, mente de, at det er medlemsstaterne, der skal være kompetente med hensyn til at definere, hvad der udgør en grov forbrydelse.

Derudover lagde adskillige medlemsstater vægt på den omstændighed[…], at **beslutningen om, hvorvidt der skal gives adgang til lagrede data, skal behandles af en judiciel eller administrativ uafhængig myndighed efter en konkret** […] **og individuel vurdering, der tager hensyn til indgrebets forholdsmæssighed og nødvendighed i hver enkelt sag. Derfor skal medlemsstaterne indrømmes en skønsmargen med hensyn til i deres respektive nationale (straffe-)lovgivning at fastsætte, hvilke forbrydelser der skal anses for "grov kriminalitet", som kan begrunde adgang til data.**

2.2 Cyberkriminalitet og (andre) forbrydelser, der begås online

Medlemsstaterne gav udtryk for mange forskellige holdninger. Nogle medlemsstater kategoriserer udtrykkeligt cyberkriminalitet som en kriminalitetsform, der giver adgang til lagrede data, mens andre skelner mellem grove og ikkegrove lovovertrædelser. Yderligere tre spørgsmål blev bragt på bane af en række medlemsstater: I den brede offentlighed betragtes nogle forbrydelser, som begås online (f.eks. onlineforfølgelse, -chikane og -svig), som en stor fare pga. den skade, de forårsager, uanset at de ikke nødvendigvis ligger på linje med "grov kriminalitet" pga. deres lave strafferamme. Desuden udgør visse former for cyberkriminalitet (f.eks. cyberangreb på kritisk infrastruktur) en alvorlig trussel mod samfundet som helhed. Medlemsstaterne pegede også på det forhold, at den strafferetlige efterforskning i sager om cyberkriminalitet uden adgang til lagrede data hyppigere end i andre straffesager viser sig nytteløs, fordi der ikke er adgang til digitalt bevismateriale.

2.3 "Eftersøgning & Redning"

Adgang til lagrede data med henblik på at eftersøgning af forsvundne eller bortførte personer er ikke blevet specifikt behandlet i Domstolens domme. Drøftelser mellem medlemsstaterne førte til den konklusion, at sådanne sager ofte ikke **henhører under anvendelsesområdet for straffesager,** men under andre (offentlig sikkerhed) af politiets pligter eller varetages af andre kompetente myndigheder (f.eks. efterretningstjenester). Adgang til lagrede data i sådanne sager blev anset for at ligge **uden for anvendelsesområdet for Domstolens domme**.

3. Proceduremæssige juridiske krav for adgang til lagrede data.

Domstolen kritiserede i både *Digital Rights Ireland*- og *Tele 2*-dommen manglen på regler for de proceduremæssige kriterier, efter hvilke der kan gives adgang til trafik- og lokaliseringsdata.

Det juridiske krav, som Domstolen har fastsat, var en opfordring til medlemsstaterne til at "*fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav"* for at give *"tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger […] mod risikoen for misbrug"*[20].

3.1. Kontrol fra en judiciel myndighed eller en uafhængig administrativ myndighed, herunder nødsituationer

Ifølge Domstolen "*[...] er det afgørende, at de kompetente nationale myndigheders adgang til de lagrede data i princippet er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne [...] afgørelse træffes på grundlag af en begrundet anmodning [...]*"[21].

Derfor er en beskyttelsesforanstaltning, som Domstolen har fremhævet, **forudgående kontrol fra en judiciel myndighed eller en uafhængig administrativ myndighed**.

---

20 *Tele 2*, præmis 109.

21 *Tele2,* præmis 120 ((jf. analogt for så vidt angår direktiv 2006/24, *Digital Rights Ireland*-dommen, præmis 62).

Et stort flertal af medlemsstaterne beskrev deres juridiske kontrolordninger som værende i overensstemmelse med de forudsætninger, som Domstolen har fastsat, gennem en forudgående kontrol fra en domstol/dommer, en uafhængig administrativ myndighed eller anklagemyndig. Særlige betingelser gælder for nødsituationer, hvor de retlige rammer kan give undtagelser fra den generelle regel om forudgående kontrol, f.eks. ved at sørge for et system for anmeldelse eller efterfølgende godkendelse i nødsituationer. Kun en medlemsstat anvender en generel *efterfølgende* kontrol fra en domstol.

Under drøftelserne fremhævede mange medlemsstater en skelnen mellem de forskellige datakategorier, når det drejer sig om forudgående kontrolordninger. **Abonnentdata anses for ikke at være underlagt forudgående kontrolmekanismer, mens adgang til lagrede trafik- og lokaliseringsdata i forbindelse med strafferetlige undersøgelser sædvanligvis anses for at kræve en forudgående kontrol fra en domstol/dommer elle uafhængig administrativ myndighed, undtagen i behørigt begrundede hastende tilfælde.** Dette hænger sammen med det forhold, at anvendelsesområdet for Domstolens *Digital Rights Ireland- og Tele 2-domme* […] kun strækker til trafik- og lokaliseringsdata og ikke dækker abonnentdata (jf. også indledningen ovenfor).

3.2 Indførelse af en lovbestemt datatilsynsmyndighed

Det blev endvidere drøftet, om der kan udpeges en uafhængig lovbestemt datatilsynsmyndighed som supplerende garanti for beskyttelsen af individets grundlæggende rettigheder.

Medlemsstaterne gav dog under drøftelsen klart udtryk for deres forbehold over for at indføre et sådant yderligere organ. **Generelt blev de sædvanlige kontrolmekanismer i straffesager på administrativt eller retsligt niveau ved den offentlige anklager, undersøgelsesdommeren eller dommeren under retssagen anset for at udgøre en** […] **tilstrækkelig garanti** […] **for beskyttelsen af individets (grundlæggende) rettigheder.**

3.3. Særlige regler for adgang til lagrede data for visse persongrupper

3.3.1 Undtagelser for personer, der er omfattet af tavshedspligt

I *Digital Rights Ireland* fastslog Domstolen, at "*[direktiv 2006/24] ikke indeholder nogen undtagelsesbestemmelse, således at det finder anvendelse selv på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt*"[22].

Advokater, læger, journalister, dommere og medlemmer af parlamentet blev nævnt som eksempler på enkeltpersoner, der kan være omfattet af tavshedspligt eller retten til fortrolighed mellem advokat eller klient. Under drøftelsen den 11. september 2018 blev spørgsmålet om, hvorvidt der bør være undtagelser for disse personer, og i bekræftende fald, hvordan disse undtagelser skal defineres, debatteret.

Flere medlemsstater har undtagelser for personer, der er omfattet af tavshedspligt, og nogle angav, at de anså sådanne undtagelser for at være i overensstemmelse med Domstolens faste retspraksis, selv om der i deres respektive retsorden endnu ikke var fastsat bestemmelser om sådanne undtagelser. Én medlemsstat nævnte, at der var fastsat yderligere garantier for visse grupper af personer, hvilket medførte krav om særlig omhu og yderligere hensyn i lyset af disse gruppers tavshedspligt.

Nogle medlemsstater gav dog udtryk for tvivl om, hvorvidt en sådan begrænsning ville være gennemførlig i praksis, eftersom den omstændighed, at en bestemt person tilhørte en bestemt faggruppe, ofte ikke ville være kendt på det tidspunkt, hvor der blev opnået adgang til lagrede data, navnlig ikke ved begyndelsen på en efterforskning. Hvis den pågældende persons identitet først blev afsløret på et senere tidspunkt i sagen, kunne de tilgåede data blive anset for ulovligt indhentet bevismateriale og fjernet fra sagen. Endvidere blev der givet udtryk for betænkeligheder ved, at sådanne undtagelser for bestemte faggrupper kunne være i modstrid med en effektiv strafferetlig forfølgelse, eftersom disse personer også kunne være genstand for en efterforskning.

3.3.2 Adgang til data hos personer, der ikke er mistænkte eller anklagede personer

For at efterforske og retsforfølge kriminalitet kan der være behov ikke blot for adgang til mistænkte eller anklagede personers lagrede data, men også for adgang til lagrede data hos ofre eller vidner eller hos personer med en løsere tilknytning til en forbrydelse.

22 *Digital Rights Ireland*, præmis 58.

Domstolen fastslår i den forbindelse, at den ser et behov for en tærskel, og anfører følgende: *"[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"*[23].

Medlemsstaterne blev opfordret til at drøfte mulighederne for adgang til lagrede data hos personer, der ikke er mistænkte eller anklagede.

Hovedindvendingen fra flere medlemsstater var, at en retssag ofte ikke anlægges mod bestemte personer, men mod (i hvert fald i begyndelsen) ukendte gerningsmænd. Derfor ville en udelukkelse på forhånd af personer omfattet af adgang til data hindre eller endda skade en effektiv efterforskning.

Derfor **er de fleste medlemsstater ikke tilhængere af begrænsninger i adgangen til data for personer, der ikke er mistænkte eller anklagede personer, så længe der består en forbindelse til efterforskningen/straffesagen**.

3.4. Underretning af de berørte personer og retsmidler

Det østrigske formandskab opfordrede også medlemsstaterne til at drøfte behovet for at underrette personer, der er berørt af adgang til deres lagrede data, samt kravene til en efterfølgende kontrol af afgørelsen om adgang.

Domstolen fastslår således i *Tele 2*, at det er nødvendigt at indføre regler om underretning og at bane vej for en judiciel kontrol: "*Denne underretning er nemlig de facto nødvendig for at gøre det muligt for disse personer navnlig at udøve deres adgang til retsmidler*"[24].

---

23 *Tele 2*, præmis 119.
24 *Tele 2*, præmis 121.

Indledningsvis blev spørgsmålet om en definition af begrebet "berørte personer" bragt på bane, hvilket før[…]te til forskellige svar. Anklagede personer eller mistænkte blev af alle uden undtagelse betragtet som henhørende under denne kategori. Nogle medlemsstater mente, at personer med tilknytning til den mistænkte/anklagede person eller alle personer, der deltog i den kommunikation, der var berørt af de relevante trafikdata, også kunne henhøre under kategorien. Andre medlemsstater trækker skillelinjen mellem på den ene side ofre, vidner, mistænkte/anklagede personer og på den anden side tredjeparter, der, uagtet at de kan forekomme i en efterforskningsforanstaltning, alligevel ikke henhører under anvendelsesområdet for begrebet "berørt" (f. eks. udtagning af oplysninger fra mobilmaster).

Som næste skridt opfordrede det østrigske formandskab medlemsstaterne til at drøfte behovet for at underrette de berørte personer, når deres data har været tilgået. Drøftelserne pegede på en bred vifte af valgmuligheder: Nogle medlemsstater underrettede (kun) den mistænkte eller anklagede person, nogle anvendte en mere generel tilgang, andre betragtede dette som et spørgsmål om parternes ret til aktindsigt i straffesagen og atter andre underrettede ikke aktivt personer om adgangen til de lagrede data. Desuden fremførte flere medlemsstater behovet for undtagelser fra pligten til underretning, f.eks. når identiteten af en person, hvis data er berørt, ikke kan fastslås uden yderligere undersøgelser, eller i tilfælde, hvor underretningen af den berørte person er til skade for en igangværende efterforskning. Det blev også gjort gældende, at det i sidstnævnte tilfælde bør være muligt at udsætte underretningen til et senere tidspunkt.

Med hensyn til retten til **retsmidler** forholdt det sig sådan, at kun få medlemsstater allerede indrømmede denne i den præjudicielle fase; de fleste medlemsstater giver kun anklagede personer appelmuligheder under selve retssagen. Et par medlemsstater giver derudover på visse betingelser berørte personer ret til at anmode om oplysninger om, hvorvidt de er berørt af, at lagrede data er tilgået som led i en straffesag eller ej, og i så fald yderligere retsmidler mod en sådan adgang. Én medlemsstat nævnte, at enkeltpersoner (ikke begrænset til berørte personer), uanset om de er blevet underrettet eller ej, kan bringe retsmidler i anvendelse, hvis de har rimelig grund hertil.

IV. Konklusion

Formandskabet opfordrer De Faste Repræsentanters Komité og Rådet til at notere sig status for drøftelserne i arbejdsgruppen om datalagring under DAPIX/Gruppen af Formandskabets Venner, jf. ovenstående, og udveksle idéer om det videre forløb.