JUSTITSMINISTERIET

Dato: 25. maj 2022
Kontor: Sikkerhedskontor II
Sagsbeh: DASI, LING, TRRA
Sagsnr.: 2022-187-0056
Dok.: 2411185

Notat om betydningen af EU-Domstolens dom af 5. april 2022 i sagen C-140/20, Commissioner of An Garda Síochána m.fl. for de danske logningsregler samt for de retshåndhævende myndigheders indhentning og anvendelse af loggede oplysninger

1. Indledning

EU-Domstolen har den 5. april 2022 afsagt dom i den præjudicielle sag C-140/20, Commissioner of An Garda Síochána m.fl., om irske logningsregler.

Ved brev af 6. april 2022 orienterede Justitsministeriet Folketingets Retsudvalg og Europaudvalg om dommen. I den forbindelse blev det anført, at det umiddelbart var Justitsministeriets vurdering, at dommen indebærer, at politiet under efterforskning af grov kriminalitet ikke kan indhente trafikdata registreret og opbevaret (logget) generelt og udifferentieret med henblik på at beskytte den nationale sikkerhed af udbydere (forstået i overensstemmelse med udbyderbegrebet i lov nr. 291 af 8. marts 2022). Justitsministeriet tilkendegav desuden, at ministeriet, Rigspolitiet og Rigsadvokaten ville overveje dommens betydning for politiets indhentning af loggede oplysninger i konkrete sager, og at Justitsministeriet ville vende tilbage over for udvalgene, når ministeriet havde nærlæst dommen.

I nærværende notat foretages en nærmere vurdering af EU-Domstolens dom af 5. april 2022 og dens betydning for de danske logningsregler samt for de retshåndhævende myndigheders mulighed for at indhente og anvende loggede oplysninger.

Neden for under pkt. 2 redegøres kort for de relevante gældende danske logningsregler. Dernæst redegøres under pkt. 3 for de relevante præmisser i EU-Domstolens dom af 5. april 2022. Pkt. 4 indeholder Justitsministeriets

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

vurdering af dommens betydning for de danske logningsregler, herunder muligheden for at opretholde gældende lovgivning, samt for de retshåndhævende myndigheders mulighed for indhentning og anvendelse af registrerede og opbevarede oplysninger.

2. Kort om relevante gældende danske logningsregler

Reglerne om registrering og opbevaring af trafikdata blev revideret med lov nr. 291 af 8. marts 2022, som trådte i kraft den 30. marts 2022, kl. 12.00 (herefter logningsreglerne).

Med loven indførtes bl.a. en todelt ordning for registrering og opbevaring af trafikdata.

For det første indførtes en ordning, hvor udbydere meddeles pålæg om at foretage målrettet personbestemt og geografisk registrering og opbevaring af trafikdata med henblik på bekæmpelse af grov kriminalitet.

For det andet indførtes en ordning med generel og udifferentieret registrering og opbevaring af trafikdata med henblik på beskyttelse af den nationale sikkerhed, hvorefter justitsministeren bemyndiges til efter forhandling med erhvervsministeren at kunne fastsætte regler, der pålægger udbydere at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må antages at være reel og aktuel eller forudsigelig.

Med logningsreglerne blev der desuden indført en mulighed for, at politiet og anklagemyndigheden kan indhente trafikdata registreret og opbevaret generelt og udifferentieret med henblik på at beskytte den nationale sikkerhed til brug for sager om grov kriminalitet. Som det fremgår af forarbejderne, vurderede Justitsministeriet, at dette medførte en væsentlig procesrisiko, jf. pkt. 3.7.2 i de almindelige bemærkninger til lovforslag nr. L 93 af 18. november 2021, jf. Folketingstidende 2021-22, tillæg A.

Med logningsreglerne blev politiets mulighed for at meddele udbydere pålæg om hastesikring af elektronisk data endvidere indsnævret i forhold til hidtil gældende regler, således at det efter de gældende logningsregler alene er muligt at meddele pålæg om hastesikring, hvis det sker som led i efterforskning af grov kriminalitet.

3. EU-Domstolens dom af 5. april 2022

3.1 Logning af trafik- og lokaliseringsdata

I dommens præmis 58 gentager EU-Domstolen, at artikel 15, stk. 1, i e-databeskyttelsesdirektivet[1] sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke er 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* (dvs. registrering og opbevaring eller "logning") af trafik- 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.

Desuden konstaterer EU-Domstolen i præmis 67 med henvisning til præmis 168 i La Quadrature du Net-dommen, at artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med artikel 7, 8 og 11 samt 52, stk. 1, i Chartret ikke er til hinder for lovgivningsmæssige foranstaltninger, der med henblik på bekæmpelse af grov kriminalitet 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,
- *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,
- *generel og udifferentieret lagring af de data, der vedrører identiteten* på brugerne af elektroniske kommunikationsmidler, og
- mulighed for, 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* (quick freeze) 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 omhandlende data er underlagt overholdelsen af materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.

[1] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

I dommens præmis 92 konstaterer Domstolen, at de foranstaltninger, der nævnes i dommens præmis 67, kan finde anvendelse samtidig. E-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, som fortolket i La Quadrature du Net-dommen er således ikke er til hinder for en kombination af disse foranstaltninger.

3.2 Indhentning af loggede oplysninger

I dommens præmis 96 henviser EU-Domstolen til den danske regerings indlæg under forhandlingerne, som vedrørte både den her refererede sag og de præjudicielle sager C-793/19 og C-794/19, SpaceNet m.fl. om de tyske lognigsregler (hvor der endnu ikke foreligger dom). Den danske regering argumenterede for, at de nationale myndigheder med henblik på bekæmpelse af grov kriminalitet bør kunne indhente trafik- og lokaliseringsdata, som er blevet lagret generelt og udifferentieret for at håndtere en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

Domstolen afviser i EU-Domstolens dom af 5. april 2022 imidlertid den danske regerings argumentation og anfører tre grunde hertil.

For det *første* ville den danske regerings argumentation efter Domstolens opfattelse skabe en forskellig retstilstand i medlemsstaterne med henblik på at kunne bekæmpe grov kriminalitet, der ikke kan begrundes, jf. præmis 97. Såfremt der med henblik på bekæmpelse af grov kriminalitet kunne indhentes data, som er blevet lagret generelt og udifferentieret af hensyn til den nationale sikkerhed, ville denne adgang således afhænge af omstændigheder, som er dette formål uvedkommende, afhængigt af, om der i den pågældende medlemsstat foreligger eller ikke foreligger en alvorlig trussel mod den nationale sikkerhed.

For det *andet* kan indhentning af de trafik- og lokaliseringsdata, som udbyderne lagrer som følge af en foranstaltning vedtaget i henhold til artikel 15, stk. 1, i e-databeskyttelsesdirektivet, efter Domstolens opfattelse i princippet kun begrundes med det formål, som udbyderne er blevet pålagt at foretage lagringen, jf. præmis 98.

Anderledes forholder det sig kun, såfremt det formål, der forfølges med adgangen, er vigtigere end det, der har begrundet lagringen, jf. også La Quadrature du Net-dommens præmis 165 og 166. Domstolen fastslår i forlængelse heraf, at såfremt der som led i bekæmpelsen af grov kriminalitet blev

indhentet data, der er lagret af hensyn til beskyttelse af den nationale sikkerhed, ville det være i strid med hierarkiet af mål af almen interesse, jf. præmis 99.

For det *tredje* ville forbuddet mod generel og udifferentieret lagring med henblik på bekæmpelse af grov kriminalitet efter Domstolens opfattelse blive berøvet sin effektive virkning, hvis der i sager om grov kriminalitet kunne indhentes oplysninger lagret generelt og udifferentieret af hensyn til den nationale sikkerhed, jf. præmis 100.

3.3 Betingelserne for hastesikring

For så vidt angår hastesikring ("hurtig lagring" i henhold til dommen) af trafik- og lokaliseringsdata gentager EU-Domstolen sine konstateringer fra La Quadrature du Net-dommen. Der kan efter Domstolens opfattelse således opstå situationer, hvor det kan være nødvendigt at lagre sådanne trafik- og lokaliseringsdata, som behandles af udbyderne på grundlag af artikel 5, 6 og 9 i e-databeskyttelsesdirektivet eller artikel 15, stk. 1, ud over de lovbestemte frister med henblik på at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed, både i den situation, hvor sådanne handlinger og angreb er konstateret, og i de situationer, hvor der er rimelig grund til mistanke om, at sådanne handlinger eller angreb er begået, jf. dommens præmis 85.

I en sådan situation kan medlemsstaterne med hjemmel i e-databeskyttelsesdirektivets artikel 15, stk. 1, fastsætte mulighed for ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, de råder over, jf. dommens præmis 86.

Domstolen udtaler videre i dommens præmis 87, at i det omfang formålet med en hurtig lagring ikke længere svarer til de formål, hvortil dataene oprindeligt blev indsamlet og lagret, og da enhver behandling af data i henhold til Chartrets artikel 8, stk. 2, skal opfylde udtrykkeligt angivne formål, skal medlemsstaterne i deres lovgivning præcisere det formål, med henblik på hvilket en hurtig lagring kan finde sted. Henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikret ved Chartrets artikel 7 og 8, som hurtig lagring kan indebære, er det kun bekæmpelsen af grov kriminalitet og a fortiori (dvs. så meget desto mere) beskyttelsen af den nationale sikkerhed, der kan begrunde dette indgreb. Og det i så fald på den

betingelse, at hurtig lagring og indhentningen af de hurtigt lagrede data holder sig inden for grænserne af det strengt nødvendige, jf. præmis 164-167 i La Quadrature du Net-dommen.

3.4 Anvendelse af ulovligt indhentede oplysninger som bevis

I præmis 127-128 gentager Domstolen, at spørgsmålet om antageligheden af beviser, der er fremskaffet ved hjælp af en lagring i strid med e-databeskyttelsesdirektivet, i overensstemmelse med princippet om medlemsstaternes procesautonomi henhører under national ret, dog under overholdelse af navnlig ækvivalensprincippet og effektivitetsprincippet, jf. bl.a. også præmis 41-44 i EU-Domstolens dom i sag C-746/18, Prokuratuur (herefter Prokuratuur-dommen).

4. Dommens betydning for gældende danske logningsregler mv.

4.1 Betydningen for registrering og opbevaring af data

På baggrund af det under pkt. 3.1 anførte er det Justitsministeriets vurdering, at dommen giver mulighed for fortsat at:

- Foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig (retsplejelovens § 786 e).
- Foretage målrettet personbestemt og geografisk registrering og opbevaring af trafikdata (retsplejelovens §§ 786 b-786 d).
- Foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet, herunder oplysninger om IP-adresser, der ikke i sig selv gør det muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode (retsplejelovens § 786 f).
- Meddele udbydere pålæg om at hastesikre elektroniske data (retsplejelovens § 786 a). Det vil imidlertid i lyset af dommen efter Justitsministeriets vurdering alene være muligt at hastesikre trafikdata, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed, i sager om beskyttelse af den nationale sikkerhed. Trafikdata, der er registreret og opbevaret som følge af en pligt til målrettet registrering og opbevaring med henblik på bekæmpelse af grov kriminalitet, vil dog fortsat kunne hastesikres i sager om grov kriminalitet. For så vidt angår spørgsmålet om, hvorvidt det

vil være muligt for politi og anklagemyndighed at hastesikre trafik- og lokaliseringsdata, som udbyderne råder over på andet grundlag end en registrerings- og opbevaringspligt vedtaget i medfør af artikel 15, stk. 1, i e-databeskyttelsesdirektivet)[2] henvises til pkt. 4.2.2.

Det er således Justitsministeriets vurdering, at EU-Domstolens dom af 5. april 2022 ikke har betydning for de danske logningsregler for så vidt angår udbydernes pligt til at registrere og opbevare data, og at der derfor ikke er behov for at ændre gældende ret på dette punkt. Der er til gengæld behov for at præcisere, at myndighederne alene kan pålægge udbyderne at hastesikre data, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed, i sager om beskyttelse af den nationale sikkerhed.

Justitsministeriet vil på den baggrund iværksætte et arbejde med revision af retsplejelovens § 786 a, så den på dette punkt bringes i overensstemmelse med EU-retten. Indtil den relevante ændring er gennemført ved lov, er det Justitsministeriets opfattelse, at bestemmelsen skal fortolkes i overensstemmelse med EU-retten, således at der efter bestemmelsen alene kan anmodes om hastesikring af trafikdata registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed i sager om beskyttelse af den nationale sikkerhed.

4.2 Betydning for indhentning af registrerede og opbevarede oplysninger

4.2.1. Indhentning af registrerings- og opbevaringspligtige trafikdata

De gældende bestemmelser i retsplejelovens §§ 781, 781 a, 804 og 804 a giver adgang til at foretage indgreb i meddelelseshemmeligheden og meddele pålæg om edition af trafik- og lokaliseringsdata, uanset om udbyderne registrerer disse data på grundlag af en pligt til at registrere og opbevare data eller ej.

Bestemmelserne giver således bl.a. mulighed for, at der som led i efterforskningen af grov kriminalitet kan meddeles en udbyder pålæg om at udlevere trafikdata, som udbyderen har registreret og opbevaret som følge af forplig-

[2] Når der i nærværende notat anvendes terminologien "registrerings- og opbevaringspligt" eller "en pligt til registrering og opbevaring" menes en registrerings- og opbevaringspligt (logningspligt) vedtaget i overensstemmelse med e-databeskyttelsesdirektivets artikel 15, stk. 1.

telsen i retsplejelovens § 786 e eller regler udstedt i medfør heraf, dvs. trafikdata, registreret og opbevaret generelt og udifferentieret med henblik på beskyttelse af den nationale sikkerhed. Der henvises til pkt. 3.7.2 og 3.7.3.1 i de almindelige bemærkninger til lovforslag nr. L 93 af 18. november 2021, jf. Folketingstidende 2021-22, tillæg A.

Med EU-Domstolens dom af 5. april 2022 er det imidlertid slået fast, at politiet ikke må indhente trafik- og lokaliseringsdata, der er registreret og opbevaret generelt og udifferentieret med henblik på beskyttelse af den nationale sikkerhed, hvis formålet med adgangen er at bekæmpe grov kriminalitet, der ikke angår den nationale sikkerhed, jf. ovenfor under pkt. 3.2. Derimod må politiet indhente sådanne oplysninger, hvis efterforskningen angår beskyttelse af den nationale sikkerhed i form af overtrædelser af straffelovens kapitel 12 og 13.

Konsekvensen af dommen er derfor, at retsplejelovens §§ 781, 781 a, 804 og 804 a ikke længere i overensstemmelse med EU-retten kan benyttes til at pålægge udbyderne at udlevere trafikdata, der er registreret og opbevaret i medfør af retsplejelovens § 786 e eller regler udstedt i medfør af denne bestemmelse, medmindre formålet er at beskytte den nationale sikkerhed.

Justitsministeriet vil på den baggrund iværksætte et arbejde med revision af retsplejelovens §§ 781 a og 804 a, så de bringes i overensstemmelse med EU-retten. Indtil de relevante ændringer er gennemført ved lov, er det Justitsministeriets opfattelse, at bestemmelserne skal fortolkes i overensstemmelse med EU-retten, således at der efter bestemmelserne alene kan indhentes trafikdata, der er registreret og opbevaret som følge af en forpligtelse for udbyderne til at foretage generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af national sikkerhed, hvis efterforskningen angår beskyttelse af den nationale sikkerhed i form af overtrædelser af straffelovens kapitel 12 og 13.

EU-Domstolens dom af 5. april 2022 ændrer ikke ved, at de retshåndhævende myndigheder efter retsplejelovens §§ 781, 781 a, 804 og 804 a kan indhente trafikdata, der er registrerings- og opbevaringspligtige efter retsplejelovens §§ 786 b-786 d, i sager om grov kriminalitet. Det bemærkes, at målrettet personbestemt og geografisk registrering og opbevaring af trafikdata efter retsplejelovens §§ 786 b-786 d først foretages, når udbyderne meddeles pålæg herom. Udbyderne er på nuværende tidspunkt ikke meddelt sådanne pålæg.

4.2.2. Hastesikring og indhentning af oplysninger, som udbyderne råder over på andet grundlag end en registrerings- og opbevaringspligt

Det kan i forlængelse af dommen af 5. april 2022 overvejes, om de retshåndhævende myndigheder i sager om grov kriminalitet efter retsplejelovens §§ 781, 781 a, 804 og 804 a kan indhente trafikdata, i den periode udbyderne råder over sådanne data *på andet grundlag* end en registrerings- og opbevaringspligt vedtaget i overensstemmelse med artikel 15, stk. 1, i e-databeskyttelsesdirektivet. Dommen rejser ligeledes spørgsmålet om, hvorvidt samme mulighed er gældende i forhold til hastesikring, jf. retsplejelovens § 786 a.

Det skal ses i lyset af, at dommen som nævnt medfører, at der ikke længere kan gives politiet mulighed for at hastesikre eller indhente trafikdata, der er registreret og opbevaret generelt og udifferentieret med henblik på beskyttelse af den nationale sikkerhed, hvis formålet med hastesikringen eller indhentningen er at bekæmpe grov kriminalitet, der ikke angår den nationale sikkerhed. Det bliver derfor relevant, om der er mulighed for at hastesikre og indhente trafikdata, hvis udbyderne råder over dem på andet grundlag end en registrerings- og opbevaringspligt.

Teleindustrien har over for Justitsministeriet oplyst, at udbyderne registrerer og opbevarer både trafik- og lokaliseringsdata i en begrænset periode af andre årsager end en registrerings- og opbevaringspligt (f.eks. af hensyn til fejlretning mv.). Hvis ikke der eksisterede en pligt til registrering og opbevaring af trafikdata, ville udbyderne således alligevel registrere og opbevare bl.a. trafikdata generelt og udifferentieret i en begrænset periode.

Teleindustrien har endvidere oplyst, at udbyderne registrerer og opbevarer teleoplysninger på en måde, så der kan skelnes mellem bl.a. trafikdata, der registreres og opbevares på grundlag af en registrerings- og opbevaringspligt, og trafik- og lokaliseringsdata, der er registreret og opbevaret af hensyn til fejlretning mv. og dermed på et andet grundlag og af andre grunde end en registrerings- og opbevaringspligt.

Det er Justitsministeriets opfattelse, at trafikdata, som udbyderne har registreret og opbevaret på et andet grundlag end en registrerings- og opbevaringspligt, ikke er omfattet af EU-Domstolens praksis på logningsområdet, herunder EU-Domstolens dom af 5. april 2022, idet denne praksis alene omfatter oplysninger, der er registreret og opbevaret på grundlag af en registrering og opbevaring, som medlemsstaterne i medfør af e-databeskyttelsesdirektivets artikel 15, stk. 1, pålægger udbyderne at foretage.

Det kan dog i lyset af EU-Domstolens praksis give anledning til tvivl, om de retshåndhævende myndigheder i sager om grov kriminalitet efter henholdsvis retsplejelovens § 786 a (om hastesikring) og §§ 781, 781 a, 804 og 804 a (om udlevering af trafik- og lokaliseringsdata) kan hastesikre og indhente trafikdata, som udbyderne registrerer og opbevarer på andet grundlag end en registrerings- og opbevaringspligt, når der samtidig foreligger en pligt for udbyderne til at foretage generel og udifferentieret registrering og opbevaring af trafikdata med henblik på beskyttelse af den nationale sikkerhed.

De trafikdata, der er registreret og opbevaret generelt og udifferentieret med henblik på beskyttelse af den nationale sikkerhed – og som EU-Domstolen i sin seneste dom af 5. april 2022 har fastslået, alene kan indhentes med henblik på at beskytte den nationale sikkerhed, når teleudbyderne er pålagt generel og udifferentieret logningsforpligtelse på grund af samme hensyn – vil i vidt omfang være de samme, som de oplysninger udbyderne registrerer og opbevarer af hensyn til fejlretning mv. og dermed på et andet grundlag end en registrerings- og opbevaringspligt.

Der er derfor en risiko for, at EU-Domstolen vil finde, at når der foreligger en pligt til generel og udifferentieret registrering og opbevaring af trafikdata med henblik på beskyttelse af den nationale sikkerhed, vil der ikke samtidig i sager om grov kriminalitet kunne indhentes samme trafikdata, uanset at udbyderne ville have registreret og opbevaret disse oplysninger uanset logningsforpligtelsen.

Der kan i den forbindelse bl.a. henvises til det af Domstolen anførte om, at forbuddet mod at udstede nationale regler om generel og udifferentieret lagring med henblik på bekæmpelse af grov kriminalitet ville blive berøvet sin effektive virkning, hvis der i sager om grov kriminalitet kunne indhentes oplysninger lagret generelt og udifferentieret af hensyn til den nationale sikkerhed, jf. også pkt. 3.2.

Omvendt kan der til støtte for, at der bør være en sådan mulighed anføres, at medlemsstaterne ikke bør stilles ringere i relation til hastesikring og indhentning af trafikdata til brug for bekæmpelse af grov kriminalitet, hvis den pågældende medlemsstat af hensyn til beskyttelse af den nationale sikkerhed har pålagt udbyderne en pligt til generel og udifferentieret registrering og opbevaring af trafikdata. Det bemærkes i øvrigt, at politiet – også i perioder med generel og udifferentieret registrering og opbevaring af trafikdata

– efter reglerne om edition bl.a. som led i efterforskning af grov kriminalitet har mulighed for at meddele udbydere pålæg om udlevering af lokaliseringsdata, der ikke falder ind under logningsreglernes definition af trafikdata, og som udbyderne råder over på andet grundlag end en registrerings- og opbevaringspligt, hvis der er grund til at antage, at oplysninger kan tjene som bevis (det gælder bl.a. oplysninger om, hvor f.eks. en telefon har været i forbindelse med datakommunikation, og oplysninger om, hvor f.eks. en telefon, der er tændt, men ikke aktiv, har været).

Domstolen ses ikke at have forholdt sig til det rejste spørgsmål, og det er på baggrund af ovenstående Justitsministeriets vurdering, at de retshåndhævende myndigheder – under en procesrisiko – vil kunne hastesikre samt indhente trafikdata, som udbyderne har registreret og opbevaret på et andet grundlag end en registrerings- og opbevaringspligt, og som er opbevaret på en måde, så de kan skelnes fra trafikdata registreret og opbevaret på grundlag af en registrerings- og opbevaringspligt, i sager om grov kriminalitet i medfør af henholdsvis retsplejelovens § 786 a (om hastesikring) og §§ 781, 781 a, 804 eller 804 a (om udlevering af trafik- og lokaliseringsdata).[3]

Dommen af 5. april 2022 får dermed den konsekvens for de retshåndhævende myndigheders mulighed for at efterforske og strafforfølge grov kriminalitet, at hvor myndighederne før dommen havde mulighed for at hastesikre og indhente registrerings- og opbevaringspligtig trafikdata (oplysninger om, hvem der har ringet eller skrevet (opkald, tilkald, sms og mms) sammen med hvem, hvornår, og hvor de pågældende personer har befundet sig på tidspunktet for kommunikationen) i et år fra registreringstidspunktet, vil de efter dommen alene have mulighed for at hastesikre og indhente trafikdata, som udbyderne registrerer og opbevarer på andet grundlag end en registrerings- og opbevaringspligt, i den periode, hvor udbyderne råder over disse oplysninger af hensyn til fejlretning mv. Teleindustrien har over for Justitsministeriet oplyst, at teleudbyderne registrerer og opbevarer al data af hensyn til fejlretning i kort tid, f.eks. 14 dage, mens andre data opbevares i længere tid.

Trafikdata, som udbyderne råder over på andet grundlag end en registrerings- og opbevaringspligt, og som opbevares på en måde, så de kan skelnes

[3] De retshåndhævende myndigheder vil i praksis indhente ikke-registrerings- og opbevaringspligtige oplysninger fra udbyderne ved editionspålæg eller indgreb i meddelelseshemmeligheden, som forpligter selskaberne til at udlevere oplysningerne til politiet. Det er Justitsministeriets vurdering, at sådan indhentning vil kunne ske inden for rammerne af databeskyttelsesforordningen, jf. herved forordningens artikel 5, stk. 1, litra a og b, og artikel 6, stk. 1, litra c.

fra trafikdata registreret og opbevaret på grundlag af en registrerings- og opbevaringspligt, vil således skulle behandles på linje med, hvad der i dag gælder for lokaliseringsdata, der ikke falder ind under logningsreglernes definition af trafikdata, og som udbyderne råder over på andet grundlag end en registrerings- og opbevaringspligt.

Det er således fortsat Justitsministeriets vurdering, at EU-Domstolens praksis på logningsområdet alene vedrører den registrering og opbevaring af trafik- og lokaliseringsdata, som medlemsstaterne i medfør af e-databeskyttelsesdirektivets artikel 15, stk. 1, pålægger udbyderne at foretage. Domstolens praksis om myndighedernes adgang til trafik- og lokaliseringsdata regulerer således alene data, der gøres registrerings- og opbevaringspligtige i medfør af regler, der udformes på baggrund af artikel 15, stk. 1, i e-databeskyttelsesdirektivet. Der henvises til pkt. 3.7.3.1 i de almindelige bemærkninger til lovforslag nr. L 93 af 18. november 2021, jf. Folketingstidende 2021-22, tillæg A.

Det bemærkes, at præcist hvor længe de forskellige udbydere hver især opbevarer forskellige typer af data/oplysninger på et andet grundlag end en registrerings- og opbevaringspligt, varierer afhængigt af de pågældende udbyderes behov for at opbevare de pågældende oplysninger.

4.3 Muligheden for at anvende allerede indhentede oplysninger som bevis

Dommen af 5. april 2022, der er en afgørelse i en præjudiciel sag, har konstaterende – og ikke retsstiftende – virkning fra ikrafttrædelsen af den EU-retlige regel, som fortolkes ved dommen. Det betyder, at dommen ikke skaber ny ret, men fortolker eksisterende EU-ret (e-databeskyttelsesdirektivet). Fortolkningen skal derfor tillægges virkning fra det tidspunkt, hvor reglen blev indført. Direktivet trådte i kraft den 31. juli 2002, og fristen for gennemførelse i national ret udløb den 31. oktober 2003.

Der vil være situationer, hvor oplysninger, der generelt og udifferentieret er blevet registreret og opbevaret af udbyderne med henblik på beskyttelse af den nationale sikkerhed, jf. retsplejelovens § 786 e eller regler udstedt i medfør af denne bestemmelse, er blevet udleveret til politiet i verserende sager med henvisning til et formål, der har mindre betydning i hierarkiet af mål af almen interesse end det, der har begrundet registreringen og opbevaringen. Dette afsnit adresserer, om sådanne oplysninger kan bruges som bevis i konkrete straffesager i lyset af det ovenfor under pkt. 4.1 og 4.2 anførte.

4.3.1. Praksis fra EU-Domstolen
Som det fremgår ovenfor under pkt. 3.4, gentager Domstolen i præmis 127-128 i sin dom af 5. april 2022, at spørgsmålet om antageligheden af beviser, der er fremskaffet ved hjælp af en lagring i strid med e-databeskyttelsesdirektivet, i overensstemmelse med princippet om medlemsstaternes procesautonomi henhører under national ret, dog under overholdelse af navnlig ækvivalensprincippet og effektivitetsprincippet, jf. bl.a. også præmis 41-44 i Prokuratuur-dommen.

4.3.2. Retten til retfærdig rettergang
Chartrets artikel 47 og Den Europæiske Menneskerettighedskonvention (EMRK) artikel 6 fastslår retten til en retfærdig rettergang.

Det følger af praksis fra Den Europæiske Menneskerettighedsdomstol (EMD), at retten til en retfærdig rettergang indebærer begrænsninger i adgangen til at gøre brug af beviser, der er fremskaffet i strid med bl.a. national ret, såkaldte ulovligt tilvejebragte beviser. Der gælder imidlertid ikke noget generelt forbud mod brug af sådanne beviser, jf. Jon Fridrik Kjølbro, *Den Europæiske Menneskeretskonvention*, 5. udgave (2020), side 668.

Det bemærkes, at det – uanset EU-Domstolens praksis på logningsområdet – efter Justitsministeriets opfattelse er tvivlsomt, om EMD vil finde, at beviser i form af registrerede og opbevarede oplysninger, der anvendes i en straffesag, herunder som led i efterforskningen, kan anses for at være ulovligt *tilvejebragt* i EMRK's forstand.

Hvis det lægges til grund, at EMD vil anse oplysninger, som er registreret og opbevaret med henvisning til beskyttelse af den nationale sikkerhed, men som politiet har fået adgang til med henvisning til et formål, der har mindre betydning i hierarkiet af mål af almen interesse end det, der har begrundet registreringen og opbevaringen, som ulovligt tilvejebragte beviser, vil det ifølge praksis fra EMD være afgørende for, om retten til en retfærdig rettergang er respekteret, hvorvidt straffesagen – uanset brugen af det anfægtede bevis – ud fra en helhedsbedømmelse har været retfærdig. I den vurdering indgår det bl.a., om beviset er det eneste eller afgørende bevis, jf. f.eks. EMD's dom af 11. juli 2006 i sagen *Jalloh mod Tyskland*, præmis 96. I vurderingen indgår endvidere, om forsvarets rettigheder er respekteret, dvs. om forsvaret har mulighed for at anfægte og imødegå beviset, ligesom bevisets værdi indgår, dvs. om der er tale om et sikkert bevis. Ydermere skal der ske en afvejning mellem det offentliges interesse i efterforskning og straffor-

følgning af forbrydelser og den anklagedes interesse i, at beviser tilvejebringes på en lovlig måde. Det er op til de nationale domstole at bedømme de tilvejebragte beviser, og om processen ud fra en helhedsbedømmelse har været retfærdig, jf. Jon Fridrik Kjølbro, *Den Europæiske Menneskeretskonvention*, 5. udgave (2020), side 668.

I tilfælde, hvor der er tale om beviser, som er tilvejebragt i strid med EMRK, har det betydning, om der er tale om en mere alvorlig krænkelse af EMRK. Anvendelse af beviser tilvejebragt i strid med EMRK artikel 8 om retten til privatliv, hvorunder registrerede og opbevarede trafik- og lokaliseringsdata hører, vil således som udgangspunkt ikke udgøre en krænkelse, hvis forsvarets rettigheder er respekteret, og beviserne er pålidelige, jf. f.eks. EMD's dom af 12. maj 2000 i sagen *Khan mod Storbritannien*, samt Jon Fridrik Kjølbro, *Den Europæiske Menneskeretskonvention*, 5. udgave (2020), side 670.

Det bemærkes endelig, at det i vurderingen af, om retten til en retfærdig rettergang i EMRK artikel 6 og Chartrets artikel 47 er overholdt, endvidere skal indgå, om kontradiktionsprincippet er iagttaget. Også i den forbindelse bemærkes det, at EU-Domstolen i præmis 127-128 i sin dom af 5. april 2022 gentager, at spørgsmålet om antageligheden af beviser, der er fremskaffet ved hjælp af en lagring i strid med e-databeskyttelsesdirektivet, i overensstemmelse med princippet om medlemsstaternes procesautonomi henhører under national ret, dog under overholdelse af navnlig ækvivalensprincippet og effektivitetsprincippet, jf. bl.a. også præmis 41-44 i Prokuratuur-dommen.

4.3.3. Vurdering

Det bemærkes, at det fremgår af Rigsadvokatmeddelelsen, afsnittet om anvendelse af teledata i straffesager, jf. cirkulære nr. 9343 af 30. marts 2022, at teledata, herunder registrerede og opbevarede oplysninger fra udbydere, altid vil indgå som ét blandt flere beviser i en sag, og betydningen af et bevis i form af teledata altid vil bero på en konkret vurdering af dels det enkelte bevis, dels sagens samlede omstændigheder i øvrigt.

Rigsadvokaten og Rigspolitiet har også oplyst, at registrerede og opbevarede oplysninger anvendes under efterforskningen i straffesager, men at oplysningerne ikke i praksis vil være eneste bevis til brug for f.eks. rettens beslutning om varetægtsfængsling.

Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt et bevis i form af teledata skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse.

Herudover vil der i overensstemmelse med det såkaldte "ligestillingsprincip" være adgang til kontradiktion samt fuld transparens i processen.

Det følger således af "det almindelige kontradiktionsprincip", at forsvareren under hovedforhandlingen på lige fod med anklageren vil kunne foretage dokumentation af registrerede og opbevarede oplysninger fra udbydere og stille spørgsmål til vidner mv. Retten vil endvidere være berettiget og forpligtet til at stille spørgsmål til vidner, som afhøres, når som helst der i sandhedens interesse er grund til dette.

I det omfang anklageren eller forsvareren under hovedforhandlingen finder, at der er behov for at få registrerede og opbevarede oplysninger indhentet hos udbydere yderligere belyst, vil såvel anklageren som forsvareren kunne – og anklageren efter omstændighederne skulle – anmode om supplerende bevisførelse, f.eks. indkaldelse af yderligere vidner. Retten vil også selv kunne beslutte, at yderligere beviser skal føres, hvis retten anser det for nødvendigt for sagens fuldstændige oplysning.

Endvidere må det antages, at det ikke har betydning for bevisets værdi, hvis oplysninger, der er registreret og opbevaret med henvisning til beskyttelse af den nationale sikkerhed, udleves til brug for et formål, der har mindre betydning i hierarkiet af mål af almen interesse end det, der har begrundet registreringen og opbevaringen.

Under iagttagelse af disse principper er det Justitsministeriets opfattelse, at oplysninger, der generelt og udifferentieret er blevet registreret og opbevaret af udbyderne med henblik på beskyttelse af den nationale sikkerhed i medfør af retsplejelovens § 786 e eller regler udstedt i medfør af denne bestemmelse eller de hidtil gældende regler (bekendtgørelse nr. 988 af 28. september 2006 med senere ændringer (logningsbekendtgørelsen), der bortfaldt ved ikrafttrædelsen af lov nr. 291 af 8. marts 2022 den 30. marts 2022 kl. 12), men som måtte være blevet udleveret til politiet i verserende sager, der ikke omfattes af straffelovens kapitel 12 og 13, fortsat vil kunne anvendes som bevis i konkrete straffesager.