JUSTITSMINISTERIET

Dato: 23. marts 2021
Kontor: Sikkerhedskontor II
Sagsbeh: Sarah Skafte-Vaabengaard
Sagsnr.: 2020-187-0036
Dok.: 1899781

Skitse for revision af logningsreglerne mv.

1. Indledning

Det er af afgørende betydning for regeringen at sikre, at politiet og Politiets Efterretningstjeneste har de efterforskningsredskaber, der skal til for at kunne bekæmpe kriminalitet og sikre borgernes tryghed, og for at anklagemyndigheden kan strafforfølge tiltalte ved domstolene.

Det har i årevis været centralt for politiets efterforskning at kunne indhente loggede oplysninger om teletrafik. I større straffesager om alvorlig kriminalitet indgår dette redskab ofte i politiets efterforskning. Det gælder bl.a. i sager om bandekriminalitet, drab, narkotikakriminalitet og terrorisme, hvor politiet bl.a. kan bruge loggede oplysninger til at se, hvor en potentiel gerningsmand har befundet sig på et givent tidspunkt eller som baggrund for at indhente yderligere kendelser eller indlede internationalt samarbejde.

EU-Domstolen har den 6. oktober 2020 afsagt dom i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. Dommen medfører, at der er behov for at ændre i de gældende danske regler om registrering og opbevaring af oplysninger om teletrafik (logning[1]). Samtidig skal det vurderes, i hvilket omfang dommen giver anledning til at ændre reglerne om adgang til loggede oplysninger i retsplejelovens bestemmelser om edition og indgreb i meddelelseshemmeligheden.

Den teknologiske udvikling gør det endvidere nødvendigt at opdatere politiets efterforskningsredskaber, så reglerne i større omfang tager højde for, at brugernes kommunikation i stigende grad går fra traditionel telebaseret kommunikation (som er omfattet af den nuværende logningsforpligtelse) til internetbaseret kommunikation (som i det væsentligste ikke er omfattet af den nuværende logningsforpligtelse).

I lyset af at politiets anvendelsesmuligheder for loggede teleoplysninger i fremtiden bliver meget begrænset, er der behov for, at de få tilbageværende redskaber bliver så effektive som muligt. Med henblik på at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse, har Justitsministeriet således fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til nærmere overvejelse. Dette er begrundet i hensynet til at minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede

[1] Ordene "logning" og "lagring" anvendes som synonymer i skitsen.

taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle mv.

I det følgende præsenteres Justitsministeriets foreløbige og overordnede overvejelser vedrørende den kommende revision af logningsreglerne mv. Skitsen er tænkt som et oplæg til de videre drøftelser med Folketinget, interessenter og telebranchen med henblik på, at regeringen til oktober 2021 vil fremsætte et lovforslag om revision af logningsreglerne mv.

Indledningsvist redegøres der for EU-Domstolens praksis vedrørende medlemsstaternes logningsregler (afsnit 2). Herefter præsenteres Justitsministeriets overvejelser vedrørende logning med henblik på beskyttelse af den nationale sikkerhed (afsnit 3), logning med henblik på bekæmpelse af grov kriminalitet mv. (afsnit 4), hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed (afsnit 5), udlevering af basale oplysninger, krav om registrering af taletidskort og logning af oplysninger om civil identitet (afsnit 6) samt adgang til loggede oplysninger (afsnit 7). I afsnit 8 redegøres der for Justitsministeriets umiddelbare overvejelser for perioden, indtil et nyt regelsæt træder i kraft, og endelig sammenfattes overvejelserne under afsnit 9.

2. EU-Domstolens praksis vedrørende medlemsstaters logningsregler

EU-Domstolen har afsagt flere domme, der angår medlemsstaternes logningsregler mv. I det følgende redegøres der for Digital Rights-sagen (dom af 8. april 2014), Tele2-sagen (dom af 21. december 2016), Ministerio Fiscal-sagen (dom af 2. oktober 2018), La Quadrature du Net-sagen (dom af 6. oktober 2020) og H.K.-sagen (dom af 2. marts 2021).

2.1. Dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (Digital Rights-sagen)

Ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights, erklærede EU-Domstolen direktiv 2006/24/EF (logningsdirektivet) for ugyldigt.

I dommen udtaler Domstolen, at logningsdirektivet ikke fastsætter et objektivt kriterium, der gør det muligt at afgrænse myndighedernes adgang til lagrede data og den efterfølgende anvendelse af disse med henblik på fore-

byggelse, afsløring eller strafferetlig retsforfølgning vedrørende kriminalitet, der kan anses for tilstrækkeligt grov til at begrunde et sådant indgreb – henset til rækkevidden og alvoren af indgrebet i rettighederne, der er beskyttet i artikel 7 om respekt for privatliv og artikel 8 om beskyttelse af personoplysninger i EU's Charter om Grundlæggende Rettigheder (herefter Chartret). I direktivets artikel 1, stk. 1, er der i stedet alene henvist til "grov kriminalitet" som defineret i national ret.

Domstolen udtaler videre, at logningsdirektivet ikke indeholder materielle og processuelle betingelser for myndighedernes adgang til dataene og den efterfølgende anvendelse heraf. Direktivet foreskriver således ikke udtrykkeligt, at denne adgang og efterfølgende anvendelse skal være strengt begrænset til forebyggelse og afsløring af præcist afgrænsede strafbare handlinger eller strafferetlig retsforfølgning heraf.

Domstolen bemærker herefter, at logningsdirektivet ikke fastsætter noget objektivt kriterium, der gør det muligt at begrænse antallet af personer, der er bemyndigede til at få adgang til og efterfølgende anvende lagrede data til det strengt nødvendige henset til formålet.

Domstolen udtaler endvidere, at myndighedernes adgang til lagrede data ikke med direktivet er undergivet en forudgående kontrol, der udøves enten af en retsinstans eller af en uafhængig administrativ enhed.

Endelig fastslår dommen, at logningsdirektivet ikke fastsætter tilstrækkelige garantier, der gør det muligt at sikre en effektiv beskyttelse mod risikoen for misbrug og mod enhver ulovlig adgang til og benyttelse af disse data, idet direktivet ikke indeholder regler, som er specifikke og tilpasset den meget store mængde data, til disse datas følsomme karakter samt til risikoen for ulovlig adgang til dataene. Der er således ikke med direktivet fastsat en klar og streng regulering af beskyttelsen og sikkerheden af dataene med henblik på at sikre deres integritet og fortrolighed, navnlig giver direktivet ikke en irreversibel destruktion af dataene ved udløbet af lagringsperioden, og der er ikke fastsat krav om, at dataene skal lagres inden for EU's område. I den forbindelse fastslår EU-Domstolen, at det heller ikke kan antages, at det fuldt ud er sikret, at overholdelse af kravene om beskyttelse og sikkerhed kontrolleres af en uafhængig myndighed.

2.2. Dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15 (Tele2-sagen)

EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2, har sit afsæt i dels de svenske logningsregler, dels de britiske regler for myndigheders adgang til kommunikationsdata, og omhandler fortolkningen af direktiv 2002/58 (herefter e-databeskyttelsesdirektivet) sammenholdt med Chartrets artikel 7, 8 og 11 (om respekt for privat- og familieliv, beskyttelse af personoplysninger og ytrings- og informationsfrihed).

E-databeskyttelsesdirektivet indeholder regler om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor. Det fremgår af e-databeskyttelsesdirektivet artikel 15, stk. 1, at det er muligt for medlemsstaterne under iagttagelse af de i direktivet fastsatte betingelser at vedtage "retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i [direktivets] artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9". Dette omfatter bl.a. retsforskrifter, der pålægger udbyderne af elektroniske kommunikationstjenester at lagre trafik- og lokaliseringsdata.

I dommen udtaler EU-Domstolen sig om *logningsforpligtelsen for teleudbyderne*. Den anfører indledningsvist, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere, er et meget vidtrækkende og særligt alvorligt indgreb i de grundlæggende rettigheder som fastslået i Chartrets artikel 7 og 8. Domstolen bemærker hertil, at lagringen af trafik- og lokaliseringsdata kan have en indvirkning på brugen af de elektroniske kommunikationsmidler, og følgelig på brugernes udøvelse af deres ytringsfrihed, som er sikret ved Chartrets artikel 11.

Domstolen udtaler herefter, at henset til alvoren af indgrebet i de grundlæggende rettigheder er det alene bekæmpelse af grov kriminalitet, som kan begrunde en sådan foranstaltning. Desuden bemærker Domstolen, at selv om effektiviteten af bekæmpelsen af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker, kan et sådant mål af almen interesse, hvor grundlæggende det end er, ikke i sig selv begrunde, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata, anses for nødvendig.

En national lovgivning, der forskriver en generel og udifferentieret lagring af samtlige trafik- og lokaliseringsdata bevirker, at lagringen af trafik- og lokaliseringsdata er hovedreglen, hvorimod e-databeskyttelsesdirektivet opstiller et krav om, at denne lagring af data skal være undtagelsen.

Domstolen udtaler herefter, at en lovgivning, der omfatter alle abonnenter og registrerede brugere generelt, og som er rettet mod alle elektroniske kommunikationsmidler og samtlige trafikdata, ikke foreskriver nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål. Den omfatter generelt alle personer, der gør brug af elektroniske kommunikationstjenester, uden at disse personer – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning. Den finder dermed anvendelse selv på personer, for hvis vedkommende der ikke findes noget som helst indicium for, at deres adfærd kan have – selv en indirekte eller fjern – forbindelse til grove straffelovsovertrædelser. Endvidere indeholder den ikke nogen undtagelsesbestemmelse, således at den tilmed finder anvendelse på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt.

Domstolen udtaler videre, at det for en sådan lovgivning gælder, at den ikke kræver nogen sammenhæng mellem de data, som foreskrives lagret, og en trussel mod den offentlige sikkerhed. Den er navnlig ikke begrænset til en lagring, som er rettet mod data vedrørende et tidsrum og/eller et geografisk område og/eller en personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af kriminalitet.

Domstolen konkluderer herefter, at en sådan lovgivning overskrider det strengt nødvendige og ikke i et demokratisk samfund kan anses for at være begrundet, således som det er påkrævet i henhold til EU-retten.

Domstolen fastslår herefter, at artikel 15, stk. 1, i e-databeskyttelsesdirektivet sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, derimod ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet. Dette forudsat, at lagringen af disse data begrænses til det strengt nødvendige for

så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen.

En sådan national lovgivning skal *for det første* fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, så de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige.

Hvad *for det andet* angår de materielle betingelser som en sådan national lovgivning skal opfylde, bemærker Domstolen, at lagringen af trafik- og lokaliseringsdata altid skal opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds.

Hvad angår afgrænsningen af en sådan foranstaltning med hensyn til personkredsen og de potentielt omfattede situationer, skal den nationale lovgivning være baseret på objektive forhold. Disse skal gøre det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed. En sådan afgrænsning kan sikres gennem et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive forhold finder, at der i et eller flere geografiske områder er en forhøjet risiko for, at sådan kriminalitet bliver planlagt eller begået.

I dommen udtaler EU-Domstolen sig derudover om de nærmere betingelser for myndighedernes *adgang* til de lagrede trafik- og lokaliseringsdata. Domstolen udtaler, at for at sikre at myndighedernes adgang til lagrede data begrænses til det strengt nødvendige, skal betingelserne for, hvornår udbyderne af elektroniske kommunikationstjenester skal give en sådan adgang til myndighederne, fastsættes i national ret. Den nationale lovgivning kan ikke begrænse sig til at opstille et krav om, at adgangen opfylder et af målene i artikel 15, stk. 1, i e-databeskyttelsesdirektivet, men skal også fast-

sætte de materielle og processuelle betingelser, der skal gælde for myndighedernes adgang til de lagrede data. Dette gælder også, når der er tale om, at formålet er bekæmpelse af grov kriminalitet.

Domstolen fastslår i den forbindelse i dommens præmis 119:

> ”119. For så vidt som en generel adgang til samtlige lagrede data – uafhængigt af, om der foreligger nogen forbindelse, selv indirekte, til det forfulgte mål – ikke kan anses for at være begrænset til det strengt nødvendige, skal den pågældende nationale lovgivning således være baseret på objektive kriterier med henblik på fastlæggelsen af de omstændigheder og betingelser, hvorunder de kompetente nationale myndigheder skal gives adgang til abonnenters eller registrerede brugeres data.”

Domstolen bemærker videre, at der i forbindelse med målet om bekæmpelse af kriminalitet i princippet kun gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan. I særlige situationer, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, kan der imidlertid også gives adgang til andre personers data, når der foreligger objektive forhold, som gør det muligt at antage, at disse data i en konkret sag kan bidrage effektivt til bekæmpelsen af en sådan virksomhed.

Domstolen bemærker herefter, at det er afgørende, at de nationale myndigheders adgang til lagrede data i princippet er undergivet en forudgående kontrol, der foretages enten af en domstol eller af en uafhængig administrativ enhed. Dette gælder dog ikke i behørigt begrundede hastende tilfælde. Domstolen eller enhedens afgørelse skal træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af myndighederne inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning.

Endelig udtaler Domstolen, at myndighederne, som har fået adgang til de lagrede data, så snart det ikke kan skade efterforskningen, skal underrette de berørte personer inden for rammerne af de gældende nationale procedurer. Det skyldes, at underretningen er nødvendig for at gøre det muligt for de berørte personer at bruge den adgang til retsmidler, som er fastsat i artikel 15, stk. 2, i e-databeskyttelsesdirektivet sammenholdt med artikel 22 i di-

rektiv 95/46 (dagældende persondatadirektiv, i dag erstattet af databeskyttelsesforordningen, forordning 2016/679), hvis deres rettigheder er blevet tilsidesat.

2.3. Dom af 2. oktober 2018 i sag C-207/16 (Ministerio Fiscal-sagen)

Dommen af 2. oktober 2018 i sag C-207/16, Ministerio Fiscal, vedrørte ligeledes fortolkningen af e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7 og 8. Sagen angik en situation, hvor den spanske anklagemyndighed havde fået afslag på at få adgang til de telefonnumre og SIM-kort, der var blevet aktiveret på en stjålen mobiltelefons identitetskode (et såkaldt IMEI-nummer), samt de tilknyttede personoplysninger, såsom navn og adresse. Spørgsmålet for Domstolen var, hvorvidt og i hvilket omfang det formål, som anmodningen forfulgte, var tilstrækkelig alvorligt til at begrunde offentlige myndigheders adgang til sådanne data (data med henblik på at identificere indehavere af SIM-kort, der er blevet aktiveret med en stjålet mobiltelefon, såsom efternavn, fornavn og eventuelt adresse).

Domstolen udtaler i den forbindelse, at det formål, der forfølges med en lovgivning, der regulerer en adgang til loggede oplysninger, skal stå i forhold til alvoren af det indgreb i de omhandlede grundlæggende rettigheder, som denne adgang indebærer. I overensstemmelse med proportionalitetsprincippet er et alvorligt indgreb således kun begrundet med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet. Når indgrebet ikke er alvorligt, kan det derimod begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt.

Domstolen bemærker i den forbindelse, at den adgang til data, der var omfattet af sagen, kun gjorde det muligt i en bestemt periode at sammenkæde det eller de SIM-kort, der var blevet aktiveret med den stjålne mobiltelefon, med indehaverne af disse SIM-korts identitet. Uden sammenholdning af data vedrørende den kommunikation, der var foretaget med de nævnte SIM-kort, med lokaliseringsdata, gjorde disse data det hverken muligt at kende datoen, tidspunktet, varigheden og modtagerne af den kommunikation, der var foretaget med det eller de omhandlede SIM-kort, eller de steder, hvor denne kommunikation havde fundet sted eller hyppigheden heraf med visse personer i en bestemt periode. De nævnte data gjorde det dermed ikke muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis

data er omhandlet. Under disse omstændigheder fandt Domstolen, at adgangen til de data alene ikke kan kvalificeres som et "alvorligt" indgreb i de grundlæggende rettigheder for de personer, hvis data er omhandlet.

Adgangen til data med henblik på at identificere indehavere af SIM-kort, der er blevet aktiveret med en stjålet mobiltelefon, såsom efternavn, fornavn og eventuelt adresse, kan derfor begrundes i formål om forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt, uden at det er nødvendigt, at disse forbrydelser kvalificeres som "alvorlige".

2.4. Dom af 6. oktober 2020 i de forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl. (La Quadrature du Net-sagen)

EU-Domstolens dom af 6. oktober 2020 i de forenede sager forenede sager C-511/18 og C-512/18, La Quadrature du Net m.fl. og C-520/18, Ordre des barreaux francophones et germanophone m.fl., vedrører foreneligheden af de franske og belgiske logningsregler med e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7 om respekt for privatlivet, artikel 8 om beskyttelse af personoplysninger og artikel 11 om ytringsfrihed.

I dommen gentager Domstolen udgangspunktet i Tele2-dommen om, at EU-retten er til hinder for national lovgivning, der pålægger teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata med henblik på, at offentlige myndigheder kan få adgang til disse data. Domstolen anfører dog samtidig under hvilke betingelser, udgangspunktet kan fraviges, således at medlemsstaterne kan pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata.

Domstolen fastslår således for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere mv. at lagre trafik- og lokaliseringsdata med henblik på at *beskytte den nationale sikkerhed* (præmis 134-139). I den forbindelse bemærker Domstolen, at artikel 4, stk. 2, i EU-Traktaten fastslår, at den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, samt at formålet om beskyttelse af national sikkerhed vejer tungere end f.eks. formålet om bekæmpelse af kriminalitet, hvorfor formålet kan retfærdiggøre mere alvorlige indgreb i grundlæggende rettigheder.

Som følge heraf er EU-retten ikke til hinder for, at medlemsstaterne kan pålægge teleudbydere mv. at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata for en begrænset tidsperiode, så længe der er tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig. Lagringen må dog kun ske i en afgrænset periode, der skal begrænses til det strengt nødvendige. Perioden kan forlænges, hvis den alvorlige trussel fortsætter, men EU-Domstolen understreger i den forbindelse, at lagring af data ikke må have en systematisk karakter. Endelig skal den generelle og udifferentierede lagring ledsages af mulighed for en efterfølgende effektiv prøvelse af bl.a., om der foreligger en sådan alvorlig trussel mod den nationale sikkerhed.

Dernæst fastslår Domstolen, at *grov kriminalitet* og *beskyttelse mod alvorlige trusler mod den offentlige sikkerhed* ikke kan retfærdiggøre en generel og udifferentieret lagring af trafik- og lokaliseringsdata (præmis 140-151).

Men Domstolen udelukker i den forbindelse ikke, at der med henblik på bl.a. at bekæmpe grov kriminalitet kan pålægges en målrettet lagringsforpligtelse af trafik- og lokaliseringsdata. Domstolen gentager her, hvad den tidligere sagde i bl.a. Tele2-dommen, hvorefter medlemsstaterne kan pålægge teleudbydere mv. en pligt til at lagre trafik- og lokaliseringsdata "vedrørende et bestemt tidsrum og/eller et bestemt geografisk område og/eller en given personkreds, der på den ene eller anden måde vil kunne være indblandet i alvorlige lovovertrædelser, eller mod personer, der af andre grunde gennem lagring af deres data ville kunne bidrage til bekæmpelse af grov kriminalitet".

Domstolen bemærker – som noget nyt – at det kan være berettiget at logge målrettet i områder med høj hyppighed af grov kriminalitet samt steder, hvor der i særlig grad kan begås grov kriminalitet. Det kan f.eks. være steder eller infrastrukturer, som regelmæssigt har mange besøgende-. Endelig bemærker Domstolen, at det kan være berettiget at logge målrettet i strategiske områder, såsom lufthavne, banegårde og vejafgiftsområder.

Den målrettede lagring af disse data må kun lagres, så længe det er strengt nødvendigt i lyset af formålet og de omstændigheder, der retfærdiggør laggringen. Det vil dog være muligt at forlænge foranstaltningerne, hvis fortsat lagring er nødvendig.

Domstolen anfører videre – som noget nyt – at medlemsstaterne kan fastsætte national lovgivning, der muliggør *generel og udifferentieret lagring af IP-adresser* på kilden til kommunikationen (præmis 152-159). Dette må dog alene ske med henblik på at bekæmpe grov kriminalitet eller forhindre alvorlige trusler mod den nationale sikkerhed eller offentlige sikkerhed. Lagring af IP-adresserne må alene ske i en periode, der er begrænset til det strengt nødvendige, og myndighedernes adgang til IP-adresserne skal være nøje reguleret i lovgivningen.

Domstolen anfører endvidere i præmis 140, at det kun er indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, der ikke er alvorlige, som kan begrundes i formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

For så vidt angår *oplysninger om identiteten* på brugerne af elektroniske kommunikationsmidler fastslår Domstolen, at medlemsstaterne kan pålægge teleudbydere mv. at lagre data vedrørende personers identitet med henblik på at forhindre eller efterforske alle strafbare handlinger og beskytte mod trusler mod den offentlige sikkerhed.

Lagring af data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, kan principielt ikke kvalificeres som et alvorligt indgreb. Det skyldes, at disse data ikke i sig selv gør det muligt at få kendskab til datoen og tidspunktet for en kommunikation, varigheden og modtagerne af en kommunikation, de steder, hvorfra en kommunikation har fundet sted, eller oplysning om, hvor ofte en kommunikation har været foretaget med visse personer i en bestemt periode. Det indebærer, at disse data bortset fra de pågældendes kontaktoplysninger, såsom deres adresser, ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om disse personers privatliv (præmis 157).

I den forbindelse bemærker Domstolen, at der ikke er noget krav om, at kriminaliteten eller truslen er alvorlig. Krav om lagring af data om personers identitet er ikke underlagt nogen tidsbegrænsning.

Domstolen fastslår endelig, at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. *en hurtig lagring af trafik- og lokaliseringsdata, som de allerede råder over*, f.eks. som led i lovlig forretningspraksis eller lignende eller som følge af en retlig forpligtelse (præmis 160-165). De trafik- og lokaliseringsdata,

som behandles og lagres af teleudbyderne, skal principielt slettes eller gøres anonyme efter udløbet af de lovbestemte frister, der er fastsat i overensstemmelse med gennemførelsen af e-databeskyttelsesdirektivet. Der kan imidlertid opstå situationer, hvori det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed.

Der kan således i visse situationer i et udvidet omfang ske hurtig lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået eller planlagt, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds.

En sådan hurtig lagring kan udelukkende ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske.[2]

2.5. Dom af 2. marts 2021 i sag C-746/18 (H.K.-sagen)

EU-Domstolens dom af 2. marts 2021 i sag C-746/18 (H.K.-sagen) vedrører de estiske regler om adgang til loggede trafik- og lokaliseringsdata i forbindelse med en konkret straffesag, hvor en kvinde var blevet idømt en frihedsstraf på to år for bl.a. tyveri. I straffesagen indgik bl.a. trafik- og lokaliseringsdata, som anklagemyndigheden havde fået adgang til fra teleudbydere, idet teleudbyderne var underlagt en lovbestemt forpligtelse til i et år at foretage generel og udifferentieret lagring af sådanne data. Efter de estiske regler kunne anklagemyndigheden anmode om adgang til oplysningerne for enhver form for straffelovsovertrædelse. Spørgsmålet var bl.a., om adgangen til disse data var i strid med e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, idet adgangen ikke var begrænset til formålet om at bekæmpe grov kriminalitet.

EU-Domstolen anfører indledningsvist, at EU-retten er til hinder for lovgivningsmæssige foranstaltninger, der i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafik- og lokaliseringsdata. I overensstemmelse med proportionalitetsprincippet er det kun bekæmpelsen af grov

[2] Derudover forholdt Domstolen sig til en særlig fransk regel vedrørende mulighederne for at få kunne adgang til trafik- og lokaliseringsdata i realtid, jf. dommens pr. 183-189.

kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde de indgreb, som lagring af trafik- og lokaliseringsdata indebærer, uanset om der er tale om generel og udifferentieret lagring eller målrettet lagring (præmis 33). Derimod kan bekæmpelsen af kriminalitet i almindelighed godt begrunde mindre alvorlige indgreb, som for eksempel behandling af data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, idet disse data ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om brugernes privatliv (præmis 34).

Domstolen fastslår således, at det kun er bekæmpelsen af grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde offentlige myndigheders adgang til lagrede trafik- eller lokaliseringsdata. Andre faktorer vedrørende forholdsmæssigheden af en anmodning om adgang, såsom varigheden af den periode, for hvilken der er anmodet om adgang til de nævnte data, og mængden eller arten af de data, der er tilgængelige i en sådan periode, kan derimod ikke føre til, at formålet om bekæmpelse af kriminalitet i almindelighed kan begrunde en sådan adgang (præmis 39). Domstolen medgiver, at sådanne momenter indgår i vurderingen af, om en adgang i det konkrete tilfælde er begrænset til det strengt nødvendige, men det kan altså ikke medføre, at der kan gives adgang til sådanne oplysninger uden krav om, at adgangen har til formål at bekæmpe grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed.

Endelig anfører Domstolen, at der i princippet kun kan gives adgang til data vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse. I særlige situationer, såsom de situationer, hvor vitale interesser for den nationale sikkerhed, forsvaret eller den offentlige sikkerhed er truet af terrorvirksomhed, kan der imidlertid også gives adgang til andre personers data, når der foreligger objektive forhold, som gør det muligt at antage, at disse data i en konkret sag kan bidrage effektivt til bekæmpelsen af en sådan virksomhed (præmis 50). Adgangen til de lagrede data skal endvidere være undergivet en kontrol, der sker forudgående – eller i hastende tilfælde hurtigst muligt – og som foretages af enten en domstol eller en uafhængig administrativ enhed.

3. Logning med henblik på beskyttelse af den nationale sikkerhed

3.1. Gældende ret

3.1.1. Retsplejelovens § 786, stk. 4

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren kan efter forhandling med erhvervsministeren og klima, energi- og forsyningsministeren fastsætte nærmere regler herom.

Det fremgår af forarbejderne til lov nr. 378 af 6. juni 2002 (bemærkningerne til § 2, nr. 2 og 3, i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 879), at retsplejelovens § 786, stk. 4, indebærer en pligt for udbydere af telenet og teletjenester til at registrere både tele- og internetkommunikation.

Bestemmelsen blev foreslået med henblik på at styrke politiets efterforskningsmuligheder, jf. pkt. 1.2 i de almindelige bemærkninger i lovforslag nr. L 35 som fremsat, jf. Folketingstidende 2001-02 (2. samling), Tillæg A, side 816. Formålet med bestemmelsen var at sikre tilstedeværelsen af de oplysninger, som politiet kan få adgang til ved blandt andet indgreb i meddelelseshemmeligheden i form at teleoplysning og udvidet teleoplysning. Forslaget berørte ikke de materielle og formelle betingelser for, at politiet kan foretage indgreb i meddelelseshemmeligheden herunder kravet om retskendelse.

Det bemærkes, at det i pkt. 1.2 i de almindelige bemærkninger til lovforslaget er forudsat, at der alene er tale om registrering og opbevaring af trafikdata og ikke af selve indholdet af kommunikationen.

De nærmere regler om logning, herunder hvilke oplysninger udbyderne skal logge, fremgår af logningsbekendtgørelsen, jf. nærmere herom nedenfor under pkt. 3.1.2.

De nærmere betingelser for, hvornår teleudbyderne skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. nærmere herom nedenfor under pkt. 7.1. Det betyder bl.a., at udlevering af oplysningerne i hvert enkelt tilfælde som udgangspunkt kræver, at rettens kendelse opnås forud for udleveringen, ligesom teleudbyderen er forpligtet til at udlevere oplysninger i henhold til rettens kendelse.

Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786, stk. 4, for teleudbydere til at registrere både tele- og internetkommunikation til brug for efterforskning og retsforfølgning af strafbare forhold ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for logning med henblik på beskyttelse af den nationale sikkerhed.

3.1.2. Logningsbekendtgørelsen

Bekendtgørelse nr. 988 af 28. september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i bl.a. retsplejelovens § 786, stk. 4. Bekendtgørelsen trådte i kraft den 15. september 2007.

Bekendtgørelsen blev ændret ved bekendtgørelse nr. 660 af 19. juni 2014, hvorved reglerne om logning af oplysninger om såkaldt sessionslogning (logning af en række forbindelsesoplysninger om internettrafik) blev ophævet.

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

Udtrykket »udbyder« skal forstås i overensstemmelse med samme udtryk i § 2, nr. 1, i lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer om elektroniske kommunikationsnet og -tjenester (teleloven). Det betyder, at alle parter, der på kommercielt grundlag stiller kommunikationsnet eller -tjenester til rådighed for slutbrugere, skal foretage registrering og opbevaring af en række oplysninger. Logningsforpligtelsen påhviler således alene de kommercielle udbydere af kommunikationsnet mv., hvorfor bl.a. en række offentlige myndigheder og institutioner ikke er omfattet heraf. Det gælder bl.a. biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende mv.).

Logningsbekendtgørelsen finder ikke anvendelse for transport af radio- og tv-programmer og for andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf, der inden for foreningen eller sammenslutningen udbyder elektroniske kommunikationsnet eller -tjenester til færre end 100 enheder, jf. §§ 2 og 3.

Efter logningsbekendtgørelsens § 4 skal udbyderne registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation. Det gælder bl.a. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler, som en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen, samt oplysninger om anonyme tjenester (taletidskort). Oplysningerne giver dermed mulighed for, at politiet kan fastslå, hvem der har kommunikeret med hvem, hvornår de har kommunikeret, og hvor de befandt sig på tidspunktet for kommunikationen.

Efter logningsbekendtgørelsens § 5 skal udbyderne registrere visse nærmere angivne oplysninger om en brugers adgang til internettet. Efter logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, skal en udbyder således bl.a. registrere oplysninger om tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse) på det pågældende tidspunkt.

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

Udbyderne skal i ingen tilfælde registrere eller opbevare indholdet af kommunikation, hverken i forbindelse med telekommunikation, brug af internettet eller brug af udbyderens egne kommunikationstjenester.

Hvis de i §§ 4-6 nævnte oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne, jf. logningsbekendtgørelsens § 7.

Efter logningsbekendtgørelsens § 8 kan registrering og opbevaring af de i §§ 4-6 nævnte oplysninger efter aftale med udbyderen på dennes vegne foretages af en anden udbyder eller af en tredjemand.

De registrerede oplysninger opbevares i 1 år, jf. logningsbekendtgørelsens § 9.

Manglende iagttagelse af logningspligten efter bekendtgørelsen straffes med bøde, jf. logningsbekendtgørelsens § 10.

3.2. Relevante dele af La Quadrature du Net-dommen

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår logning med henblik på beskyttelse af den nationale sikkerhed er de relevante dele af dommen præmis 134-139. Det fremgår heraf navnlig,

- at der kan fastsættes nationale regler, der foreskriver generel og udifferentieret logning af trafik- og lokaliseringsdata vedrørende alle brugere i en begrænset periode, når der foreligger tilstrækkeligt konkrete omstændigheder, der gør det muligt at antage, at en medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed,
- at dette gælder i situationer, hvor staten har en interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser og omfatter forebyggelse og bekæmpelse af aktiviteter, der alvorligt

kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed,

- at truslen mod den nationale sikkerhed skal kunne anses for at være reel og aktuel eller forudsigelig,
- at lagringen tidsmæssigt skal begrænses til det strengt nødvendige, og at selv om en lagring kan forlænges som følge af, at en trussel fortsat består, må varigheden af hvert enkelt påbud ikke overstige et forudseeligt tidsrum,
- at en sådan lagring skal være omfattet af begrænsninger og underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug,
- at lagringen således ikke må have en systematisk karakter, og
- at en afgørelse, hvorved der pålægges en sådan lagring, skal kunne gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ enhed med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

3.3. Justitsministeriets overvejelser og den foreslåede ordning

3.3.1. Alvorlig trussel mod national sikkerhed, der er reel og aktuel eller forudsigelig

Justitsministeriet har overvejet, hvad der kan udgøre et velunderbygget og tilstrækkeligt grundlag til at vurdere, om der er en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, således at der er basis for en generel og udifferentieret logning af trafik- og lokaliseringsdata[3] vedrørende alle brugere i en begrænset periode.

[3] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata".

Center for Terroranalyse (CTA)[4] udgiver i dag "Vurderingen af Terrortruslen mod Danmark". Vurderingen er CTA's samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet. Vurderingen, der i udgangspunktet udgives årligt, bygger på et stort antal underliggende analyser fra CTA, der strækker sig fra vurderinger af truslen mod konkrete personer, lokaliteter og begivenheder til bredere tendensanalyser og vurderinger af fænomener med betydning for terrortruslen mod Danmark og danske interesser i udlandet. Vurderingen er baseret på bl.a. efterretninger fra Politiets Efterretningstjenestes operationer, oplysninger fra internationale partnere, indberetninger fra myndigheder og privatpersoner samt offentligt tilgængeligt materiale.

Vurderingen af Terrortruslen mod Danmark indeholder en overordnet vurdering af terrortruslen mod Danmark fra bl.a. militant islamisme, højreekstremisme og venstreekstremisme. Inden for hver af disse kategorier vurderes terrortruslen mod Danmark. Som led heri vurderes det bl.a., om det er sandsynligt, at en eller flere aktører har kapacitet og/eller intention om at begå et terrorangreb, og om planlægning af et terrorangreb i det kommende år er sandsynlig. Endvidere vurderes det mest sandsynlige terrorangreb og de mest sandsynlige mål.

CTA anvender trusselsniveauer og sandsynlighedsgrader for at sikre analytisk stringens og give offentligheden et redskab til at sammenligne og forstå, hvordan forskellige trusler udvikler sig over tid. Skalaen for terrortrusselsniveauer og niveauernes definitioner fremgår af figur 1 herunder.

[4] CTA er opbygget som et fusionscenter, der består af medarbejdere fra Forsvarets Efterretningstjeneste (FE), Politiets Efterretningstjeneste (PET), Udenrigsministeriet, Beredskabsstyrelsen og Rigspolitiets Nationale Efterforskningscenter. CTA-konstruktionen medvirker til at sikre hurtig og effektiv koordination samt udveksling af information mellem relevante danske myndigheder med henblik på at imødegå eventuelle trusler på et så tidligt tidspunkt som muligt. Arbejdet bidrager bl.a. til dimensioneringen af det nationale beredskab på terrorområdet.

Figur 1: Terrortrusselsniveauer og deres definitioner	
Terrortrusselsniveau	**Definition**
Meget alvorlig	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse.
Alvorlig	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning.
Generel	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning.
Begrænset	Der er en potentiel trussel. Der er begrænset kapacitet og/eller hensigt.
Ingen	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

Seneste Vurdering af Terrortruslen mod Danmark blev udgivet den 20. marts 2020. Det fremgår heraf, at CTA vurderer, at terrortruslen mod Danmark er alvorlig. Det fremgår også af tidligere vurderinger af terrortruslen, at CTA har vurderet, at truslen mod Danmark er alvorlig, jf. CTA's vurderinger i årene fra 2014-2020.[5] Siden 2014 har CTA brugt terrortrusselsniveauerne og definitionerne gengivet ovenfor i figur 1, herunder begrebet "alvorlig", som en indikation på et specifikt defineret trusselsniveau.[6]

Terrortruslen mod Danmark og danske interesser i udlandet udgik ved oprettelsen af CTA i 2007 primært fra militante islamister, der var motiveret af Danmarks aktive udenrigs- og sikkerhedspolitik, herunder engagementet i Irak og Afghanistan. Danmark blev betragtet som et legitimt, men ikke prioriteret terrormål.

Terrortruslen mod Danmark har således ikke altid været på trusselniveauet "alvorlig".

Det generelle trusselsbillede, der påvirker terrortrusselsniveauet for Danmark, er dynamisk og komplekst, hvilket blandt andet kan ses ved markante

[5] Vurdering af Terrortruslen mod Danmark af 20. marts 2020, Vurdering af Terrortruslen mod Danmark af 12. januar 2018, Vurdering af Terrortruslen mod Danmark af 7. februar 2017, Vurdering af Terrortruslen mod Danmark af 28. april 2016, Vurdering af Terrortruslen mod Danmark af 18. marts 2015, Vurdering af Terrortruslen mod Danmark af 12. december 2014 og 24. januar 2014.

[6] Før 2014 var CTA's vurdering af Terrortruslen mod Danmark en mere beskrivende gengivelse af trusselsbilledet. Vurderingen var ikke niveauinddelt, og indeholdt således ikke en konklusion på det samlede niveau for terrortruslen. Af samme årsag kan brugen af begreberne "generel" og "alvorlig", der har været anvendt i Vurderingen af Terrortruslen før 2014, ikke i sig selv anvendes til at konkludere, om trusselsniveauet har haft et niveau, der er sammenligneligt med niveauinddelingen i figur 1.

udsving i antal gennemførte og afværgede angreb mod lande i Vesten. Fastsættelse af et terrortrusselsniveau er således et udtryk for en samlet vurdering baseret på konkrete hændelser og tilgængelige oplysninger.

Udviklingen i terrortrusselsniveauet i Danmark har over en årrække især været præget af konflikter i udlandet, herunder i Syrien og Irak, og sager om opfattede krænkelser af islam. Disse forhold har i de seneste år medvirket til at skærpe terrortruslen mod Danmark og danske interesser i udlandet.

Der er også løbende faktorer i trusselsbilledet i Danmark eller udlandet, herunder terrorgruppers intention og kapacitet der kan tiltage eller aftage, som kan have effekt på det generelle trusselsbillede, således at terrortruslen i Danmark også kan skærpes eller reduceres. Dette vil som nævnt bero på en samlet vurdering af relevante forhold og tilgængelige oplysninger.

Det er Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark bygger på tilstrækkeligt konkrete omstændigheder, herunder konkrete efterforskninger og straffesager i Danmark, der gør det muligt at vurdere og sandsynliggøre, om der er en alvorlig trussel mod den nationale sikkerhed, hvor f.eks. aktiviteter alvorligt kan destabilisere Danmarks grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed. Endvidere er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark ud fra dens analytiske kvalitet, systematik og metodik kan sandsynliggøre, at en sådan trussel er reel og aktuel eller forudsigelig.

Endelig er det Justitsministeriets opfattelse, at Vurderingen af Terrortruslen mod Danmark er tilstrækkelig dynamisk i karakter til, at logningen ikke herved vil få en systematisk karakter. Der henvises til, at der tidligere har været perioder, hvor truslen mod Danmark har været vurderet anderledes af nationale myndigheder, samt at vurderingen efter Justitsministeriets opfattelse har en kvalitet, systematik og metodik, der sandsynliggør det valgte trusselsniveau, uanset at vurderingen i en årrække har været på samme niveau.

Ud over Vurderingen af Terrortruslen mod Danmark, kan også en række andre analyseprodukter udgivet af enten Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center For Cybersikkerhed, belyse en trussel mod Danmarks sikkerhed inden for et specifikt område. Det kunne

f.eks. være Center For Cybersikkerheds årlige "Trusselsvurdering 2020: Cybertruslen mod Danmark", men også andre relevante trusselsvurderinger vil kunne indgå.

Disse analyser vil kunne indgå i en samlet vurdering af truslen mod Danmark, der vil kunne foretages regelmæssigt, så det sikres, at både nationale og internationale forhold af betydning for Danmarks nationale sikkerhed inddrages. Inddragelsen af flere af hinanden uafhængige analyseprodukter vil kunne styrke det vurderingsmæssige grundlag af det samlede trusselsbillede.

Det er således Justitsministeriets vurdering, at der bl.a. på baggrund af Vurderingen af Terrortruslen mod Danmark og øvrige analyseprodukter, kan foretages en velunderbygget vurdering af truslen mod Danmarks nationale sikkerhed med henblik på at konstatere, om der er tilstrækkelige solide grunde til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

Det foreslås på den baggrund, at der indføres en ordning, hvorefter justitsministeren, såfremt der foreligger en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, kan fastsætte en forpligtelse for teleudbydere mv. til at foretage logning af teleoplysninger mv.

Forpligtelsen vil gælde generelt og udifferentieret. Forpligtelsen vil være tidsmæssigt afgrænset, jf. nærmere nedenfor. Det forventes, at Vurderingen af Terrortruslen mod Danmark kan indgå som et hovedmoment i en samlet vurdering, hvor også andre analyseprodukter udgivet af Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed kan indgå.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master,

mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra "ikke-aktiv" kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

3.3.2. Tidsmæssig udstrækning

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen tidsmæssigt begrænses til det strengt nødvendige, og at varigheden af hvert enkelt påbud ikke overstiger et forudseeligt tidsrum, således at logningen ikke får en systematisk karakter.

De sager, der er omfattet af straffelovens kapitel 12 om forbrydelser vedrørende landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed og kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme mv., herunder efterforskningen af sådanne sager, har ofte en kompleksitet og et tidsmæssigt perspektiv, der kan strække sig over lang tid.

Det foreslås på den baggrund, at der indføres en ordning, hvorefter justitsministeren kan fastsætte en forpligtelse for teleudbydere mv. til i op til 1 år

at foretage logning af teleoplysninger mv. af hensyn til beskyttelse mod en alvorlig trussel mod den nationale sikkerhed.

En sådan tidsmæssig udstrækning vurderes at være proportionel under hensyn til sagernes alvorlige karakter og kompleksiteten af sagerne, herunder nødvendigheden af bagudrettet at kunne afdække miljøer og netværk, der er kendetegnet ved en meget høj grad af sikkerhedsbevidsthed. Den tidsmæssige udstrækning skal begrænses til det strengt nødvendige, og udstrækningen kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt. Endvidere vil begrænsningen sikre, at varigheden af hvert enkelt påbud ikke overstiger et forudseeligt tidsrum.

3.3.3. Retsgarantier og domstolsprøvelse mv.

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen er underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug, og hvordan afgørelsen, hvorved der pålægges en sådan logningsforpligtelse, kan gøres til genstand for en effektiv prøvelse.

Det er Justitsministeriets umiddelbare opfattelse, at de nuværende regler om teleudbydernes behandling af loggede oplysninger, herunder de sektorspecifikke databeskyttelsesregler, samt krav om sikkerhedsgodkendelse mv. kan videreføres, og at disse regler effektivt beskytter mod risikoen for misbrug.[7]

Som nævnt ovenfor, forventes Vurderingen af Terrortruslen mod Danmark samt andre uklassificerede efterretningsmæssige analyseprodukter at kunne udgøre grundlaget for vurderingen af, om der er en alvorlig trussel mod den nationale sikkerhed. Justitsministeriets vurdering kan gøres til genstand for en domstolsprøvelse af, om der foreligger en sådan situation, samt om de betingelser og garantier, der skal være fastsat, er overholdt.

Det er Justitsministeriets opfattelse, at detaljeringsgraden i den uklassificerede udgave af Vurderingen af Terrortruslen mod Danmark udgør et tilstrækkeligt sikkert grundlag til, at der kan foretages en effektiv retlig prøvelse af Justitsministeriets vurdering af grundlaget for et pålæg om logning.

[7] Der kan bl.a. henvises til bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, herunder bekendtgørelsens §§ 10 og 11 om krav til udbydernes behandling af trafik- og lokaliseringsdata.

Ved domstolsprøvelsen er det alene Justitsministeriets vurdering, der kan efterprøves, da de efterretningsmæssige analyseprodukter i vidt omfang baserer sig på klassificeret materiale. Det kan i den forbindelse nævnes, at der vil være betydelige fordele forbundet med, at prøvelsen sker i en sædvanlig retsproces, hvor den fremlagte dokumentation – i det omfang det vurderes nødvendigt – evt. kan suppleres med vidneforklaringer fra ledende medarbejdere, der kan forklare om metodikken og tilblivelsesprocessen af de konkrete vurderinger mv.

Det er endvidere Justitsministeriets opfattelse, at der vil kunne fastsættes nærmere tekniske krav til udbydernes målrettede logning, herunder nærmere regler om opbevaringsformat, foranstaltninger med henblik på at sikre oplysningernes integritet og beskyttelse mod uautoriseret adgang, opbevaringssted mv. Det vil medvirke til at sikre, at der løbende kan ske den fornødne tilpasning i lyset af den teknologiske udvikling.

Det foreslås på den baggrund, at der med den foreslåede ordning sikres mulighed for, at der kan ske en efterfølgende prøvelse af den fastsatte forpligtelse ved domstolene af, om der foreligger en situation, hvor der er en alvorlig trussel mod den nationale sikkerhed, som er reel og aktuel eller forudsigelig.

3.3.4. Forpligtelser for teleudbyderne mv.

Justitsministeriet har overvejet, hvilke forpligtelser for teleudbyderne mv. den foreslåede logning vil medføre, udover selve logningsforpligtelsen.

Det foreslås, at i det omfang, der måtte blive fastsat regler om et fælles opbevaringsformat, og dette adskiller sig fra det af teleudbyderen anvendte, vil det påhvile udbyderen at foretage konvertering af den relevante data, herunder sikring af den fornødne dataintegritet og -kvalitet. Det følger af telelovens § 10, stk. 1, nr. 1, at det påhviler udbyderne uden udgift for staten at sikre, at deres tekniske systemer og tekniske udstyr er indrettet således, at politiet kan få adgang til oplysninger om bl.a. teletrafik. Det foreslås, at denne ordning videreføres. Udbyderne vil således være forpligtede til at indrette deres tekniske systemer og tekniske udstyr således, at de har kapaciteten til at understøtte de krav, som forslagene medfører.

4. Logning med henblik på bekæmpelse af grov kriminalitet mv.

4.1. Gældende ret

Der henvises til beskrivelsen ovenfor under pkt. 3.1 vedrørende retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786, stk. 4, for teleudbydere til at registrere både tele- og internetkommunikation til brug for efterforskning og retsforfølgning af alle typer strafbare forhold ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for logning med henblik på bekæmpelse af grov kriminalitet mv.

4.2. Relevante dele af La Quadrature du Net-dommen

De centrale dele af EU-Domstolens dom af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår målrettet logning er de relevante dele af dommen præmis 140-151. Det fremgår heraf navnlig,

- at der kan vedtages lovgivning, der som en forebyggende foranstaltning muliggør en målrettet logning af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt med henblik på beskyttelse af den nationale sikkerhed,
- at dette forudsætter, at en sådan logning begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal logges, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af logningen,
- at logningsforpligtelsen kan fastsættes på baggrund af objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafik- og lokaliseringsdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed eller endog en risiko for den nationale sikkerhed (personbestemt målrettet logning),
- at logningsforpligtelsen kan fastsættes på baggrund af et geografisk kriterium, når der på grundlag af objektive og ikke-diskriminerende forhold findes, at der i et eller flere geografiske områder er en forhøjet risiko for, at grov kriminalitet bliver planlagt eller begået, samt at disse områder navnlig kan være steder, der er kendetegnet ved et

højt antal tilfælde af grov kriminalitet, steder, hvor der i særlig grad kan begås grov kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder (geografisk målrettet logning), og

- at varigheden af sådanne foranstaltninger ikke må overstige, hvad der er strengt nødvendigt i forhold til det forfulgte formål og de omstændigheder, der begrunder dem, dog med forbehold af muligheden for at forlænge foranstaltningen som følge af, at det fortsat er nødvendigt at foretage en sådan lagring.

For så vidt angår logning af IP-adresser er de relevante dele af dommen præmis 152-156. Det fremgår heraf navnlig,

- at der kan fastsættes lovgivningsmæssige foranstaltninger, der foreskriver generel og udifferentieret logning af de IP-adresser, der er tildelt kilden til en forbindelse, såfremt det kan begrundes af hensyn til bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, i lighed med beskyttelsen af den nationale sikkerhed,
- at logningsperioden ikke må overstige, hvad der er strengt nødvendigt for at nå det forfulgte formål, og
- at en sådan foranstaltning skal indeholde strenge betingelser og garantier for så vidt angår brugen af disse data, bl.a. ved hjælp af sporing, med hensyn til de kommunikationer og de aktiviteter, som de berørte personer foretager online.

4.3. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan en ordning med logning med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed, kan indrettes. Når der i det følgende henvises til grov kriminalitet "mv.", dækker dette udtryk foruden grov kriminalitet også over alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed.

Det er i den forbindelse af central betydning, hvordan grov kriminalitet mv. defineres. Der henvises til pkt. 7.3.1 nedenfor.

Som det fremgår ovenfor, kan fastsættelse af en forpligtelse til logning med henblik på bekæmpelse af grov kriminalitet mv. ske ved en målrettet logning

(pkt. 4.3.1 og 4.3.2 nedenfor) og en generel og udifferentieret logning af IP-adresser (pkt. 4.3.3 nedenfor).

4.3.1. Personbestemt målrettet logning

Justitsministeriet har overvejet, hvordan en logningsforpligtelse fremadrettet kan målrettes bestemte persongrupper med henblik på bekæmpelse af grov kriminalitet mv.

Efter Justitsministeriets opfattelse har EU-Domstolen fastsat en forholdsvis lav tærskel – jf. anvendelsen af begrebet *"kan afsløre en forbindelse"* – for kravet til, hvor underbygget grundlaget skal være for beslutningen om, at en given person skal være omfattet af et pålæg om personbestemt målrettet logning.

Det er på denne baggrund Justitsministeriets vurdering, at personer kan være omfattet af et pålæg om personbestemt målrettet logning, når myndighederne finder, at visse objektive forhold tilsiger, at trafik- og lokaliseringsdata[8] om den pågældende – direkte eller indirekte – på et senere tidspunkt *kan* tjene til at afsløre en forbindelse til grov kriminalitet mv. Justitsministeriet tillægger det i den forbindelse vægt, at et sådant pålæg alene indebærer, at de pågældende oplysninger opbevares af de berørte teleudbydere i en nærmere fastsat og tidsbegrænset periode. Udlevering af oplysningerne til retshåndhævende myndigheder til brug for efterforskningen mv. af en konkret straffesag vil alene kunne ske, når en domstol konkret vurderer, at retsplejelovens krav er opfyldt, jf. beskrivelsen nedenfor under afsnit 7.

Det foreslås på den baggrund, at en afgrænsning af personkredsen omfattet af et pålæg om personel målrettet logning af hensyn til bekæmpelsen af grov kriminalitet mv. kan indeholde følgende kategorier af personer:

[8] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata".

- Personer der inden for en nærmere bestemt årrække er dømt for grov kriminalitet mv., idet personer, der er dømt for sådan kriminalitet bl.a. må antages at have en forhøjet tendens til at pleje omgang og relationer med personer tilknyttet miljøer, hvor der begås sådan kriminalitet.
- Personer der tidligere har været genstand for indgreb efter retsplejelovens kapitel 71 med henblik på bekæmpelse af grov kriminalitet mv., idet der for at foretage sådanne indgreb stilles særlige krav til navnlig mistankegrundlaget. Således vil det ved en retskendelse være konstateret, at der er grundlag for en mistanke, hvilket efter Justitsministeriets opfattelse kan betegnes som objektive forhold, der kan begrunde, at en person omfattes at et pålæg om personbestemt målrettet logning.
- Personer der tidligere har været i kontakt med personer, som har været aflyttet med henblik på bekæmpelse af grov kriminalitet mv., idet der i givet fald er en indirekte tilknytning til grov kriminalitet mv., der kan bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde, ligesom der må antages at være en vis forhøjet tendens til, at personer, der for nylig har haft kontakt til en aflyttet person, selv er involveret i grov kriminalitet mv., hvilket ofte er tilfældet i efterforskning af alvorlig organiseret kriminalitet, herunder menneskesmugling, handel med euforiserende stoffer samt rocker- og bandekriminalitet.
- Personer som retshåndhævende myndigheder har en konkret formodning om har forbindelse til grov kriminalitet mv., uden at der har været tilstrækkeligt grundlag for at iværksætte indgreb i meddelelseshemmeligheden eller domfælde pågældende. Dette kan f.eks. være personer, som Politiets Efterretningstjeneste behandler oplysninger om, mistænkte inden for områder, der er undergivet systematisk, politimæssig monitering, eksempelvis rocker- og bandemiljøer, personer, der indgår i militant islamistiske grupper, randpersoner fra rocker-/bandemiljøet, personer med kontakt til menneskesmuglere eller andre organiserede kriminelle, herunder nære relationer, som f.eks. ægtefæller eller samlevere til personer, der er genstand for målrettet personel logning eller en konkret efterforskning af grov kriminalitet mv. En sådan kategori indebærer et lavere krav til mistanken mod den enkelte end det, der f.eks. skal opfyldes for at retten kan tillade politiet at foretage aflytning efter retsplejelovens § 780, stk. 1, nr. 1, som er et mere vidtgående indgreb.

Det foreslås på den baggrund, at der indføres en hjemmel til, at politiet kan pålægge teleudbydere mv. personbestemt målrettet logning.

Efterforskningen af sager om grov kriminalitet, der ofte kan have en international dimension, vil ofte strække sig over længere perioder, ligesom grove kriminelle handlinger eller forberedelseshandlinger dertil ofte også vil strække sig over længere perioder. Det opleves endvidere, at når større sager om grov kriminalitet efterforskes over længere tid, vil efterforskningen mange gange kaste lys over ældre forhold, hvor det viser sig, at der er brug for oplysninger længere tilbage i tid. Der henvises endvidere til oven for under afsnit 3.3.2 vedrørende alvorlige trusler mod den nationale sikkerhed.

Det foreslås på den baggrund, at oplysninger, der logges på baggrund af en personbestemt eller geografisk afgrænset logning, skal opbevares i op til 1 år. Det foreslås endvidere, at tidsrummet for pålægget om registrering og opbevaring af oplysninger skal være så kort som muligt og højst kan fastsættes for 1 år ad gangen. Den tidsmæssige udstrækning kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt, så logningen begrænses til det strengt nødvendige.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra "ikke-aktiv" kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet

(IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

Der foreslås endvidere, at der fastsættes nærmere regler om, hvordan det afgøres hvilke telefoner eller kommunikationsenheder, der konkret vil være omfattet af den personbestemte målrettede logning. Dette kan f.eks. indebære, at teleudbydere modtager CPR-numre på de personer, som er genstand for målrettet logning, hvorefter det vil påhvile udbyderne at foretage logning af de abonnementer og enheder, der er tilknyttet den pågældende person. En sådan indretning vil således imødegå, at målpersoner skifter telefoner eller abonnementer.

4.3.2. Geografisk målrettet logning

Justitsministeriet har endvidere overvejet, hvordan logningsforpligtelsen fremadrettet kan målrettes et eller flere geografiske områder med henblik på bekæmpelse af grov kriminalitet mv.

Det er Justitsministeriets opfattelse, at teleudbydere mv. vil kunne pålægges at etablere geografisk målrettet logning ud fra myndighedernes vurdering af – på grundlag af objektive og ikke-diskriminerende forhold – en forhøjet risiko for, at der planlægges eller begås alvorlig kriminalitet i et givent område.

Det vil for det første være muligt at pålægge etablering af målrettet logning på steder, der er kendetegnet ved et højt antal tilfælde af grov kriminalitet mv., f.eks. hvis politiet har konstateret, at der i et givent område – f.eks. en bydel – statistisk set oftere begås grov kriminalitet end andre steder. Der kan

også være tale om, at politiet konstaterer, at der ligger "rockerborge" eller hashklubber mv. i det pågældende område, eller at der aktuelt verserer en rocker/bande konflikt i området. Politiets vurdering af om et område bør omfattes af målrettet logning vil bl.a. kunne baseres på efterretninger og oplysninger fra politiets registre og sagsbehandlingssystemer (eksempelvis POLSAS), der indikerer en varig eller tiltagende tendens til, at grov kriminalitet planlægges eller fuldbyrdes i området.

For det andet vil det være muligt, at pålægge etablering af målrettet logning på steder, hvor der i særlig grad kan begås grov kriminalitet mv., såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer. Herudover kan der i et område også vurderes at være en forhøjet risiko for grov kriminalitet mv. i forbindelse med konkrete begivenheder – f.eks. sportsarrangementer, konferencer eller statsbesøg.

Endelig, og for det tredje, vil det være muligt, at pålægge etablering af målrettet logning på strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

Det vil kunne variere over tid hvor i landet, der er en forhøjet risiko for, at der planlægges eller begås grov kriminalitet mv. Logningen vil således skulle tilpasses løbende ud fra en vurdering af de aktuelle forhold.

Myndighederne – i praksis Rigspolitiet og Politiets Efterretningstjeneste – vil i den forbindelse have pligt til at dokumentere og underbygge grundlaget for den vurdering, der danner baggrund for at pålægge geografisk målrettet logning i et givet område, samt eventuelle efterfølgende revurderinger om, at logning skal opretholdes, således at behovet kan underbygges ved en eventuel efterfølgende domstolsprøvelse. Det bemærkes i den forbindelse, at der i visse områder vil kunne være behov for løbende forlængelser.

Det foreslås på den baggrund, at der indføres hjemmel til, at politiet for op til 1 år kan pålægge teleudbydere mv. målrettet logning for et nærmere afgrænset geografisk område, hvis der på baggrund af objektive og ikke-diskriminerende forhold er grund til at antage, at der er en forhøjet risiko for, at grov kriminalitet mv. bliver planlagt eller begået i området.

Efterforskningen af sager om grov kriminalitet, der ofte kan have en international dimension, vil ofte strække sig over længere perioder, ligesom grove kriminelle handlinger eller forberedelseshandlinger dertil ofte også

vil strække sig over længere perioder. Det opleves endvidere, at når større sager om grov kriminalitet efterforskes over længere tid, vil efterforskningen mange gange kaste lys over ældre forhold, hvor det viser sig, at der er brug for oplysninger længere tilbage i tid. Der henvises endvidere til oven for under afsnit 3.3.2 vedrørende alvorlige trusler mod den nationale sikkerhed.

Det foreslås på den baggrund, at oplysninger, der logges på baggrund af en personbestemt eller geografisk afgrænset logning skal opbevares i op til 1 år. Det foreslås endvidere, at tidsrummet for pålægget om registrering og opbevaring af oplysninger skal være så kort som muligt og kan højst fastsættes for 1 år ad gangen.

Det foreslås, at logningen som udgangspunkt kommer til at omfatte de oplysninger, der i dag logges i henhold til logningsbekendtgørelsens §§ 4-6, dog under hensyntagen til den teknologiske udvikling.

Det foreslås således, at logningen gælder registrering af en række nærmere angivne oplysninger forbundet med anvendelsen af fastnet- og mobiltelefoner, som f.eks. oplysninger om det opkaldende og det opkaldte nummer, tidspunktet for kommunikationens start og afslutning, og – for så vidt angår mobiltelefoni – den eller de celler og placeringen af de tilhørende master, mobiltelefonen er forbundet til under kommunikationen (med udgangspunkt i den gældende § 4 i logningsbekendtgørelsen). Dette kan også omfatte lokaliseringsdata hidrørende fra "ikke-aktiv" kommunikation, f. eks. lokaliseringsdata genereret ved, at en tændt mobiltelefon automatisk kommunikerer sin position til netværket.

Det foreslås endvidere, at det skal gælde visse nærmere angivne oplysninger om en brugers adgang til internettet, som bl.a. tidspunktet for kommunikationens start og afslutning og oplysninger om den tildelte brugeridentitet (IP-adresse, som er nærmere behandlet i pkt. 4.3.3.) på det pågældende tidspunkt (med udgangspunkt i den gældende § 5 i logningsbekendtgørelsen). Endelig foreslås det, at logningen gælder registrering af en række nærmere angivne oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder bl.a. oplysninger om modtagende og afsendende e-mailadresser (med udgangspunkt i den gældende § 6 i logningsbekendtgørelsen).

Det vil skulle overvejes nærmere, hvorvidt det fortsat er relevant, at lade alle de kommunikationsformer, der i dag er oplistet i logningsbekendtgørelsens §§ 4 – 6, være omfattet af logningsforpligtelsen, ligesom det vil skulle overvejes, om nyere kommunikationsformer i stedet bør omfattes, herunder hvilke oplysninger om sådanne kommunikationsformer der i givet fald skal være omfattet af logningen.

4.3.3. Generel og udifferentieret logning af IP-adresser

Justitsministeriet har endvidere overvejet, hvordan der kan fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser med henblik på bekæmpelse af grov kriminalitet mv.

Politiet har ofte behov for at kunne afdække, hvilke brugere, der benytter givne IP-adresser på givne tidspunkter, idet sådanne oplysninger er helt afgørende i forbindelse med efterforskningen af en lang række sager om grov kriminalitet mv. Dette gør sig særligt gældende i forhold til forbrydelser begået i den digitale verden, navnlig digitale sexkrænkelser og seksuelt misbrug af mindreårige, hvor det er en central del af politiets efterforskning at kunne bevise, hvem der har anvendt en IP-adresse på gerningstidspunktet. De seneste års stigning i forekomsten af grov kriminalitet begået gennem brug af internettet, f.eks. hacking, digitale sexkrænkelser og seksuelt misbrug af mindreårige mv., tilsiger generelt, at politiets behov for entydigt og effektivt at kunne fastlægge identiteten på en bruger af en given IP-adresse vil blive af stadig mere central betydning.

Det er Justitsministeriets overordnede vurdering, at de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, der foreskriver generel og udifferentieret logning af de tildelte brugeridentiteter (herunder IP-adresser), der er anvendt ved adgang til internettet, er i overensstemmelse med La Quadrature du Net-dommen.

Samtidig er det Justitsministeriets opfattelse, at det bl.a. på baggrund af den teknologiske udvikling er nødvendigt med en modernisering af de nugældende regler, samt at der er behov for en revision af de regler, der giver adgang til loggede IP-adresser. Det er således Justitsministeriets vurdering, at det af EU-Domstolen anførte i pr. 156 om, at der kan fastsættes nationale regler om generel og udifferentieret logning af IP-adresser, såfremt det kan begrundes af hensyn til bekæmpelsen af grov kriminalitet og forebyggelsen

af alvorlige trusler mod den offentlige sikkerhed, i lighed med beskyttelsen af den nationale sikkerhed, vil kunne sikres ved opstilling af materielle betingelser for politiets adgang til loggede oplysninger om IP-adresser. Der henvises til afsnit 7 for nærmere om adgang til loggede oplysninger.

Det er endvidere Justitsministeriets vurdering, at der foruden logning af selve den IP-adresse, der er anvendt ved adgangen til internettet, også vil kunne ske logning af de såkaldte portnumre (”source port number”), som teleudbydere mv. tildeler slutbrugerne for at identificere trafikken til og fra den enkelte slutbruger. Det skyldes, at der i dag anvendes teknologi, der gør det muligt for et større antal brugere at anvende den samme IP-adresse samtidig, hvorfor en IP-adresse således ikke alene kan tjene til at identificere den fysiske person, der ejer det udstyr gennem teleudbydere mv., hvorfra en kommunikation via internettet foretages. Portnummeret kan – i lighed med IP-adressen – ikke afsløre indholdet af, hvad der bliver kommunikeret om og hvem, der bliver kommunikeret med.

Endvidere vil der efter Justitsministeriets vurdering også kunne ske registrering af det tidspunkt, hvor en slutbruger har været tildelt en given IP-adresse. Det skyldes, at IP-adressen kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som en IP-adresse var tildelt på det tidspunkt, hvor en overtrædelse blev begået. En identifikation af slutbrugeren forudsætter således også registrering af de tidspunkter, hvor en slutbruger har været tildelt en given IP-adresse.

Det foreslås på den baggrund, at der for en periode på 1 år fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser for en brugers adgang til internettet (”kilde-IP-adressen”), logning af det portnummer, der er anvendt ved internetkommunikationen, samt registrering af tidspunktet for tildeling af kilde-IP-adressen og tilhørende portnummer.

Det bemærkes, at det er Justitsministeriets vurdering, at en opbevaringsperiode på 1 år kan anses for begrænset til det strengt nødvendige, idet den helt grundlæggende betydning som internettets udbredelse og anvendelse har for det danske samfund, generelt tilsiger, at politiet skal have mulighed for effektivt at efterforske grov kriminalitet mv. begået eller understøttet gennem brug af internettet i en længere periode. Det bemærkes i den forbindelse, at sager om alvorlig kriminalitet online ofte er komplekse og derfor tager lang tid at efterforske, bl.a. fordi der ofte er en international dimension som f. eks. seksuelt misbrug af børn. Endvidere kan der i sager om alvorlig

organiseret kriminalitet være behov for logning af kilde-IP-adresser i længere tid, idet disse sagstyper ofte involverer en større mængde kommunikationsenheder, som computere og mobiltelefoner, som skal beslaglægges og undersøges med henblik på udfindelse af IT-tekniske spor, såsom IP-adresser på bagmænd.

Det foreslås endvidere, at der kan fastsættes regler, der forpligter teleudbydere til at registrere oplysninger, der identificerer det abonnement, der er benyttet til internetadgangen, f.eks. telefonnummer, der identificerer det benyttede mobilabonnement ved internetadgang via mobildatatjenester, eller ID-nummer, f.eks. kredsløbsnummer, som identificerer det benyttede bredbåndsabonnement ved internetadgang via faste net. Ved afgrænsningen af hvilke oplysninger der kan registreres i tilknytning til en kilde-IP-adresse, tillægger Justitsministeriet det vægt, om de registrerede oplysninger gør det muligt for teleudbyderne over for politiet helt umiddelbart at foretage en entydig identifikation af den slutbruger, der på et givent tidspunkt har været tildelt kilde-IP-adressen til en forbindelse. Der vil ikke kunne fastsættes regler om registrering af oplysninger, der afslører, hvem der er kommunikeret med via kilde-IP-adressen, eller hvad der er kommunikeret om. Der henvises endvidere til EU-Domstolens praksis om identitetsoplysninger som redegjort for i pkt. 2.3 og 2.4.

4.3.4. Retsgarantier og domstolsprøvelse mv.

Justitsministeriet har overvejet, hvordan det kan sikres, at logningen er underlagt strenge garantier, der gør det muligt effektivt at beskytte mod risikoen for misbrug, og hvordan afgørelsen, hvorved der pålægges en målrettet logningsforpligtelse, kan gøres til genstand for en effektiv prøvelse.

Det er Justitsministeriets umiddelbare opfattelse, at de nuværende regler om teleudbydernes behandling af loggede oplysninger, herunder de sektorspecifikke databeskyttelsesregler, samt krav om sikkerhedsgodkendelse mv. kan videreføres, og at disse regler effektivt beskytter mod risikoen for misbrug.[9]

[9] Der kan bl.a. henvises til bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, herunder bekendtgørelsens §§ 10 og 11 om krav til udbydernes behandling af trafik- og lokaliseringsdata

Det er endvidere Justitsministeriets opfattelse, at der vil kunne fastsættes nærmere tekniske krav til udbydernes logning, herunder nærmere regler om opbevaringsformat, foranstaltninger med henblik på at sikre oplysningernes integritet og beskyttelse mod uautoriseret adgang, opbevaringssted mv. Det vil medvirke til at sikre, at der løbende kan ske den fornødne tilpasning i lyset af den teknologiske udvikling.

Der vil endvidere kunne fastsættes nærmere regler om fremgangsmåde mv. for udstedelse af pålæg til teleudbyderne om de personer, der er omfattet af et pålæg om målrettet personel logning.

Der vil også kunne fastsættes nærmere regler om, at oplysninger om f.eks., hvilke konkrete telefoner og kommunikationsenheder der er genstand for personbestemt målrettet logning, samt hvilke geografiske områder, der er omfattet af et pålæg om geografisk afgrænset logning, skal være fortrolige. Endvidere vil der kunne fastsættes regler om, at ansatte ved udbydere, der er underlagt en logningsforpligtelse, har tavshedspligt med hensyn til alle oplysninger modtaget som led i opfyldelsen af logningsforpligtelsen, og at straffelovens §§ 152 og 152 c-152 f finder tilsvarende anvendelse. En sådan regulering vil i øvrigt svare til den gældende tavshedspligt, der er fastsat i telelovens § 7, stk. 2, men vil omfatte enhver, der opnår kendskab til indholdet af et pålæg uanset om de er omfattet af telelovens regulering.

Forpligtelsen til at holde ovennævnte oplysninger fortrolige vil også kunne omfatte en forpligtelse til at sikre, at den enkelte bruger ikke, f.eks. gennem anmodninger om indsigt i egne oplysninger efter de databeskyttelsesretlige regler – eller på anden vis – kan tilegne sig oplysninger om, hvordan den geografiske og personbestemte målrettede logning på et givet tidspunkt er tilrettelagt.

Endelig vil der være mulighed for, at der kan ske en efterfølgende prøvelse ved domstolene ved politiets adgang til loggede oplysninger, hvor der i den forbindelse vil ske en prøvelse af, om proportionalitetskravet er opfyldt.

4.3.5. Forpligtelser for teleudbyderne mv.

Justitsministeriet har overvejet, hvilke forpligtelser for teleudbyderne mv. den foreslåede logning vil medføre, udover selve logningsforpligtelsen.

Det foreslås, at i det omfang, der måtte blive fastsat regler om et fælles opbevaringsformat, og dette adskiller sig fra det af teleudbyderen anvendte, vil det påhvile udbyderen at foretage konvertering af den relevante data, herunder sikring af den fornødne dataintegritet og -kvalitet. Det følger af telelovens § 10, stk. 1, nr. 1, at det påhviler udbyderne uden udgift for staten at sikre, at deres tekniske systemer og tekniske udstyr er indrettet således, at politiet kan få adgang til oplysninger om bl.a. teletrafik. Det foreslås, at denne ordning videreføres. Udbyderne vil således være forpligtede til at indrette deres tekniske systemer og tekniske udstyr således, at de har kapaciteten til at understøtte de krav, som forslagene medfører.

Det vil dog kunne fastsættes nærmere regler om økonomisk godtgørelse for udgifter forbundet med et konkret pålæg om personbestemt eller geografisk målrettet logning. De nærmere regler vil kunne omfatte regler om betingelserne for at yde godtgørelse for udgifter forbundet med et konkret pålæg mv., om standardtakster for godtgørelsen og eventuelt om betingelser for at yde godtgørelse ud over standardtaksterne. I det omfang sådanne regler fastsættes, forudsættes det, at der ikke ydes godtgørelse ud over standardtaksterne, medmindre der ekstraordinært måtte være tale om, at et konkret pålæg mv. medfører uforholdsmæssige udgifter for en udbyder.

Det bemærkes, at det forudsættes, at teleudbyderne ved udstedelse af pålæg om personbestemt eller geografisk målrettet logning kan have fuld klarhed over deres forpligtelser, således at de kan opfylde dem på den hurtigste og mest effektive måde.

Så snart adressaterne modtager og bliver gjort bekendt politiets pålæg, er disse underlagt en retlig handlepligt til at efterkomme pålægget.

Det følger i dag af telelovens § 10, stk. 4, at det påhviler udbyderen at sikre, at politiets anmodninger om fremskaffelse af oplysninger om teletrafik samt historisk teleoplysning og historisk udvidet teleoplysning behandles straks og på en sådan måde, at hensigten med indgrebet ikke forspildes.

Der vil for politiets pålæg om at påbegynde logning kunne fastsættes tilsvarende regler, der specificerer den ovenfor nævnte retlige handlepligt, og som forpligter teleudbyderne til at efterkomme pålægget straks efter modtagelse, således at formålet med pålægget ikke forspildes.

Det bemærkes, at det er Justitsministeriets vurdering, at det ikke vil udgøre en overtrædelse af de sektorspecifikke regler i bl.a. teleloven, hvis en teleudbyder, i overensstemmelse med et pålæg fra f.eks. Rigspolitiet, har foretaget logning, og pålægget senere f.eks. måtte blive underkendt ved en domstolsprøvelse. Ansvaret for at betingelserne for at påbegynde logning er opfyldt ligger således alene hos de myndigheder, der er kompetente til at pålægge logning, og der er ikke noget selvstændigt ansvar for, eller adgang til, at teleudbyderen vælger at foretage en retlig efterprøvelse af, om betingelserne konkret er opfyldt. Enhver efterprøvelse af et pålægs grundlag, udstrækning mv., ligger således i sidste ende hos domstolene. Teleudbyderne vil fra modtagelsen af pålægget være retligt forpligtet til straks at iværksætte logningen.

Foretager teleudbyderen behandling af en eller flere slutbrugeres personoplysninger i form af logning på baggrund af den retlige forpligtelse, et pålæg om logning indebærer, påhviler det samtidig alene teleudbyderen at kunne dokumentere, at et sådant pålæg er udstedt. Såfremt et pålæg konkret måtte give anledning hertil, f.eks. grundet dets omfang, er der imidlertid ikke noget til hinder for, at teleudbyderen søger pålæggets udstrækning bekræftet hos politiet. Politiets bekræftelse heraf vil i den forbindelse være tilstrækkelig dokumentation for, at teleudbyderen har sikret den fornødne dokumentation af grundlaget for den iværksatte logning.

5. Hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed

5.1. Gældende ret

Retsplejelovens § 786 a blev indsat ved § 2 i lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven. Bestemmelsen trådte i kraft den 1. juli 2004.

Retsplejelovens § 786 a blev indsat med henblik på at opfylde forpligtelserne til at fastsætte regler om hastesikring af elektronisk data efter artikel 16 og 17 i Europarådets konvention om IT-kriminalitet (CETS nr. 185), jf. pkt. 7.3 i de almindelige bemærkninger i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1812. Formålet med bestemmelsen var at sikre, at politiet kan udstede pålæg og sikring af elektroniske data med henblik på, at oplysningerne er tilstede og – hvis betingelserne herfor

er opfyldt – på et senere tidspunkt kan udleveres til politiet til brug for efterforskningen.

Efter retsplejelovens § 786 a, stk. 1, kan politiet som led i en efterforskning, hvor elektronisk bevismateriale kan være af betydning, meddele udbydere af telenet og teletjenester pålæg om at foretage hastesikring af elektroniske data, herunder trafikdata.

Det følger af retsplejelovens § 786 a, stk. 2, at et pålæg om hastesikring alene kan omfatte elektroniske data, som opbevares på det tidspunkt, hvor pålægget meddeles. I pålægget skal det anføres, hvilke data der skal sikres, og i hvilket tidsrum de skal sikres (sikringsperioden). Pålægget skal afgrænses til alene at omfatte de data, der skønnes nødvendige for efterforskningen, og sikringsperioden skal være så kort som mulig og kan ikke overstige 90 dage. Et pålæg kan ikke forlænges.

Det fremgår af forarbejderne til loven (bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827), at retsplejelovens § 786 a, stk. 1, omfatter alle elektroniske data - det vil sige både indholdsdata, trafikdata og øvrige elektroniske data, f.eks. oplysninger om navn og adresse på en internetudbyder eller et teleselskabs kunder (kundeoplysninger).

Det fremgår endvidere af forarbejderne til loven (bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827), at både udbydere af offentlige telenet og teletjenester samt udbydere, der henvender sig til specifikke, på forhånd afgrænsede kundesegmenter, er omfattet af bestemmelsen.

Efter retsplejelovens § 786 a, stk. 3, påhviler det udbydere af telenet og teletjenester som led i hastesikring efter retsplejelovens § 786 a, stk. 1, uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere, hvis net eller tjenester har været anvendt i forbindelse med den elektroniske kommunikation, som kan være af betydning for efterforskningen.

Retsplejelovens § 786 a, stk. 3, omfatter alene trafikdata. Oplysningerne, som udbydere af telenet og teletjenester skal videregive til politiet, er alene oplysninger om de elektroniske stier, som føres fra den pågældende udbyder

til en eller flere andre udbydere, jf. bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, Tillæg A, s. 1827.

Forsætlig eller uagtsom overtrædelse af pligten til at sikre elektroniske data og pligten til uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere kan straffes med bøde, jf. retsplejelovens § 786 a, stk. 4.

De nærmere betingelser for, hvornår teleudbydere skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. nærmere herom nedenfor under pkt. 7.1.

Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786 a for teleudbydere til at sikre elektroniske data og pligten til uden ugrundet ophold at videregive trafikdata om andre telenet- eller teletjenesteudbydere ikke differentierer efter karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for hastesikring af data med henblik på bekæmpelse af grov kriminalitet eller beskyttelsen af den nationale sikkerhed.

5.2. Relevante dele af La Quadrature du Net-dommen

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen er gennemgået under afsnit 2.

For så vidt angår hastesikring af elektronisk data er de relevante dele af dommen præmis 160-165. Det fremgår heraf navnlig,

- at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere mv. en hurtig lagring af trafik- og lokaliseringsdata, som de allerede råder over, f.eks. som led i lovlig forretningspraksis eller lignende eller som følge af en retlig forpligtelse,
- at de trafik- og lokaliseringsdata, som behandles og lagres af teleudbyderne, principielt skal slettes eller gøres anonyme efter udløbet af de lovbestemte frister, der er fastsat i overensstemmelse med gennemførelsen af e-databeskyttelsesdirektivet,
- at der kan opstå situationer, hvori det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed,

- at der således i visse situationer i et udvidet omfang kan ske hurtig lagring af data, f.eks. fra det geografiske område, hvor en forbrydelse netop er begået eller planlagt, eller fra personer, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds,
- at en sådan hurtig lagring udelukkende kan ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske.

5.3. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan en ordning med hastesikring af trafik- og lokaliseringsdata[10] med henblik på bekæmpelse af grov kriminalitet samt beskyttelse af den nationale sikkerhed kan indrettes. Ved hastesikring forstås et indgreb, der pålægger udbyderne at sikre og opbevare trafik- og lokaliseringsdata, som de råder over, i en længere periode end det sædvanligvis er tilladt (”hurtig lagring” i La Quadrature du Net-dommen).

Det er Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter La Quadrature du Net-dommen ikke vil kunne begrundes af hensyn til bekæmpelsen af almindelig kriminalitet.

I lyset af Domstolens bemærkninger i dommens præmis 160ff er det Justitsministeriets opfattelse, at denne vurdering tillige gør sig gældende for regler, der tillader, at politiet i konkrete tilfælde kan pålægge udbydere af elektroniske kommunikationsnet- og tjenester at foretage en hastesikring af de trafik- og lokaliseringsdata, som de råder over. Det er således Justitsministeriets opfattelse, at politiets adgang til at pålægge hastesikring af trafik- og lokaliseringsdata, som udbyderne råder over, alene vil kunne anvendes, når

[10] I La Quadrature du Net-dommen behandles bl.a. spørgsmålet om logning af og adgang til ”lokaliseringsdata”. Begrebet i dommen skal forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter ”lokaliseringsdata” forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender. Begrebet anvendes på samme måde her. I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet ”historiske masteoplysninger”. Når begrebet ”lokaliseringsdata” i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb ”signaleringsdata”.

det sker af hensyn til bekæmpelse af grov kriminalitet og beskyttelsen af den nationale sikkerhed.

Der er på den baggrund tillige behov for en ændring af de gældende regler i retsplejelovens § 786 a om hastesikring af elektronisk data, så der for trafik- og lokaliseringsdata indføres et kriminalitetskrav, der lever op til EU-Domstolens praksis. Det bemærkes, at § 786 a som nævnt ovenfor også omfatter indholdsdata og øvrige elektroniske data, som ikke umiddelbart er omfattet af dommen. Disse elementer vil blive nærmere overvejet.

Det er Justitsministeriets vurdering, at et pålæg om hastesikring af trafik- og lokaliseringsdata fremadrettet vil kunne ske for at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. For Justitsministeriets overvejelser vedrørende den nærmere afgrænsning af grov kriminalitet henvises til nedenfor under pkt. 7.1.3.

Brugen af et pålæg om hastesikring kan overordnet tænkes anvendt i to forskellige scenarier.

For det første kan et pålæg tænkes anvendt i forhold til trafik- og lokaliseringsdata, der ikke er logningspligtige, men som udbyderen behandler som led i dets egen lovlige forretningspraksis, f. eks. data, der behandles til brug for fejlretning og debitering.

I sådanne tilfælde vil et pålæg om hastesikring indebære, at udbyderen skal opbevare data ud over de frister, der ellers måtte gælde for opbevaring til sådanne formål. Eksempelvis må udbyderne behandle og opbevare trafikdata til brug for debitering af abonnenter og afregning for samtrafik, indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger. I et sådant tilfælde vil et pålæg om hastesikring kunne anvendes til at opbevare data i en periode ud over denne frist.

For det andet kan et pålæg tænkes anvendt i forhold til trafik- og lokaliseringsdata, som udbyderne opbevarer som følge af en retlig forpligtelse, der er vedtaget i henhold til e-databeskyttelsesdirektivets artikel 15, stk. 1, f.eks. en logningsforpligtelse.

I sådanne tilfælde vil et pålæg om hastesikring indebære, at udbyderen skal opbevare data ud over de frister, der følger af logningsforpligtelsen. Er der eksempelvis grundlag for at udstede et pålæg om hastesikring af data, der tillige er genstand for målrettet geografisk logning, vil pålægget kunne anvendes til at forlænge den periode, som udbyderne ellers måtte være forpligtet til at opbevare den pågældende data i henhold til reglerne for målrettet geografisk logning.

Justitsministeriet har overvejet, hvilke betingelser der skal til for et pålæg om hastesikring. Det vil som nævnt være et krav, at et pålæg om hastesikring sker af hensyn til at efterforske eller beskytte mod grov kriminalitet og handlinger, der kan skade den nationale sikkerhed, hvor handlingen er begået, eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske. Det er dog ikke et krav, at oplysningerne vedrører personer, der konkret er mistænkt for at have begået en grov strafbar handling eller et angreb mod den nationale sikkerhed, men oplysningerne skal kunne bidrage til opklaringen af en sådan handling eller angreb.

Ifølge La Quadrature du Net-dommen kan dette omfatte oplysninger om offeret for den strafbare handling eller angrebet, om den pågældendes sociale og arbejdsmæssige omgangskreds eller om bestemte geografiske områder, såsom de steder, hvor den omhandlede strafbare handling eller det omhandlede angreb mod den nationale sikkerhed blev begået eller planlagt.

Det forslås på den baggrund, at der indføres hjemmel til at udstede et pålæg om hastesikring af trafik- og lokaliseringsdata i følgende situationer, hvor en given handling er begået, planlagt eller hvor der ud fra en objektiv vurdering af omstændighederne er en overhængende risiko for, at dette vil ske:

- Hvis der på et bestemt sted er blevet begået eller planlagt en grov kriminalitet eller et angreb mod den nationale sikkerhed. I den situation vil der kunne pålægges hastesikring af trafik- og lokaliseringsdata med tilknytning til området, f.eks. data fra de master, der dækker området.
- Hvis der på et bestemt sted er indikationer på, at et pålæg om hastesikring kan bidrage til efterforskningen af grov kriminalitet eller et angreb mod den nationale sikkerhed. Dette kan for eksempel være tilfældet, når der i efterforskningen foreligger indikationer på, at en

eller flere gerningsmænd i tiden umiddelbart op til eller efter gerningstidspunktet har passeret bestemte områder, og hvor oplysninger vedrørende disse steder kan bidrage til opklaringen.

- Hvis der ud fra en konkret vurdering er grundlag for et pålæg vedrørende en mistænkt person eller en person eller personkreds, der ikke direkte er mistænkte, men hvis oplysninger kaster lys over forbrydelsen. Dette vil bero på en politifaglig vurdering af den konkrete sags omstændigheder om hvilke personers data, der kan bidrage til efterforskningen. Disse personer og personkredse kan bl.a. omfatte offeret og den mistænktes sociale og arbejdsmæssige omgangskreds foruden den mistænkte selv.

Pålægget vil kunne anvendes både i de tilfælde, hvor politiet får kendskab til en grov strafbar handling umiddelbart efter gerningstidspunktet, men også i tilfælde, hvor politiet først får kendskab til handlingen en rum tid efter, at den blev begået. Råder udbyderne konkret over data, der kan bidrage til opklaringen af en grov strafbar handling mv., vil disse således også kunne omfattes af et pålæg om hastesikring, uanset hvor gamle de er.

Den udløsende faktor for, om data kan være genstand for et pålæg om hastesikring, er, at oplysningerne kan bidrage til opklaringen af grov kriminalitet eller et angreb mod den nationale sikkerhed. De pågældende trafik- og lokaliseringsdata skal med andre ord have efterforskningsmæssig værdi, hvilket er et parameter, det i første række tilkommer politiet at vurdere.

Det bemærkes i den forbindelse, at navnlig de indledende stadier af en efterforskning ofte er kendetegnet ved en meget bred indsamling af oplysninger, herunder om personer, der umiddelbart eller over tid viser sig ikke at have betydning for sagen.

Særligt for så vidt angår de pålæg om hastesikring af trafik- og lokaliseringsdata, der sker i nær tilknytning til en strafbars handlings gerningstidspunkt, kan der derfor efter Justitsministeriets opfattelse ikke stilles store krav til, i hvor høj grad disse efterfølgende kan antages at bidrage til opklaringen. Det tillægges i den forbindelse vægt, at et pålæg om hastesikring ikke giver politiet adgang til de pågældende oplysninger, men alene tjener det formål at sikre, at oplysningerne er til rådighed, når politiet opnår rettens som udgangspunkt forudgående godkendelse til, at der kan gives adgang hertil. Eksempelvis vil det forhold, at der på en given lokation er konstateret

en grov strafbar handling i sig selv være nok til, at der kan pålægges hastesikring af data med tilknytning til området.

For så vidt angår de processuelle betingelser for at pålægge hastesikring foreslås det, at politiet gives beføjelse til at vurdere og beslutte, hvilke trafik- og lokaliseringsdata, herunder for hvilken periode, der i den konkrete sag kan bidrage til opklaringen, og derefter udstede pålæg om hastesikring af disse til de relevante udbydere.

Politiet vil endvidere også indledningsvis skulle vurdere, om en hændelse konkret udgør en grov strafbar handling, og der må i den forbindelse indrømmes politiet en vis skønsmargin. Det kan f.eks. ikke afvises, at der vil være tilfælde, hvor det ikke øjeblikkeligt står klart, om der er tale om en grov strafbar handling eller et angreb på den nationale sikkerhed, f. eks. ved større ulykkestilfælde eller større uvarslede hændelser. Der vil således kunne udstedes pålæg, når politiet har rimelig grund til at mistænke, at der er begået en grov strafbar handling mv. For Justitsministeriets overvejelser vedrørende den nærmere afgrænsning af grov kriminalitet henvises til nedenfor under pkt. 7.1.3.

Det vil også kunne påhvile politiet at vurdere og beslutte et pålægs tidsmæssige udstrækning. Ved et pålægs tidsmæssige udstrækning forstås den periode, som udbyderne forpligtes til at opbevare den pågældende data i. Fælles for både den omhandlede data og opbevaringsperioden er, at politiet skal begrænse dette til det strengt nødvendige.

Der forudsættes ikke forudgående høring af adressaterne for pålægget, som endvidere vil være pligtige til at efterkomme pålægget straks efter modtagelse. Den udbyder, der mødes med et pålæg om hastesikring, vil kunne være forpligtet til at sikre integriteten af den data, som er genstand for pålægget, og pålægget vil gælde for dataen i udbyderens samlede net. Det foreslås, at dette indebærer, at der ikke må ske aggregering af dataen i forbindelse med sikringen og opbevaringen.

Endelig vil der kunne sikres mulighed for, at et pålæg om hastesikring på begæring kan indbringes for domstolene med henblik på at opnå rettens stillingtagen til, hvorvidt betingelserne for at pålægge hastesikring i den konkrete situation er opfyldt. Indbringelse for retten foreslås dog ikke at have opsættende virkning.

6. Udlevering af basale oplysninger, krav om registrering af taletidskort og logning af oplysninger om civil identitet

6.1. Gældende ret

6.1.1. Teleloven

Det følger af telelovens § 13, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere på begæring af politiet skal udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller –tjenester.

Telelovens § 13 er en uændret videreførelse af den tidligere § 15 c i telekonkurrenceloven. Det fremgår af de specielle bemærkninger til denne bestemmelse, at bestemmelsen vil give politiet adgang uden retskendelse til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, der ikke er indeholdt i 118-databasen, og som udbyderen er i besiddelse af. Den udbyder, der har slutbrugerforholdet, vil således være forpligtet til at udlevere oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester til politiet, herunder oplysninger om slutbrugerens adgang til internettet (IP-adresser og e-mailadresser), uden at betingelserne for edition skal være opfyldt. Der er således alene tale om oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger. Heraf følger, at der ikke er tale om oplysninger om betalingsmidler el. lign.

Der er både tale om navn til nummer og nummer til navn oplysninger. Bestemmelsen omfatter alene statiske oplysninger, idet registrering af dynamiske IP-adresser mv. vil ske i medfør af logningsforpligtelsen i retsplejeloven.

Telelovens § 13 har til formål at sikre politiet en hurtig og effektiv adgang til samtlige relevante oplysninger om en mistænkts eventuelle kommunikationsmuligheder og skabe overblik over pågældendes kommunikationsmuligheder – uden at skulle afvente kendelse om edition.

Telelovens § 13 berører derimod ikke den adgang til oplysninger om forbindelser mellem telefoner mv., som reguleres af reglerne retsplejelovens kap. 71 om indgreb i meddelelseshemmeligheden.

Bestemmelsen blev indsat på baggrund af overvejelser om danske samfunds beredskab og indsats mod terrorhandlinger, men bestemmelsen har efter dens ordlyd og forarbejder ingen kriminalitetskrav mv. Bestemmelsen vil således kunne anvendes til brug for politiets efterforskning af ethvert strafbart forhold, men også som led i politiets øvrige opgavevaretagelse, jf. politilovens § 2.

En anmodning fra politiet efter telelovens § 13, og et pålæg om edition fra domstolene, har således det til fælles, at de undergiver adressaten en aktiv handlepligt til at fremkomme med alle de oplysninger, som pålægget omhandler, og i den form som oplysningerne foreligger.

6.1.2. Logningsbekendtgørelsen

Som nævnt ovenfor under pkt. 3.1. følger det af logningsbekendtgørelsens § 4, stk. 1, nr. 8, at der skal foretages registrering af tidspunktet for første aktivering af anonyme tjenester (taletidskort).

Udbydere af forudbetalte anonyme tjenester (taletidskort) skal således registrere dato og tidspunkt for første aktivering af tjenesten og oplysninger om den mast, hvorfra aktiveringen blev foretaget. Udbyderne skal herudover registrere de oplysninger, der i øvrigt skal registreres for mobiltelefoni, jf. bekendtgørelsens § 3, på en bruger, der anvender taletidskort i udbyderens net. Dog vil oplysninger om f.eks. navn og adresse ikke nødvendigvis kunne registreres for brugere, der anvender taletidskort i udbyderens net, idet disse oplysninger typisk er ukendte for udbyderen. Oplysningerne vil – i overensstemmelse med bekendtgørelsens anvendelsesområde – alene skulle registreres, hvis de er kendte for udbyderne eller genereres eller behandles i udbydernes systemer.

6.2. Relevante dele af EU-Domstolens praksis

Dommen af 6. oktober 2020 i La Quadrature du Net-sagen samt Ministerio Fiscal-dommen er gennemgået under afsnit 2.

For så vidt angår identitetsoplysninger er de relevante dele af La Quadrature du Net-dommen præmis 157-159. Det fremgår heraf navnlig,

- at data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, principielt ikke kan kvalificeres som et alvorligt

indgreb i grundlæggende rettigheder, og at logning og adgang til disse data alene med henblik på at identificere den pågældende bruger, og uden at de nævnte data kan kædes sammen med oplysninger om den foretagne kommunikation, kan begrundes i det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed samt beskyttelse af den offentlige sikkerhed, og

- at dette også gælder i tilfælde, hvor der ikke foreligger nogen forbindelse mellem samtlige brugere af elektroniske kommunikationsmidler og de forfulgte mål, eller der ikke er fastsat en særlig frist for en sådan logning.

6.3. Justitsministeriets overvejelser og den foreslåede ordning

Oplysninger om identiteten på brugerne af elektroniske kommunikationsmidler må efter Justitsministeriets opfattelse omfatte abonnentoplysninger i form af den fysiske eller juridiske persons navn, adresse og telefonnumre for både fastnet- og mobilabonnenter, og for mobilabonnenters vedkommende også numre, der identificerer det anvendte mobilabonnement, f.eks. IMSI-numre.

Afgrænsningen, af hvilke oplysninger der i øvrigt kan være omfattet af den generelle og udifferentierede logningsforpligtelse, må efter Justitsministeriets vurdering på baggrund af EU-Domstolens praksis kunne finde sted på baggrund af, om oplysningerne kun kan anvendes til at identificere den omhandlede bruger, og at de ikke i sig selv gør det muligt at fastlægge datoen, tidspunktet, varigheden og modtagerne af foretagne kommunikationer, eller de steder, hvor en kommunikation har fundet sted eller hyppigheden heraf med visse personer i en bestemt periode.

Det vurderes på den baggrund, at der tillige kan pålægges registrering og opbevaring af oplysninger, der entydigt identificerer den enhed (mobiltelefon, tablet, PC mv.), som brugeren ejer eller anvender (herunder IMEI-numre og MAC-adresser mv.).

6.3.1. Behov for ændring af telelovens § 13 og overførsel af bestemmelsen til retsplejeloven

Det følger af den gældende bestemmelse i telelovens § 13, at teleselskaberne på begæring af politiet skal udlevere oplysninger, der identificerer en slut-

brugers adgang til elektroniske kommunikationsnet eller -tjenester. Bestemmelsen giver politiet adgang, uden kendelse, til oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, herunder IP-adresser og mail-adresser.

Bestemmelsen omfatter alene oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjenester har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger.

Bestemmelsen omfatter ikke en pligt for udbyderen til at udlevere oplysninger om hvilke telefonnumre, der er anvendt i forbindelse med et givent IMEI-nummer/mobilterminal, henholdsvis hvilke IMEI-numre/mobilterminaler, der er anvendt i forbindelse med et telefonnummer (såkaldt IMEI-oplysning). Bestemmelsen indebærer dog heller ikke, at udleveringen af sådanne oplysninger ikke må finde sted.

Det er nødvendigt at ændre bestemmelsen for at tage højde for det nye foreslåede regime for logning af IP-adresser, jf. ovenfor under pkt. 4.3.3. Behovet for at ændre bestemmelsen er endvidere aktualiseret af en varierende praksis hos teleudbyderne med hensyn til, om udlevering af oplysninger knyttet til et IMEI-nummer forudsætter editionskendelse.

Indhentelse af oplysninger om hvilke mobiltelefoner mv., der har været anvendt til et mobilabonnement og omvendt, er et centralt indledende efterforskningsskridt, der sætter politiet i stand til umiddelbart at træffe beslutning om, hvorvidt der er grundlag for at iværksætte indgreb efter retsplejelovens regler, herunder indgreb i meddelelseshemmeligheden eller pålæg om edition. Hvis dette er tilfældet, iværksættes indgrebet i overensstemmelse med retsplejelovens regler på baggrund af enten forudgående retskendelse, eller på øjemedet efterfulgt af rettens kendelse.

Dette indledende efterforskningsskridt anvendes ofte på den måde, at politiet, der kender et telefonnummer, anmoder teleudbyderne om at oplyse nærmere om aktiviteten på teleudbyderens net knyttet til dette telefonnummer i en given periode. Det foreslås, at det fastsættes entydigt, at teleudbyderen i den forbindelse vil kunne pålægges at oplyse, hvilket IMEI-nummer der f.eks. har været knyttet til et konkret telefonnummer, jf. nærmere herom nedenfor. Dette IMEI-nummer vil derefter blive sendt retur til teleudbyderne med henblik på at fastslå, om det er kendt med andre telefonnumre.

Hvis politiet omvendt kender IMEI-nummeret, vil teleudbyderne blive anmodet om at oplyse tilknyttede telefonnumre.

Dette efterforskningsskridt anvendes til helt indledningsvis at fastlægge en mulig sammenhæng mellem fysiske personer og kommunikationsenheder, f.eks. i forhold til mistænkte målpersoner, eller i tilfælde, hvor en telefon er blevet stjålet. Efterforskningsskridtet er f.eks. særligt relevant i de tilfælde, hvor personer under mistanke for strafbar virksomhed skifter mellem flere SIM-kort og flere telefoner.

Ved at ændre og flytte bestemmelsen til retsplejeloven skabes der således dels en entydig forpligtelse for udbydere af elektroniske kommunikationsnet og -tjenester til slutbrugere til at udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester. Dels skabes der ensretning og transparens på området for indhentning af oplysninger fra udbyderne af elektroniske kommunikationsnet og -tjenester til slutbrugere.

Det foreslås på den baggrund, at telelovens § 13 nyaffattes og overflyttes til retsplejeloven, så der skabes en klar hjemmel til, at udbydere af elektroniske kommunikationsnet og -tjenester – i overensstemmelse med EU-Domstolens praksis – kan pålægges at udlevere basale oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet og -tjenester til politiet.

Dette omfatter oplysninger, der angiver, om en slutbruger har benyttet udbyderens elektroniske kommunikationsnet eller -tjenester inden for en nærmere angiven periode, herunder oplysninger om IMEI-nummer, og de nødvendige oplysninger om aktiviteten knyttet hertil. Dermed vil bestemmelsen således også omfatte oplysninger om, hvilke mobiltelefoner eller andre tilsvarende kommunikationsapparater, der har været anvendt til et mobilabonnement, og omvendt. Bestemmelsen vil i den forbindelse også omfatte basale oplysninger om slutbrugeren, herunder oplysninger om hvilke mobilabonnementer og kommunikationsenheder en slutbruger er registreret med. Bestemmelsen vil dog ikke omfatte IP-adresser, der vil blive omfattet af det foreslåede regime for logning af IP-adresser, jf. ovenfor under pkt. 4.3.3.

Bestemmelsen foreslås udformet teknologineutralt, således at hvis der som følge af den almindelige teknologiske udvikling opstår nye oplysningstyper, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet

eller -tjenester, eller som identificerer en mobiltelefon mv., eller et mobilabonnement, vil disse således også kunne omfattes af bestemmelsen.

På teknologiens nuværende stadie betyder det, at navnlig IMEI-nummer, IMSI-nummer og telefonnummer, vil være omfattet.

I overensstemmelse med det almindelige proportionalitetsprincip forudsættes det, at politiet kun indhenter de omhandlede oplysninger, for en begrænset periode, og at denne periode er så kort som muligt, vurderet ud fra den enkelte sags omstændigheder.

I modsætning til det nuværende anvendelsesområde for telelovens § 13, foreslås det, at den nye bestemmelse i retsplejeloven i dets helhed fremover kun vil kunne anvendes til brug for politiets efterforskning af lovovertrædelser, men ikke til politiets øvrige opgavevaretagelse.

Denne indsnævring i anvendelsesområdet er begrundet i behovet for at bringe bestemmelsen i fuld overensstemmelse med EU-Domstolens dom af 2. oktober 2018, Ministerio Fiscal, der som nævnt fastlog, at adgang til oplysninger svarende til den foreslåede bestemmelse ikke kunne kvalificeres som et "alvorligt" indgreb i de grundlæggende rettigheder for de personer, hvis data er omfattet, og at adgangen hertil kunne begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af "straffelovsovertrædelser" generelt.

På den baggrund foreslås det, at udlevering vil kunne ske med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser generelt.

6.3.2. Behov for registrering af identitetsoplysninger på taletidskort

Når man tegner et mobilabonnement, skal man identificere sig selv over for mobilselskabet. Et sådan krav er der ikke ved køb af taletidskort. Der kan man gå ind fra gaden og købe et taletidskort og et nyt nummer, uden nogen som helst form for registrering.

Det har tidligere været diskuteret, hvorvidt der skulle indføres regler for registrering af taletidskort, idet teleoplysninger er en central del af politiets

efterforskning. I lyset af, at politiets anvendelsesmuligheder for loggede teleoplysninger i fremtiden bliver meget begrænset, er der behov for, at de få tilbageværende redskaber bliver så effektive som muligt.

Den forsatte adgang til at benytte uregistrerede taletidskort – sammenholdt med de fremtidige begrænsninger i logningen af teleoplysninger – må anses for at udgøre en væsentlig risiko for at omgå disse redskaber, med en deraf følgende negativ påvirkning af politiets muligheder for at forebygge, efterforske, afsløre og retsforfølge kriminalitet. Det må endvidere forventes, at organiserede kriminelle mv. vil udnytte sådanne sårbarheder.

Med henblik på at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse i forhold til oplysninger om brugeres civile identitet, har Justitsministeriet således fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til nærmere overvejelse. Dette er begrundet i hensynet til at minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle mv.

Det er Justitsministeriets vurdering, at La Quadrature du Net-dommen giver mulighed for at fastsætte regler om generel og udifferentieret logning af identitetsoplysninger på brugere af elektroniske kommunikationsmidler med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed samt beskyttelse af den offentlige sikkerhed, og at dette kan ske, uden er at der fastsæt en særlig frist for en sådan logning.

Det foreslås på den baggrund, at der stilles krav om, at der ved uregistrerede taletidskort fremadrettet ved salget af taletidskort er en forpligtelse til at registrere oplysninger om køberens civile identitet.

Det vil blive nærmere overvejet, om der herudover er behov for yderligere at forpligte teleudbydere mv. til at foretage registrering og opbevaring af oplysninger om alle brugeres civile identitet, både fysiske eller juridiske personer, herunder navn, adresse og telefonnumre for både fastnet- og mobilabonnenter og SIM-kortnumre (IMSI-nummer), og oplysninger der entydigt identificerer den anvendte enhed i form af IMEI-nummer og MAC-adresse.

7. Adgang til loggede oplysninger

7.1. Gældende ret

7.1.1. Retsplejelovens regler om myndighedernes adgang til loggede trafikdata

Retsplejelovens regler om edition giver myndighederne mulighed for at meddele teleudbydere mv. pålæg om at udlevere oplysninger, jf. retsplejelovens § 804, stk. 1. Lovens § 801, stk. 3, 1. pkt., fastslår imidlertid, at reglerne i lovens kapitel 71 om indgreb i meddelelseshemmeligheden mv. gælder for bl.a. oplysning om forbindelse mellem telefoner mv. Det kan i den forbindelse nævnes, at Højesteret i to afgørelser gengivet i Ugeskrift for Retsvæsen 1993, s. 1, og 1995, s. 374, har fastslået, at retten kun kan give telefonselskaber pålæg om edition med hensyn til teleoplysninger, dvs. trafikdata, hvis også betingelserne i retsplejelovens § 781 om indgreb i meddelelseshemmeligheden er opfyldt.

Betingelserne for myndighedernes mulighed for at få adgang til teleoplysninger, som teleudbyderne har lagret i medfør af retsplejelovens § 786, stk. 4, og logningsbekendtgørelsens regler, reguleres derfor i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden mv.

Efter retsplejelovens § 780, stk. 1, nr. 3, kan politiet foretage indgreb i meddelelseshemmeligheden ved at indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsmiddel, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning). Ved indgrebet opnår politiet ikke kendskab til kommunikationens indhold, men kun til dens eksistens.

Retsplejelovens § 780, stk. 1, nr. 3, er efter sin ordlyd ikke begrænset til bestemte typer af oplysninger, der kan indhentes. Det fremgår af forarbejderne til bestemmelsen, at "teleoplysning" omfatter telefonnumre, jf. pkt. 2.4.1 i de almindelige bemærkninger til lovforslag nr. L 164A af 1. februar 1985, jf. Folketingstidende 1984-85, Tillæg A, sp. 2972. Teleoplysninger kan også være oplysninger om, hvilken eller hvilke master og masteceller den omhandlede telefon registreres på (masteoplysninger).

Udlevering af oplysninger om, hvilke telefoner eller tilsvarende kommunikationsapparat der har taget kontakt til en bestemt telefon mv., udgør ikke et indgreb i meddelelseshemmeligheden, hvis der er samtykke fra indehaveren af telefonen, jf. bemærkningerne til § 780 i lovforslag nr. L 164A af 1. februar 1985, jf. Folketingstidende, 1984-85, Tillæg A, sp. 3000. Udbydere af telenet eller telefontjenester kan pålægges at udlevere sådanne oplysninger, uden at betingelserne for at foretage indgreb i meddelelseshemmeligheden skal være opfyldt, jf. retsplejelovens § 786, stk. 2.

Reglerne vedrørende teleoplysning finder kun anvendelse, når der skal indhentes oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater, der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat. Hvis der alene er tale om oplysninger om, at eksempelvis en bestemt telefon har været registreret på en bestemt sendemast (historisk), indhentes der efter reglerne om edition, jf. nærmere nedenfor under pkt. 7.1.3 om edition.

Højesteret fastslog ved kendelse af 7. maj 1997, gengivet i Ugeskrift for Retsvæsen, 1997, s. 1021 f., at retsplejelovens regler om teleoplysning, jf. § 780, stk. 1, nr. 3, giver hjemmel for indhentelse af teleoplysninger ikke blot om, hvilke telefoner mv., der har været sat i forbindelse med et bestemt telefonnummer, men også om, hvilke telefoner, der har været sat i forbindelse med telefoner på en nærmere angiven adresse, selv om numrene på telefonerne dér ikke på forhånd har kunnet angives. Derimod fandt Højesteret, at bestemmelsen ikke indeholder fornøden hjemmel til at indhente oplysninger om hvilke mobiltelefoner, der i en nærmere angiven periode havde været sat i forbindelse med hinanden via sendemaster inden for en radius af 1 km fra en nærmere angiven adresse. For den sidstnævnte type af oplysninger anvendes reglerne om udvidet teleoplysninger i § 780. stk. 1, nr. 4, jf. pkt. 7.1.2.

De almindelige betingelser for at foretage indgreb i meddelelseshemmeligheden, herunder i form af teleoplysning, findes i retsplejelovens § 781, stk. 1. Betingelserne er, at der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt (mistankekravet), og at indgrebet må antages at være af afgørende betydning for efterforskningen (indikationskravet), jf. retsplejelovens § 781, stk. 1, nr. 1 og 2.

Herudover er det en betingelse, at efterforskningen vedrører en af de lovovertrædelser, der er omfattet af § 781, stk. 1, nr. 3, stk. 2 og stk. 3 (kriminalitetskravet). Disse lovovertrædelser er dels afgrænset ved en generel henvisning til alle lovovertrædelser med en bestemt strafferamme dels specificeret ved henvisning til kapitler i straffeloven eller til lovbestemmelser.

Efter § 781, stk. 1, nr. 3, er det således en betingelse for at kunne foretage indgreb i meddelelseshemmeligheden, at efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitler 12 eller 13 eller en overtrædelse af straffelovens § 124, stk. 2 (befrielse af en anholdt eller fængslet mv), § 125 (hjælp til at unddrage nogen fra forfølgning for en forbrydelse mv.), § 127, stk. 1 (unddragelse af krigstjeneste mv.), § 233, stk. 1 (rufferi), § 235 (børnepornografi), § 266 (trusler), § 281 (afpresning) eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5 (forskellige former for forsætlig bistand til en udlænding med ulovlig indrejse, ophold eller lignende).

Kriminalitetskravet vedrørende forbrydelser, som efter loven kan medføre en straf på fængsel i 6 år eller derover blev i forarbejderne begrundet med, at lovovertrædelser, hvor strafferammen når op på fængsel i mindst 6 år, typisk er så alvorlige og af en sådan art, at det er både rimeligt og hensigtsmæssigt at give adgang til indgreb i meddelelseshemmeligheden, og at grænsen harmonerede med, at der i de senere år forud for lovforslaget var sket en nedsættelse af strafferammerne for visse forbrydelser og at dette også ville gøre sig gældende i fremtiden. Der henvises til pkt. 2.4.1 i de almindelige bemærkninger til lovforslag nr. L 164 A af 1. februar 1985, jf. Folketingstidende, 1984-85, Tillæg A, sp. 2971 f.

Retsplejelovens § 781, stk. 2 og 3, oplister herudover en række lovovertrædelser, der kan begrunde indgreb i meddelelseshemmeligheden, såfremt betingelserne i § 781, stk. 1, nr. 1 og 2, i øvrigt er opfyldt. Det drejer sig om følgende lovovertrædelser:

- Fredskrænkelser som omhandlet i straffelovens § 263, stk. 1. Denne bestemmelse vedrører den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem, jf. § 781, stk. 2.
- Krænkelser som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, jf. § 781, stk. 3, nr. 1. Denne bestemmelse

omfatter bl.a. krænkelser af en andens fred ved at forfølge eller genere den anden ved kontakt mv., hvilket omfatter at opsøge en anden ved personlig, mundtlig eller skriftlig henvendelse, herunder ved elektronisk kommunikation, eller på anden måde kontakte eller forfølge den anden, jf. § 1 i lov om tilhold, opholdsforbud og bortvisning.

- Overtrædelse af straffelovens § 279 a om databedrageri, eller § 293, stk. 1, om brugstyveri, begået ved anvendelse af en telekommunikationstjeneste, jf. § 781, stk. 3, nr. 2.
- Overtrædelse af artikel 14 eller 15 i Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014 om markedsmisbrug. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel og uretmæssig videregivelse af intern viden (artikel 14) samt forbud mod markedsmanipulation (artikel 15), jf. § 781, stk. 3, nr. 3.
- Overtrædelse af artikel 3, stk. 1, eller artikel 5 i Europa-Parlamentets og Rådets forordning (EU) nr. 1227/2011 af 25. oktober 2011 om integritet og gennemsigtighed på engrosenergimarkederne. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel (artikel 3, stk. 1) og forpligtelse til at offentliggøre intern viden (artikel 5), jf. § 781, stk. 3, nr. 4.
- Overtrædelse af artikel 38, stk. 1, artikel 39, artikel 40, jf. artikel 38, stk. 1, eller artikel 39, eller artikel 41 i Kommissionens forordning (EU) nr. 1031/2010 af 12. november 2010 om det tidsmæssige og administrative forløb af auktioner over kvoter for drivhusgasemissioner og andre aspekter i forbindelse med sådanne auktioner i medfør af Europa-Parlamentets og Rådets direktiv 2003/87/EF om en ordning for handel med kvoter for drivhusgasemissioner i Fællesskabet. Bestemmelserne vedrører henholdsvis forbud mod insiderhandel (artikel 38, stk. 1, og artikel 40) og andre anvendelser af intern viden, som er forbudt (artikel 39), jf. § 781, stk. 3, nr. 5.

Teleoplysning må ligesom andre indgreb i meddelelseshemmeligheden ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb, jf. retsplejelovens § 782, stk. 1, der udtrykker det almindelige proportionalitetsprincip, der finder anvendelse ved straffeprocessuelle tvangsindgreb.

Henvisningen til "sagens betydning" i retsplejelovens § 782, stk. 1, indebærer, at der skal tages konkret stilling til alvoren af det forhold, der er under

efterforskning, uanset at lovovertrædelsen i øvrigt er omfattet af kriminalitetskravet i § 781.

Et indgreb i meddelelseshemmeligheden sker efter rettens kendelse, jf. retsplejelovens § 783, stk. 1. I kendelsen fastsættes det tidsrum, inden for hvilket indgrebet kan foretages, jf. stk. 3. Tidsrummet skal være så kort som muligt og må ikke overstige 4 uger. Tidsrummet kan forlænges, men højest med 4 uger ad gangen. Såfremt indgrebets øjemed ville forspildes, dersom retskendelse skulle afventes, kan politiet træffe beslutning om at foretage indgrebet, jf. § 783, stk. 4. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten.

Inden retten foretager indgreb i meddelelseshemmeligheden, skal der beskikkes en advokat for den, som indgrebet vedrører, og advokaten skal have lejlighed til at udtale sig, jf. retsplejelovens § 784, stk. 1. Advokaten skal underrettes om alle retsmøder i sagen og er berettiget til at overvære disse samt til at gøre sig bekendt med det materiale, som politiet har tilvejebragt, jf. § 785, stk. 1.

Efter afslutningen af et indgreb i meddelelseshemmeligheden skal der gives underretning om indgrebet, jf. retsplejelovens § 788, stk. 1. Retten kan dog bestemme, at underretning skal undlades eller udsættes, hvis underretning vil være til skade for efterforskningen eller til skade for efterforskningen i en anden verserende sag om en lovovertrædelse, som efter loven kan danne grundlag for et indgreb i meddelelseshemmeligheden, eller hvis hensynet til beskyttelse af fortrolige oplysninger om politiets efterforskningsmetoder eller omstændighederne i øvrigt taler imod underretning, jf. § 788, stk. 4, 1. pkt.

Efter retsplejelovens § 786, stk. 1, påhviler det bl.a. udbydere af telenet eller teletjenester at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at give de i § 780, stk. 1, nr. 3, nævnte oplysninger. Reglerne i lovens § 178 om vidnetvang finder tilsvarende anvendelse. Dette indebærer eksempelvis, at udbyderen kan idømmes en bøde, hvis udbyderen uden lovlig grund undlader at yde denne bistand, jf. § 178, stk. 1, nr. 1.

7.1.2. Særligt om retsplejelovens regler om udvidet teleoplysning

Efter retsplejelovens § 780, stk. 1, nr. 4, kan politiet indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning). Reglerne om udvidet teleoplysning blev indført ved lov nr. 465 af 7. juni 2001 om ændring af straffeloven og retsplejeloven (Hæleri og anden efterfølgende medvirken samt IT-efterforskning). Loven bygger bl.a. på betænkning nr. 1377/1999 fra Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet ("Brydensholt-udvalget").

Bestemmelsen i retsplejelovens § 780, stk. 1, nr. 4, om udvidet teleoplysning blev ifølge bemærkningerne til lovforslaget indsat på baggrund af den i pkt. 7.1.1 omtalte kendelse fra Højesteret fra 1997, gengivet i Ugeskrift for Retsvæsen, 1997, s. 1021 f., der fastslog, at der ikke i § 780, stk. 1, nr. 3, om teleoplysning var fornøden hjemmel til at indhente oplysninger om hvilke mobiltelefoner, der i en nærmere angiven periode havde været sat i forbindelse med hinanden via sendemaster inden for en radius af 1 km fra en nærmere angiven adresse, jf. pkt. 4.4.1, 4.4.2 og 4.4.3.1 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5707 ff.

Det fremgår af forarbejderne, at reglerne ikke specifikt vedrører masteoplysninger, men at bestemmelsen er formuleret, så den tager højde for den teknologiske udvikling og vedrører teleoplysninger, der ikke kan specificeres på kendelsestidspunktet, jf. pkt. 4.4.3.1 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5708 f.

For at kunne foretage udvidet teleoplysning, skal henholdsvis indikationskravet og kriminalitetskravet i retsplejelovens § 781, stk. 1, nr. 2 og 3, være opfyldt. Disse betingelser er omtalt i pkt. 7.1.1 ovenfor. Mistankekravet i § 781, stk. 1, nr. 1, skal ikke være opfyldt, men udvidet teleoplysning kan kun foretages, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller betydelige samfundsværdier, jf. § 781, stk. 5.

Reglerne om proportionalitet, retskendelse, advokatbeskikkelse, og bistandspligt fra teleselskaberne, gælder også for indgreb i meddelelseshemmeligheden i form af udvidet teleoplysninger. Der henvises til pkt. 7.1.1 ovenfor.

Efter afslutning af et indgreb i meddelelseshemmeligheden i form af udvidet teleoplysning efter § 780, stk. 1, nr. 4, skal der ikke gives underretning til indehaverne af de pågældende telefoner, jf. § 788, stk. 5. Denne fravigelse af udgangspunktet om underretning begrundes i bestemmelsens forarbejder med, at det vil medføre betydelige praktiske vanskeligheder at foretage sådan underretning, jf. pkt. 4.4.3.4 i de almindelige bemærkninger til lovforslag nr. L 194 af 21. marts 2001, jf. Folketingstidende 2000-01, Tillæg A, s. 5709 f.

7.1.3. Retsplejelovens regler om adgang til historiske masteoplysninger

I EU-Domstolens dom af 6. oktober 2020 i La Quadrature du Net-sagen behandles bl.a. spørgsmålet om logning af og adgang til "lokaliseringsdata". Begrebet i dommen forstås i overensstemmelse med definitionen i artikel 2 i e-databeskyttelsesdirektivet, hvorefter "lokaliseringsdata" forstås som data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender.

I forbindelse med anvendelse af teledata i danske straffesager dækker denne definition over begrebet "historiske masteoplysninger". Når begrebet "lokaliseringsdata" i øvrigt anvendes i en dansk kontekst, dækker det imidlertid i almindelighed over det tidligere anvendte begreb "signaleringsdata", som ikke er eller har været logningspligtig, og dermed ikke omfattet af EU-Domstolens dom i La Quadrature du Net-sagen.

Hvis oplysningerne ikke angår, hvilken bestemt telefon eller andet kommunikationsapparat som en telefon eller andet kommunikationsapparat har været sat i forbindelse med, men angår eksempelvis, hvilken sendemast eller lignende telefonen eller kommunikationsapparatet har været sat i forbindelse med, foreligger der ikke et indgreb i meddelelseshemmeligheden. Hvis et teleselskab er i besiddelse af sådanne oplysninger (historiske oplysninger), eksempelvis som følge af reglerne om logning, jf. retsplejelovens § 786, stk. 4, kan disse oplysninger udleveres efter reglerne om edition. Denne

retsstilling blev lagt til grund ved Højesterets kendelse af 22. juli 2009, gengivet i Ugeskrift for Retsvæsen, 2009, s. 2620 ff.

Efter retsplejelovens § 804, stk. 1, kan der som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning meddeles en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande (edition), hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskereres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

Ligesom for indgreb i meddelelseshemmeligheden gælder det, at et pålæg om edition ikke må meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre, jf. retsplejelovens § 805, stk. 1. Ifølge bestemmelsens forarbejder lovfæster den det almindelige proportionalitetsprincip, der antages at gælde ved alle straffeprocessuelle tvangsindgreb, herunder bl.a. reglen i § 782, stk. 1, jf. ovenfor i pkt. 7.1.1. Der henvises til bemærkningerne til § 805 i lovforslag nr. L 41 af 8. oktober 1998, jf. Folketingstidende 1998-99, tillæg A, s. 876.

Betingelserne for at kunne anvende retsplejelovens regler om edition er lempeligere end kravene for at kunne foretage indgreb i meddelelseshemmeligheden. For at kunne foretage edition kræves således alene, at der skal være tale om en lovovertrædelse, som er undergivet offentlig påtale, jf. retsplejelovens § 804, stk. 1.

Afgørelse om pålæg om edition træffes af retten efter politiets begæring, jf. retsplejelovens § 806, stk. 1 og 2. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om beslaglæggelse og om edition, jf. § 806, stk. 4. Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest muligt og senest inden 24 timer forelægge sagen for retten, der ved kendelse afgør, om indgrebet kan godkendes, jf. stk. 4, 2. punktum. Retsplejelovens § 806, stk. 8 og 9, indeholder regler om kontradiktion, for så vidt angår den, pålægget om edition retter sig imod. Men der er ingen pligt til at underrette den, der måtte være genstand for oplysningerne, eksempelvis ejeren af telefonen. Efter § 804, stk. 1, 2. pkt., jf. § 189, stk. 1, kan der meddeles en erhvervsvirksomhed pålæg om tavshedspligt med hensyn til viden om sagen, når hensynet til

fremmede magter, til statens sikkerhed eller til opklaring af alvorlige forbrydelser taler derfor.

Ud over de forpligtelser til udlevering af oplysninger, der følger af retsplejelovens regler om edition, er udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere efter § 13 i lov om elektroniske kommunikationsnet og -tjenester forpligtede til på begæring af politiet at udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

7.2. Relevante dele af La Quadrature du Net-dommen og H.K.-dommen

EU-Domstolens præmisser vedrørende logning af trafik- og lokaliseringsdata er omtalt ovenfor i afsnit 2.

For så vidt angår spørgsmålet om adgangen til lagret data, omtaler EU-Domstolen dette spørgsmål i La Quadrature du Net-dommen, præmis 166-167, hvoraf følgende fremgår:

> ”166. Det skal desuden tilføjes, således som det navnlig fremgår af denne doms præmis 115 og 133, at adgangen til de trafikdata og lokaliseringsdata, som udbyderne lagrer som følge af en foranstaltning, der er vedtaget i henhold til artikel 15, stk. 1, i direktiv 2002/58, i princippet kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring. Det følger navnlig heraf, at der under ingen omstændigheder kan gives adgang til sådanne data med henblik på at retsforfølge og straffe en almindelig strafbar handling, når lagringen heraf er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed. I overensstemmelse med proportionalitetsprincippet, således som dette er blevet præciseret i denne doms præmis 131, kan en adgang til data, der er lagret med henblik på bekæmpelse af grov kriminalitet, under forudsætning af, at de i den foregående præmis nævnte materielle og proceduremæssige betingelser, der gælder for at opnå en sådan adgang, overholdes, til gengæld begrundes i formålet om beskyttelse af den nationale sikkerhed.
>
> 167. I denne henseende står det medlemsstaterne frit for i deres lovgivning at fastsætte, at der under overholdelse af disse samme materielle og proceduremæssige betingelser kan gives adgang til trafikdata og lokaliseringsdata med henblik på bekæmpelsen af grov kriminalitet eller beskyttelsen af den nationale sikkerhed, når de nævnte data af en udbyder lagres på en måde, der er i overensstemmelse med artikel 5, 6 og 9 eller artikel 15, stk. 1, i direktiv 2002/58.”

Efter EU-Domstolens opfattelse må der således i princippet kun gives adgang til lagrede trafik- og lokaliseringsdata med henblik på at efterforske og retsforfølge en strafbar overtrædelse, hvis den strafbare overtrædelse vedrører det hensyn, der er baggrunden for, at teleudbyderne mv. er pålagt at lagre de pågældende data, idet der dog kan gives adgang til lagrede trafik- og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed, selv om lagringsforpligtelsen er pålagt med henblik på at bekæmpe grov kriminalitet.

Som det fremgår af den citerede præmis 166, finder EU-Domstolen, at hensynet til at efterforske og retsforfølge almindelig kriminalitet ikke vil kunne begrunde, at politi og anklagemyndighed kan få adgang til lagrede trafik- og lokaliseringsdata. EU-Domstolen tager derimod ikke eksplicit stilling til, om hensynet til at efterforske og retsforfølge grov kriminalitet vil kunne begrunde, at politi og anklagemyndighed kan få adgang til lagrede trafik- og lokaliseringsdata, der er lagret med henblik på at beskytte den nationale sikkerhed.

Domstolen henviser dog i præmis 166 til præmis 131, som lyder:

> ”131. Det fremgår nærmere bestemt af Domstolens praksis, at medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der navnlig er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, skal vurderes ved at bedømme alvoren af det indgreb, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (jf. i denne retning dom af 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, præmis 55 og den deri nævnte retspraksis).”

Når EU-Domstolen henviser til præmis 55 i Ministerio Fiscal-dommens opstillede proportionalitetskrav, må dette kunne tages til indtægt for den opfattelse, at Domstolen herved – fortsat – har den opfattelse, at et alvorligt indgreb (dvs. teleudbyderes pligt til at lagre trafik- og lokaliseringsdata og offentlige myndigheders adgang hertil) i de grundlæggende rettigheder kan begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser, der har til formål at bekæmpe kriminalitet, der på samme måde kan kvalificeres som ”grov”, jf. Ministerio Fiscal-dommens præmis 56.

Det vurderes således – dog under en væsentlig procesrisiko i lyset af præmis 166 i logningsdommen – at dommen ikke er til hinder for, at medlemsstaterne kan give politi og anklagemyndighed adgang til lagrede trafik- og lokaliseringsdata, der er lagret med henblik på at beskytte den nationale sikkerhed, i de tilfælde, hvor politi og anklagemyndighed bekæmper grov kriminalitet. I tilknytning hertil skal det dog bemærkes, at det må antages, at den grove kriminalitet skal være af en sådan alvorlig karakter, at det vil være i overensstemmelse med det EU-retlige proportionalitetskrav at give politi og anklagemyndighed adgang til sådanne lagrede trafik- og lokaliseringsdata.

EU-Domstolens dom af 2. marts 2021 i H.K.-sagen har ikke endeligt afgjort det rejste spørgsmål. På den ene side indeholder dommens præmis 31 en gengivelse af dele af den førnævnte præmis 166 i La Quadrature du Net-dommen, idet der udtales følgende:

> ”31. Hvad angår de formål, der kan begrunde de offentlige myndigheders adgang til de data, som udbydere af elektroniske kommunikationstjenester lagrer som følge af en foranstaltning, der er i overensstemmelse med disse bestemmelser, fremgår det af Domstolens praksis, at en sådan adgang kun kan begrundes i det mål af almen interesse, med henblik på hvilket disse tjenesteudbydere er blevet pålagt at foretage denne lagring (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 166).”

På den anden side konstaterer EU-Domstolen følgende i præmis 33 i H.K.-sagen:

> ”33. Hvad angår det formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager, der forfølges med den i hovedsagen omhandlede lovgivning, er det i overensstemmelse med proportionalitetsprincippet kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, såsom de indgreb, som lagring af trafikdata og lokaliseringsdata indebærer, **uanset om der er tale om generel og udifferentieret lagring eller målrettet lagring.** Det er således kun de indgreb i de nævnte grundlæggende rettigheder, der ikke er alvorlige, som kan begrundes i det formål, der forfølges med den i hovedsagen omhandlede lovgivning, om at foretage forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed (jf. i denne retning dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 140 og 146).” (fremhævet her)

Derudover bemærkes det, at EU-Domstolen ikke forholder sig generelt til, hvad der kan kvalificeres som henholdsvis "almindelig kriminalitet", "grov kriminalitet" og "beskyttelsen af den nationale sikkerhed". Det fremgår imidlertid af præmis 166, at adgangen til loggede data "i princippet kun kan begrundes i det mål af almen interesse med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring". Justitsministeriet forstår dette således, at der skal foretages en vurdering af kriminalitetens grovhed i forhold til, hvad der har begrundet lagringen af oplysningerne.

I præmis 154 omtales i forbindelse med spørgsmålet om lagring af IP-adresser, at IP-adressen, hvor en lovovertrædelse er begået online, kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået. Det hedder videre, at dette bl.a. kan "være tilfældet for særligt alvorlige lovovertrædelser på området for børnepornografi, såsom erhvervelse, udbredelse, transmission eller tilrådighedsstillelse online af børnepornografi som omhandlet i artikel 2, litra c), i Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi (…)".

7.3. Justitsministeriets overvejelser

7.3.1. Generelle overvejelser i forhold til dommens rækkevidde i forhold til adgang til loggede oplysninger

Adgangen til loggede teledata er et helt centralt efterforskningsmiddel for politiet i forbindelse med efterforskningen af alvorlig kriminalitet, ligesom det kan være afgørende i forhold til anklagemyndighedens strafforfølgning af tiltalte ved domstolene. Det gælder for såvel trafikdata (teleoplysninger) som historiske masteoplysninger.

Teledata defineres efter Justitsministeriets opfattelse som oplysninger, som teleudbyderne indsamler, registrerer og opbevarer (logger) samt bearbejder dels i forretningsøjemed, bl.a. til brug for taksering af ydelser, fakturering af kunder og fejlretning på netværket, dels for at efterleve kravene i retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen.

Teledata indeholder oplysninger om kommunikation på telenetværket. F.eks. om hvilke telefoner der har været i kontakt med hinanden, og hvilke sendemaster de har været registreret på. Teledata indeholder, i modsætning til f.eks. telefonaflytning, ikke oplysninger om indholdet af kommunikationen.

Adgang til teledata vil typisk omfatte teleoplysning, herunder masteoplysninger, efter retsplejelovens § 780, stk. 1, nr. 3, jf. § 804, stk. 1, og udvidet teleoplysning (mastesug) efter reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens § 780, stk. 1, nr. 4, jf. § 804, stk. 1, mens udlevering af historiske masteoplysninger (som betegnes "lokaliseringsdata" i La Quadrature du Net-dommen) efter omstændighederne pålægges alene efter reglerne om edition i retsplejelovens § 804, stk. 1.

Politiet anvender loggede teledata på forskellige stadier af en efterforskning. I den indledende fase af en efterforskning kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikation og på den baggrund danne et overblik over personernes kommunikationsmønstre og færden. Herved er det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke personer fra efterforskningen, hvis de vurderes ikke at have relevans for sagen. Teledata kan være med til bl.a. at målrette politiets indsamling af andre beviser på et tidligt stadie af efterforskningen, herunder videoovervågning, f.eks. for hurtigt at finde og identificere en ellers ukendt gerningsmand. I tilfælde hvor den formodede gerningsmand er kendt af politiet, men forsvundet, kan teledata også bidrage til at opspore den mistænkte. En analyse af indhentede teledata kan også resultere i nye efterforskningsveje eller kaste lys over andre forhold, der gør det nødvendigt at indhente yderligere teledata. Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan teledata bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes teledata til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

Udvidet teleoplysning (mastesug) omfatter oplysninger om, hvilke telefoner der inden for et nærmere angivet område har været eller sættes i forbindelse med andre telefoner. Indhentelse af udvidede teleoplysninger (mastesug) anvendes til at identificere telefonnumre af interesse for politiets efterforskning, hvorefter efterforskningen kan målrettes indsamling af andre bevismidler, herunder historiske teleoplysninger. Et af områderne for anvendelse

af udvidede teleoplysninger er sager, hvor et antal ukendte personer, der mistænkes for at have begået en alvorlig forbrydelse, vurderes at have kommunikeret med hinanden umiddelbart før og efter den pågældende forbrydelse, muligvis via mobiltelefoner, og hvor den eneste efterforskningsmulighed er at få oplysninger fra den nærmeste sendemast i forhold til gerningsstedet og dermed se, hvilke telefoner der har kommunikeret via masten. Udvidede teleoplysninger kan have stor betydning i forbindelse med efterforskning af grov kriminalitet som f.eks. terror, drab, røveri mv. og i forbindelse med målrettede eftersøgninger i denne sammenhæng.

Pålæg om edition af historiske masteoplysninger, der viser, hvilke sendemaster telefonen har været registreret på i en given periode, og dermed kan vise et bevægelsesmønster for den pågældende telefon, kan derudover være et effektivt og afgørende efterforskningsskridt for politiet, ligesom det kan være afgørende i forhold til anklagemyndighedens strafforfølgning af tiltalte ved domstolene.

Det er derfor Justitsministeriets vurdering, at politiet og anklagemyndigheden i videst muligt omfang fortsat bør have adgang til loggede oplysninger inden for rammerne af EU-retten, herunder særligt La Quadrature du Net-dommen.

Justitsministeriet finder imidlertid i lyset af EU-Domstolens dom i La Quadrature du Net-sagen, navnlig præmis 166, som gennemgået ovenfor, at der er behov for at ændre reglerne om edition, sådan at det sikres, at der alene gives adgang til historiske masteoplysninger, når der er tale om efterforskning af grov kriminalitet. Justitsministeriet finder endvidere, at der er behov for at vurdere, om reglerne om adgang til loggede trafikdata ved indgreb i meddelelseshemmeligheden ligeledes bør ændres i lyset af EU-Domstolens dom, herunder om der i lyset af, at lagringen af data vil ske mere målrettet, er rum for at stille et lempeligere kriminalitetskrav for adgang til denne type oplysninger, end det nuværende.

Justitsministeriet overvejer konkrete modeller for, hvordan dette bedst sikres.

Det kan f.eks. være ved at sikre, at der gælder et tilstrækkeligt kriminalitetskrav for de pågældende indgreb, når de sker for at få udleveret loggede op-

lysninger. Et sådant kriminalitetskrav vil – som i dag for så vidt angår indgreb i meddelelseshemmeligheden – bl.a. kunne fastsættes i form af et krav til strafferammen for de lovovertrædelser, som efterforskes.

Domstolens præmisser giver imidlertid efter Justitsministeriets umiddelbare opfattelse ikke grundlag for at konkludere, at den for lovovertrædelsen foreskrevne strafferamme er det eneste kriterium, der vil kunne indgå ved vurderingen af, om en lovovertrædelse kan kvalificeres som henholdsvis "almindelig" eller "grov kriminalitet".

I denne vurdering må det efter Justitsministeriets opfattelse således også kunne indgå, om en alvorlig lovovertrædelse i praksis kun vanskeligt ville være mulig at efterforske, hvis ikke der var adgang til et bestemt tvangsindgreb, f.eks. indgreb i meddelelseshemmeligheden i form af teleoplysning, samt om lovovertrædelsen – uanset at den ikke måtte opfylde et strafferammekrav – kan karakteriseres som grov af andre årsager, f.eks. fordi der er tale om flere gentagelsestilfælde.

7.3.2. Retsplejelovens regler om adgang til loggede trafikdata

Justitsministeriet har overvejet, om La Quadrature du Net-dommen giver anledning til at ændre reglerne om indgreb i meddelelseshemmeligheden for så vidt angår adgang til teleoplysninger og udvidede teleoplysninger, som teleselskaberne pålægges at logge, i lyset af det strenge strafferammekrav, der allerede i dag som udgangspunkt gælder herfor. Justitsministeriet finder således, at et strafferammekrav på 6 års fængsel eller derover med sikkerhed må antages at opfylde betingelsen om, at indgrebet alene anvendes i relation til efterforskningen af grov kriminalitet.

Justitsministeriet finder derudover ikke, at nogen af de lovovertrædelser, der kan begrunde indgreb i meddelelseshemmeligheden efter kriminalitetskravet i § 781, på forhånd kan kvalificeres således, at de ikke vedrører grov kriminalitet. Dette vil dog skulle undersøges nærmere.

Det bemærkes i den forbindelse, at anvendelse af retsplejelovens regler om teleoplysning og udvidet teleoplysning, ligesom lovens regler om indgreb i meddelelseshemmeligheden i øvrigt, som udgangspunkt er betinget af forudgående retskendelse, hvor domstolene vurderer, om betingelserne for at foretage indgrebet er opfyldt. Som led i denne afgørelse vil domstolene vurdere, om indgrebet er proportionalt i forhold til den sag, der efterforskes, jf.

retsplejelovens § 782, stk. 1. Efter denne bestemmelse må et indgreb i meddelelseshemmeligheden ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være uforholdsmæssigt. Som beskrevet ovenfor i pkt. 7.1.1 indgår lovovertrædelsens grovhed i denne vurdering. Domstolene vil således også i dag skulle foretage en vurdering af betydningen af den sag, der forfølges, over for de oplysninger, der ønskes udleveret.

Politiet og anklagemyndigheden bør som anført sikres de bedst mulige rammer for at efterforske og retsforfølge grov kriminalitet. I forbindelse med ændringen af reglerne om teleudbydernes pligt til at logge data, vil der ske en indskrænkning i den data, som politi og anklagemyndighed vil have adgang til.

Justitsministeriet finder i den forbindelse, at det bør undersøges, om der – i lyset af at lagringen af data vil ske mere målrettet – er rum for at stille et lempeligere kriminalitetskrav end det nuværende.

7.3.3. Retsplejelovens regler om myndighedernes adgang til historiske masteoplysninger

Retsplejelovens regler om edition, jf. lovens § 804, giver politiet adgang til historiske masteoplysninger (betegnet ”lokaliseringsdata” i dommen).

For så vidt angår editionspålæg, der kan give adgang til historiske masteoplysninger som omhandlet i dommen, gælder det ligesom for indgreb i meddelelseshemmeligheden, at det ikke på baggrund af dommen kan siges generelt hvilke former for lovovertrædelser, der kan kvalificeres som henholdsvis ”almindelig kriminalitet”, ”grov kriminalitet” eller hvilke formål, der tjener til ”beskyttelse af den nationale sikkerhed”.

Retsplejelovens regler om edition omfatter på grund af det lempelige kriminalitetskrav (undergivet offentlig påtale eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning) en bred kategori af lovovertrædelser af meget forskellig karakter. Loggede data, f.eks. i form af historiske masteoplysninger, kan således pålægges udleveret som led i efterforskningen af en række lovovertrædelser, som det på forhånd kan være vanskeligt at kvalificere som ”grov kriminalitet”. Justitsministeriet vurderer på den baggrund, at der er et behov for at ændre reglerne om edition, sådan

at adgangen til historiske masteoplysninger, som teleudbyderne har været pålagt at logge, begrænses til at gælde i sager om grov kriminalitet. Dette kan bl.a. ske ved en ændring eller præcisering af kriminalitetskravet, idet et sådant krav dog ikke nødvendigvis vil kunne være eneste parameter for vurderingen af kriminalitetens grovhed, jf. ovenfor under pkt. 7.3.1. Dette vil blive undersøgt nærmere.

Justitsministeriet vil dog også i den forbindelse understrege, at der allerede i dag gælder et almindeligt proportionalitetsprincip, jf. retsplejelovens § 805, stk. 1. Domstolene vil derfor, før der meddeles pålæg om edition, skulle vurdere sagens betydning i forhold til det tab eller den ulempe, som indgrebet kan antages at medføre.

7.4. Forholdet til databeskyttelseslovgivningen

Databeskyttelsesforordningen og databeskyttelsesloven finder anvendelse for al behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Databeskyttelsesforordningen og databeskyttelsesloven finder dog ikke anvendelse i de tilfælde, der er nævnt i forordningens artikel 2, stk. 2, litra b-d, og lovens § 3. Forordningen og loven finder efter forordningens artikel 2, stk. 2, litra d, ikke anvendelse for retshåndhævende myndigheders behandling af personoplysninger til retshåndhævelsesformål, der i stedet er reguleret af bestemmelserne i retshåndhævelsesloven, som gennemfører det såkaldte retshåndhævelsesdirektiv. Endvidere finder databeskyttelsesforordningen og databeskyttelsesloven ikke anvendelse for behandling af personoplysninger, som udføres for eller af Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste, jf. databeskyttelseslovens § 3, stk. 2.

For behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet, finder reglerne i e-databeskyttelsesdirektivet anvendelse, jf. direktivets artikel 3, stk. 1. Efter direktivets artikel 1, stk. 2, specificerer og supplerer det databeskyttelsesforordningens bestemmelser på dette område. Det indebærer, at de danske regler om beskyttelse af personoplysninger, der gennemfører e-databeskyttelsesdirektivets bestemmelser, har forrang for reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Da spørgsmålet om, hvorvidt teleselskaberne må videregive trafik- og lokaliseringsdata til politiet, ikke er reguleret af e-databeskyttelsesdirektivet bestemmelser, skal regler herom fastsættes inden for rammerne af databeskyttelsesforordningen, herunder forordningens grundlæggende principper for behandling af personoplysninger og regler om, hvornår personoplysninger lovligt kan behandles.

De grundlæggende behandlingsprincipper følger af forordningens artikel 5, hvorefter personoplysninger bl.a. skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede. Endvidere skal personoplysninger indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. I forhold til dette princip om formålsbestemthed bemærkes det, at det efter forordningens artikel 6, stk. 4, og præambelbetragtning nr. 50 kan fastsættes i national ret, at der – uanset foreneligheden mellem formålene – kan ske behandling af oplysninger til et andet formål end det, de er indsamlet til. Det er en betingelse for fastsættelse af sådanne bestemmelser i national ret, at der er tale om en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er fastsat i forordningens artikel 23, stk. 1, herunder forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger.

Reglerne om, hvornår behandling af personoplysninger lovligt kan finde sted, følger af databeskyttelsesforordningens artikel 6, stk. 1, hvorefter behandling, herunder videregivelse, af ikke-følsomme personoplysninger som f.eks. trafik- og lokaliseringsdata lovligt kan finde sted, hvis det bl.a. er nødvendigt af hensyn til at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

For så vidt angår de nævnte scenarier under pkt. 7.2 ovenfor vil der efter Justitsministeriets vurdering inden for rammerne af databeskyttelsesforordningen, herunder forordningens artikel 5 og 6, stk. 1, litra c, og stk. 4, kunne fastsættes regler om politiets adgang til loggede oplysninger.

Politiets indhentning af sådanne oplysninger vil endvidere kunne ske inden for rammerne af retshåndhævelsesloven, hvorefter sådanne oplysninger kan behandles, når det bl.a. er nødvendigt for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger.

8. Perioden indtil et nyt regelsæt træder i kraft

Justitsministeriet har overvejet, om EU-Domstolens dom har betydning for, hvordan gældende regler kan administreres, indtil nye regler om revision af logningsreglerne mv. måtte træde i kraft.

Det bemærkes i den forbindelse, at forpligtelsen til at ændre national ret for at bringe den i overensstemmelse med EU-retten, som fortolket af EU-Domstolen i dommen, gælder så hurtigt som muligt. Der gælder derfor ikke en umiddelbar pligt til at ophæve eller suspendere de danske logningsregler. Tilsvarende gælder for så vidt angår reglerne om myndighedernes adgang til lagrede teledata.

Det bemærkes endvidere, at La Quadrature du Net-dommen giver mulighed for, at en medlemsstat kan fastsætte en generel og udifferentieret logningsforpligtelse med henblik på beskyttelse af den nationale sikkerhed, såfremt medlemsstaten står over for en sådan alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig. Som nævnt under afsnit 3.3.1, fremgår det af den seneste Vurdering af Terrortruslen mod Danmark, at CTA vurderer, at terrortruslen mod Danmark er alvorlig, altså det næsthøjeste niveau af fem niveauer. Det betyder i henhold til CTA's definitioner, at der er en erkendt trussel, og at der er kapacitet, hensigt og planlægning.

Det er i den forbindelse Justitsministeriets umiddelbare opfattelse, at Danmark på nuværende tidspunkt står over for en sådan alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, at en generel og udifferentieret logning vil kunne fastsættes i overensstemmelse med La Quadrature du Net-dommen.

For så vidt angår spørgsmålet om adgang til lagrede teledata, der er opnået ved hjælp af en generel og uddifferentieret logning, som måtte være uforenelig med EU-retten, har EU-Domstolen forholdt sig til dette i La Quadrature du Net-dommens præmis 228, hvoraf følgende fremgår:

> "228. […] artikel 15, stk. 1, som fortolket i lyset af effektivitetsprincippet, pålægger den nationale ret i straffesager at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt

> mod personer, som er mistænkt for at have begået kriminelle handlinger, hvis disse personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder."

Det bemærkes i den forbindelse, at loggede oplysninger altid vil indgå som ét blandt flere beviser i en sag, og at betydningen af et bevis i form af teledata altid vil bero på en konkret vurdering af dels det enkelte bevis, dels sagens samlede omstændigheder i øvrigt. Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt et bevis i form af teledata skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse. Herudover vil der i overensstemmelse med det såkaldte "ligestillingsprincip" være adgang til kontradiktion samt fuld transparens i processen.

Det bemærkes derudover, at idet oplysningerne i overensstemmelse med EU-retten vil kunne være indhentet med henblik på beskyttelse mod en alvorlig trussel mod national sikkerhed, kan det ikke antages, at oplysningernes værdi kan betvivles, fordi de er indhentet på baggrund af en logningsforpligtelse, der ikke fuldt ud vil kunne opretholdes efter EU-retten. Endvidere må det antages, at lovligheden af logningsforpligtelsen ikke har haft betydning for bevisets værdi, uanset at oplysningerne ikke ville være indhentet, hvis der ikke var en sådan pligt til logning.

Samlet set er det således Justitsministeriet vurdering, at der ikke forud for indførelsen af ny lovgivning – som forventes at kunne træde i kraft 1. januar 2022 – er behov for en suspension af anvendelsen af loggede oplysninger, der er opnået ved en generel og udifferentieret lagring af trafik- og lokaliseringsdata. Efter Justitsministeriets vurdering kan loggede oplysninger således fortsat indhentes og anvendes efter de gældende regler i retsplejelovens kapitel 71 (indgreb i meddelelseshemmeligheden) og kapitel 74 (edition) til brug for efterforskningen, ligesom disse oplysninger også fortsat kan anvendes som bevis i straffesager. Det er endvidere Justitsministeriets vurdering, at databeskyttelsesforordningen ikke er til hinder for teleselskabernes fortsatte behandling af loggede teleoplysninger i overensstemmelse med logningsbekendtgørelsens bestemmelser.

9. Sammenfatning

Loggede oplysninger er centrale for politiets og efterretningstjenesternes arbejde, og dermed beskyttelsen af danske borgere mod trusler mod navnlig den nationale sikkerhed og grov kriminalitet.

Det er derfor afgørende for regeringen, at nationale myndigheders muligheder for logning sikres i videst muligt omfang inden for EU-rettens grænser.

På den baggrund foreslås en ordning, hvorefter justitsministeren, såfremt der foreligger en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, kan fastsætte en generel og udifferentieret forpligtelse for teleudbydere mv. til at foretage logning af teleoplysninger mv. for en afgrænset periode på op til 1 år. Det forventes, at Vurderingen af Terrortruslen mod Danmark kan indgå som et hovedmoment i en samlet vurdering, hvor også andre trusselsvurderinger kan indgå. Hvorvidt der foreligger en situation, som kan begrunde en sådan logningsforpligtelse, vil kunne prøves efterfølgende ved domstolene.

Der foreslås endvidere en ordning, hvorefter teleudbydere mv. kan pålægges personbestemt og geografisk målrettet logning for en afgrænset periode på op til 1 år af hensyn til bekæmpelse af grov kriminalitet mv. Det vil nærmere skulle vurderes, hvad der kan udgøre et tilstrækkeligt kriminalitetskrav for "grov kriminalitet".

For den personbestemte logning vil et pålæg kunne omfatte følgende kategorier af personer:

- Personer der inden for en nærmere bestemt årrække er dømt for grov kriminalitet mv.
- Personer der tidligere har været genstand for indgreb efter retsplejelovens kapitel 71 med henblik på bekæmpelse af grov kriminalitet mv.
- Personer der tidligere har været i kontakt med personer, som har været aflyttet med henblik på bekæmpelse af grov kriminalitet mv.
- Personer som retshåndhævende myndigheder har en konkret formodning om har forbindelse til grov kriminalitet mv.

For den geografisk målrettede logning vil et pålæg kunne fastsættes på baggrund af myndighedernes vurdering af – på grundlag af objektive og ikke-

diskriminerende forhold – en forhøjet risiko for, at der planlægges eller begås alvorlig kriminalitet i et givent område, herunder på følgende steder:

- Steder der er kendetegnet ved et højt antal tilfælde af grov kriminalitet.
- Steder der i særlig grad kan begås grov kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer.
- Strategiske steder, såsom lufthavne, banegårde eller vejafgiftsområder.

Endvidere foreslås en ordning, hvorefter der kan fastsættes en generel og udifferentieret forpligtelse til logning af IP-adresser for brugeres adgang til internettet for en periode på 1 år.

Den målrettede logning og logning af IP-adresser vil være begrænset til det strengt nødvendige samt ledsaget af processuelle garantier. Logningen forslås i overensstemmelse med La Quadrature du Net-dommen begrænset til bekæmpelse af grov kriminalitet, forebyggelse af alvorlige trusler mod den offentlige sikkerhed, samt beskyttelse af den nationale sikkerhed. Det vil nærmere skulle vurderes, hvad der kan udgøre et tilstrækkeligt kriminalitetskrav for "grov kriminalitet".

Justitsministeriet finder endvidere, at der er behov for at ændre reglerne om edition, sådan at det sikres, at der alene gives adgang til historiske masteoplysninger ("lokaliseringsdata" i La Quadrature du Net-dommen), når der er tale om efterforskning af grov kriminalitet. Det vil ligeledes blive vurderet, om reglerne om adgang til loggede trafikdata ved indgreb i meddelelseshemmeligheden bør ændres i lyset af EU-Domstolens dom, herunder om der i lyset af, at lagringen af data vil ske mere målrettet, er rum for at stille et lempeligere kriminalitetskrav, for adgang til denne type oplysninger, end det nuværende.

For at sikre en effektiv og egnet ordning for den foreslåede logningsforpligtelse, har Justitsministeriet fundet det nødvendigt at tage adgangen til at anvende uregistrerede taletidskort op til revision. Det forslås således, at der stilles krav om, at der fremadrettet ved salget af taletidskort er en forpligtelse til at registrere oplysninger om køberens civile identitet. Dette vil minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort

udgør i dag. Endelig forslås justering af ordningen om hastesikring med henblik på bekæmpelse af grov kriminalitet og beskyttelse af den nationale sikkerhed.

De ovenstående overvejelser udgør de overordnede principper for, hvordan logning fremadrettet kan finde sted i Danmark. En lang række forhold vil skulle fastlægges nærmere i forbindelse med udformningen af det lovforslag, som regeringen forventer at fremsætte til efteråret 2021. Lovskitsen skal danne grundlag for drøftelser med branchen, interessenter mv., inden lovforslaget fremsættes.