



JUSTITSMINISTERIET

Dato: 27. september 2021
Kontor: Sikkerhedskontor II
Sagsnr.: 2020-187-0036
Dok.: 1933567

UDKAST

Forslag til

lov om ændring af retsplejeloven og lov om elektroniske kommunika- tionsnet og -tjenester

(Revision af reglerne om registrering og opbevaring af oplysninger om te-
letrafik (logning) m.v.)

§ 1

I retsplejeloven, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, som senest ændret ved § 3 i lov nr. 1174 af 8. juni 2021, foretages følgende ændringer:

1. I § 781, stk. 1, nr. 3, indsættes efter »udlændingelovens § 59, stk. 8, nr. 1-5«: », jf. dog § 781 a«.

2. Efter § 781 indsættes:

»§ 781 a. Politiet kan, uanset § 781, stk. 1, nr. 3, tillige foretage teleoplysning, jf. § 780, stk. 1, nr. 3, og udvidet teleoplysning, jf. § 780, stk. 1, nr. 4, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

medfør af disse bestemmelser, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.«

3. § 786, stk. 4 og 6, ophæves.

Stk. 5 bliver herefter stk. 4 og stk. 7 og 8 bliver herefter stk. 5 og 6.

4. I § 786, stk. 7, der bliver stk. 5, slettes »stk. 4, 2. pkt., og«.

5. I § 786 a, stk. 1, ændres »trafikdata« til: » trafik- og lokaliseringsdata«

6. § 786 a, stk. 2, 4. pkt., affattes således: »Et pålæg kan dog efterfølgende opretholdes, men højst med 90 dage ad gangen.«

7. I § 786 a indsættes efter stk. 2 som nyt stykke:

»Stk. 3. Hastesikring af trafik- og lokaliseringsdata må kun foretages, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.«

Stk. 3 og 4 bliver herefter stk. 4 og 5.

8. I § 786 a, stk. 4, der bliver stk. 5, ændres »stk. 1 og 3« til »stk. 1 og 4«.

9. Efter § 786 a indsættes:

»§ 786 b. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata efter stk. 2-5.

Stk. 2. Trafikdata omfattet af forpligtelsen i stk. 1 registreres i

- 1) 3 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr.

- 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a,
- 2) 5 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover,
- 3) 10 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 8 år eller derover.

Stk. 3. Er den pågældende person idømt en ubetinget frihedsstraf, regnes registreringsperioden, jf. stk. 2, nr. 1-3, fra tidspunktet for endelig løsladelse fra afsoning. Prøveløslades den pågældende person, regnes perioden fra tidspunktet for prøveløsladelse. Er den pågældende person idømt en betinget frihedsstraf, regnes perioden fra endelig dom. Er den pågældende person idømt anden strafferetlig retsfølge efter straffelovens §§ 68-70, regnes perioden fra endelig ophævelse af denne retsfølge, dog regnes perioden fra endelig dom, hvis den pågældende person er dømt til ambulant behandling, der ikke medfører eller kan medføre indlæggelse i institution.

Stk. 4. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata fra

- 1) kommunikationsapparater, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1 eller 3.
- 2) personer, der, jf. § 783, stk. 2, har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1 eller 3,
- 3) personer, der er indehavere af et kommunikationsapparat, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1, eller 3, og
- 4) kommunikationsapparater, der har været genstand for indgreb i medfør af § 786, stk. 2.

Stk. 5. Trafikdata registreret i medfør af stk. 4 skal registreres i 1 år fra det tidspunkt, hvor indgrebet afsluttes.

Stk. 6. Trafikdata registreret efter stk. 2-5 skal opbevares i 1 år.

§ 786 c. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på områder på 3 km gange 3 km, hvor

- 1) antallet af anmeldelser af lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af

straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, eller

- 2) antallet af beboere dømt for lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Stk. 2. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.

Stk. 3. Trafikdata registreret efter stk. 1 og 2 skal opbevares i 1 år.

Stk. 4. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om målrettet geografisk registrering og opbevaring af trafikdata som nævnt i stk. 1.

§ 786 d. Der kan meddeles udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, pålæg om at foretage målrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, hvis der er grund til at antage, at de har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller lovovertrædelser, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Stk. 2. Afgørelse om pålæg om registrering og opbevaring efter stk. 1 træffes af retten ved kendelse. I kendelsen fastsættes det tidsrum, inden for hvilket indgrebet kan foretages. Dette tidsrum skal være så kort som muligt og må ikke overstige 6 måneder. Tidsrummet kan forlænges, men højst med 6 måneder ad gangen. Forlængelsen sker ved kendelse. I kendelsen angives den person, det kommunikationsapparat eller det område, som indgrebet angår. Reglerne i § 783, stk. 2, 2., 3. og 5.-7. pkt., finder tilsvarende anvendelse ved pålæg om registrering og opbevaring af trafikdata for personer. Underretningen efter 7. pkt., jf. § 783, stk. 2, 2. og 3. pkt., skal indeholde en angivelse af de grunde, der er til at antage, at den person, som indgrebet angår, benytter sig af de pågældende numre.

Stk. 3. Trafikdata registreret i medfør af pålæg meddelt efter stk. 1 skal opbevares i 1 år.

Stk. 4. Reglerne i § 782, stk. 1, § 783, stk. 1, 3 og 4. pkt., samt stk. 4, og §§ 784 og 785 finder tilsvarende anvendelse for pålæg omfattet af stk. 1.

§ 786 e. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

Stk. 2. Regler om registreringspligt fastsat i medfør af stk. 1 kan fastsættes for en periode på højst 1 år ad gangen.

§ 786 f. Det påhviler udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet.

Stk. 2. Oplysninger registreret efter stk. 1 skal opbevares i 1 år.

Stk. 3. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om registrering og opbevaring som nævnt i stk. 1.

§ 786 g. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af §§ 786 a-786 f eller pålæg eller regler udstedt i medfør heraf.

§ 786 h. Justitsministeren kan efter forhandling med og klima-, energi- og forsyningsministeren fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters registrering og verificering af nummeroplysningsdata.

§ 786 i. Overtrædelse af § 786 b, stk. 1, 2 og 4-6, § 786 c, stk. 1-3, og § 786 f, stk. 1 og 2, samt af pålæg udstedt i medfør af § 786 d, stk. 1 og 3, straffes med bøde.

Stk. 2. For overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af § 786 c, stk. 4, § 786 e, § 786 f, stk. 3, § 786 g og § 786 h, kan der fastsættes bestemmelser om bødestraf.«

10. I § 804, *stk. 1, 1. pkt.*, indsættes efter »som kan kræve den tilbage«: », jf. dog § 804 a«.

11. Efter § 804 indsættes:

»**§ 804 a.** Pålæg om edition, jf. § 804, af oplysninger, der er registreringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, kan kun meddeles, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelser eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

§ 804 b. Uanset §§ 804 og 804 a skal udbydere af elektroniske kommunikationsnet eller -tjenester på politiets begæring som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller en krænkelser som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

Stk. 2. Oplysninger, som opbevares som følge af §§ 786 a-786 f, er ikke omfattet af stk. 1.

Stk. 3. Overtrædelse af stk. 1 straffes med bøde.

12. I § 806 indsættes efter stk. 9 som nyt stykke:

»*Stk. 10.* Ved pålæg om edition, jf. § 804 a, finder §§ 784-785 og § 788 tilsvarende anvendelse i forhold til den, som oplysningerne angår.«

Stk. 10 bliver herefter stk. 11.«

13. I § 807 a, 3. pkt., ændres »§ 806, stk. 10« til: »§ 806, stk. 11«

§ 2

I lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014, som senest ændret ved § 4 i lov nr. 1176 af 8. juni 2021, foretages følgende ændringer:

1. § 13 ophæves.

2. I § 31, stk. 2, indsættes efter »indeholdende«: »unikt ID«, og efter »eventuelle oplysninger om stilling«: »eventuelle oplysninger om bruger«.

§ 3

Stk. 1. Loven træder i kraft den 1. januar 2022, jf. dog stk. 2.

Stk. 2. Justitsministeren kan efter forhandling med erhvervsministeren i en overgangsperiode fastsætte nærmere regler om registrering og opbevaring af trafikdata for så vidt angår retsplejelovens § 786 b, § 786 c, stk. 1, nr. 2, og § 786 d, stk. 1, som affattet ved denne lovs § 1, nr. 9.

Stk. 3. For oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, finder kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition som affattet ved denne lovs § 1, nr. 9, anvendelse.

Stk. 4. Oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, skal opbevares i 1 år fra registreringstidspunktet.

Stk. 5. Regler fastsat i medfør af retsplejelovens § 786, stk. 5, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 4.

Stk. 6. Regler fastsat i medfør af retsplejelovens § 786, stk. 7, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 5.

Stk. 7. Regler fastsat i medfør af retsplejelovens § 786, stk. 8, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 6.

Stk. 8. Retsplejelovens § 786 b, stk. 2 og 4, som affattet ved denne lovs § 1, nr. 9, finder kun anvendelse for domme afsagt og indgreb iværksat efter lovens ikrafttræden.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning	11
2. Lovforslagets baggrund og formål.....	18
2.1. EU-Domstolens praksis før La Quadrature du Net-dommen..	18
2.2. La Quadrature du Net-dommen	20
2.3. EU-Domstolens praksis efter La Quadrature du Net-dommen	23
3. Hovedpunkterne i lovforslaget.....	23
3.1. Målrettet registrering og opbevaring af trafikdata	23
3.1.1. Gældende ret	23
3.1.2. EU-Domstolens praksis.....	31
3.1.3. Justitsministeriets overvejelser og den foreslåede ordning	32
3.2. Generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed	54
3.2.1. Gældende ret	54
3.2.2. EU-Domstolens praksis.....	54
3.2.3. Justitsministeriets overvejelser og den foreslåede ordning	55
3.3. Registrering og opbevaring af oplysninger om en brugers adgang til internettet	60
3.3.1 Gældende ret	60
3.3.2. EU-Domstolens praksis.....	62
3.3.3. Justitsministeriets overvejelser og den foreslåede ordning	63
3.4. Registrering og verificering af nummeroplysningsdata	69
3.4.1 Gældende ret	69
3.4.2. Justitsministeriets overvejelser og den foreslåede ordning	70
3.5. Hastesikring	73
3.5.1. Gældende ret	73
3.5.2. EU-Domstolens praksis.....	75

3.5.3. Justitsministeriets overvejelser og den foreslåede ordning	76
3.6. Domstolsprøvelse	80
3.6.1. Gældende ret	80
3.6.2. EU-Domstolens praksis	80
3.6.3. Justitsministeriets overvejelser og den foreslåede ordning	81
3.7. Adgang til registrerede og opbevarede data	90
3.7.1. Gældende ret	90
3.7.2. EU-Domstolens praksis	104
3.7.3. Justitsministeriets overvejelser	108
3.7.4. Den foreslåede ordning	121
3.8. Ændring af telelovens § 31, stk. 2, om nummeroplysningsdata	126
3.8.1. Gældende ret	126
3.8.2. Justitsministeriets overvejelser og den foreslåede ordning ...	127
3.9. Opbevaring af registrerings- og opbevaringspligtige oplysninger	128
3.9.1. Gældende ret	128
3.9.2. EU-Domstolens praksis	129
3.9.3. Justitsministeriets overvejelser og den foreslåede ordning ...	130
3.10. Forholdet til tavshedspligt	131
3.10.1. Gældende ret	131
3.10.2. EU-Domstolens praksis	132
3.10.3. Justitsministeriets overvejelser	136
4. Konsekvenser for opfyldelsen af FN's verdensmål	136
5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige	137
6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.	137
7. Administrative konsekvenser for borgerne	138
8. Klimamæssige konsekvenser	139
9. Miljø- og naturmæssige konsekvenser	139
10. Forholdet til EU-retten	139

11. Hørte myndigheder og organisationer m.v.	145
12. Sammenfattende skema	146

1. Indledning

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. (La Quadrature du Net-dommen). Dommen medfører, at der er behov for at ændre i de gældende danske regler om registrering og opbevaring af teletrafik, herunder reglerne om adgang til registrerede og opbevarede oplysninger.

Det følger af retsplejelovens § 786, stk. 4, at det påhviler 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. Reglerne om adgang til registrerede og opbevarede oplysninger findes navnlig i retsplejelovens bestemmelser om edition og indgreb i meddelelseshemmeligheden.

Indhentelse af registrerede og opbevarede oplysninger om teletrafik er et centralt efterforskningsværktøj for politiet i forbindelse med efterforskningen af kriminalitet, ligesom det kan være afgørende for anklagemyndighedens muligheder for strafforfølgning ved domstolene. Det gælder bl.a. i sager om bandekriminalitet, drab, narkotikakriminalitet og terrorisme.

Politiet anvender oplysninger fra udbyderne af elektroniske kommunikationsnet eller -tjenester på forskellige stadier af efterforskningen. I den indledende fase kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikationsmønstre og færden. Det gør det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke personer fra efterforskningen, der ikke har relevans for sagen.

Oplysninger registreret og opbevaret af udbyderne af elektroniske kommunikationsnet eller -tjenester kan navnlig være med til at målrette politiets indsamling af andre beviser på et tidligt stadie af efterforskningen, 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 trafikdata også bidrage til at opspore den mistænkte. En analyse af indhentede oplysninger fra udbyderne af elektroniske kommunikationsnet eller -tjenester kan også resultere i nye spor i efterforskningen eller kaste lys over andre

forhold, der gør det nødvendigt at indhente yderligere oplysninger fra udbyderne af elektroniske kommunikationsnet eller -tjenester. Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan oplysninger registreret og opbevaret af udbyderne af elektroniske kommunikationsnet eller -tjenester bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes oplysninger fra udbyderne af elektroniske kommunikationsnet eller -tjenester til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

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

Regeringen foreslår på den baggrund en revision af reglerne om registrering og opbevaring af trafikdata, der i videst muligt omfang skal medvirke til at sikre, at trafikdata fortsat kan anvendes til effektiv kriminalitetsbekæmpelse. Den foreslåede revision vil alt andet lige medføre, at politiet ikke får adgang til den samme mængde data som i dag. Revisionen bidrager i imidlertid til at sikre en så effektiv kriminalitetsbekæmpelse på baggrund af registrerede og opbevarede oplysninger som muligt inden for rammerne af EU-retten.

Det foreslås, at registrering og opbevaring fremover vil kunne iværksættes for de data, der er registrerings- og opbevaringspligtige i dag. Det vil sige de data, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som ”teletrafik”. For at modernisere sprogbrugen foreslås det dog, at denne form for data fremover kaldes trafikdata.

Visse lokaliseringsdata, som udgør trafikdata i forbindelse med telefoni og sms/mms-kommunikation, er også i dag registrerings- og opbevaringspligtige, idet de anses for omfattet af forpligtelsen i retsplejelovens § 786, stk. 4, eller regler fastsat i medfør heraf. Det gælder oplysninger om den eller de celler, en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen. Disse data vil efter lovforslaget også fremadrettet være registrerings- og opbevaringspligtige og betegnes i det følgende også som trafikdata.

Ved trafikdata forstås således nærmere:

- 1) opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 2) opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 3) ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 4) kvittering for modtagelse af meddelelser,
- 5) identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre),
- 6) den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,
- 7) tidspunktet for kommunikationens start og afslutning,
- 8) oplysninger om afsendende e-mailadresse og
- 9) oplysninger om modtagende e-mailadresse.

For nærmere om omfanget af de registrerings- og opbevaringspligtige oplysninger henvises til pkt. 3.1.3.4.

Det foreslås, at der fremover vil skulle gælde en todelt ordning for registrering og opbevaring af trafikdata.

For det første foreslås en ordning med målrettet personbestemt og geografisk registrering og opbevaring af trafikdata (målrettet registrering og opbevaring).

For så vidt angår den målrettede personbestemte registrering og opbevaring foreslås det, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, forpligtes til at foretage registrering og opbevaring af trafikdata vedrørende personer dømt for grov kriminalitet. Efter forslaget vil pligten til registrering gælde i 3, 5 eller 10 år afhængigt af strafferammen for den begåede kriminalitet. Oplysningerne vil skulle opbevares i 1 år.

Det foreslås desuden, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, forpligtes til at foretage per-

sonbestemt målrettet registrering og opbevaring af trafikdata fra kommunikationsapparater eller personer, der har været genstand for visse indgreb i meddelelseshemmeligheden (teleoplysning og telefonaflytning). Det foreslås, at pligten til registrering skal gælde i 1 år fra indgrebets afslutning, samt at oplysningerne skal opbevares i 1 år.

For så vidt angår den målrettede geografiske registrering og opbevaring foreslås det, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, forpligtes til at foretage målrettet geografisk registrering og opbevaring af trafikdata på områder på 3 km gange 3 km, hvor

- 1) antallet af anmeldelser af grov kriminalitet begået i området udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, eller
- 2) antallet af beboere dømt for grov kriminalitet udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Det foreslås endvidere, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage målrettet geografisk registrering og opbevaring af trafikdata vedrørende særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.

Det foreslås, at politiet årligt udarbejder en oversigt over, hvilke områder der skal etableres målrettet geografisk registrering og opbevaring af trafikdata vedrørende, som kan videregives til de relevante udbydere. Oplysninger registreret og opbevaret som følge af en pligt til målrettet geografisk registrering og opbevaring vil efter forslaget skulle opbevares i 1 år.

Endelig foreslås det, at der vil kunne meddeles udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden,

konkret begrundede pålæg om at foretage målrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, hvis der er grund til at antage, at de har forbindelse til grov kriminalitet.

Et sådant pålæg vil kræve indhentelse af retskendelse. I forbindelse med indhentelsen af kendelsen vil der skulle tages stilling til tidsrummet for registreringen. Tidsrummet skal være så kort som muligt og må maksimalt fastsættes til 6 måneder ad gangen.

Oplysninger registreret og opbevaret på baggrund af konkret begrundede pålæg vil efter forslaget skulle opbevares i 1 år.

Målrettet registrering og opbevaring af trafikdata vil være udgangspunktet, når der ikke foreligger en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig (se nedenfor). Det bemærkes, at målrettet registrering og opbevaring af trafikdata ikke vil sikre samme muligheder for at efterforske kriminalitet, herunder terror og grov kriminalitet, som i dag eller under perioder med generel og udifferentieret registrering og opbevaring, idet der ikke vil kunne registreres og opbevares samme mængde trafikdata.

Der henvises til pkt. 3.1.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til pkt. 3.1.3.1.

For det andet foreslås en ordning med generel og udifferentieret registrering og opbevaring, hvorefter justitsministeren bemyndiges til efter forhandling med erhvervsministeren at kunne fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må antages at være reel og aktuel eller forudsigelig (generel og udifferentieret registrering og opbevaring). Registrerings- og opbevaringspligten vil skulle udmøntes ved bekendtgørelse. Det foreslås, at registreringspligten højst vil kunne fastsættes for en periode på 1 år ad gangen.

Der henvises til pkt. 3.2.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til pkt. 3.2.3.1.

Det foreslås endvidere, at den forpligtelse, der i dag følger af logningsbekendtgørelsens § 5, stk. 1, om registrering og opbevaring af oplysninger om en brugers adgang til internettet ved den tildelte internetprotokol-adresse (IP-adresse) m.v., videreføres i retsplejeloven.

Der henvises til pkt. 3.3.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til pkt. 3.2.3.1.

Til brug for politiets og anklagemyndighedens arbejde med at sikre entydig identifikation af brugeren af et kommunikationsmiddel, bl.a. til brug for målrettet registrering og opbevaring af data, foreslås det, at der fastsættes en bemyndigelse for justitsministeren til efter forhandling med klima-, energi- og forsyningsministeren at kunne udstede regler om verificering af nummeroplysningsdata. Det forudsættes, at der fastsættes regler, hvorefter udbydere af elektroniske kommunikationsnet eller -tjenester vil kunne blive pålagt at verificere nummeroplysningsdata, som registreres og opbevares til brug for nummeroplysningsdatabasen. Dette særligt med det formål, at den såkaldte 118-database, som politiet har adgang til, opnår en datakvalitet, der kan understøtte målrettet personbestemt registrering og opbevaring af trafikdata. Herudover foreslås det, at telelovens § 31, stk. 2, ændres, så nummeroplysningsdatabasen fremadrettet også vil skulle indeholde oplysninger om unikt ID og eventuelle oplysninger om bruger. Dette med henblik på at understøtte, at politiet entydigt kan identificere en slutbruger af et givet kommunikationsmiddel.

Der lægges desuden op til, at der skal gælde et krav om registrering af nummeroplysningsdata for taletidskort. Det vil indebære, at der fra lovens ikrafttræden ikke længere vil kunne købes såkaldte ”anonyme” taletidskort (uregistrerede taletidskort).

Der henvises til pkt. 3.4 og 3.8.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til pkt. 3.2.3.1.

Endvidere foreslås det, at de gældende regler om hastesikring i retsplejelovens § 786 a ændres, så de er i overensstemmelse med EU-retten. Det vil efter forslaget således alene være muligt at anmode om hastesikring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet.

Der henvises til pkt. 3.5.

For så vidt angår domstolsprøvelse foreslås det, at der for registrering og opbevaring af trafikdata på grundlag af konkret begrundede pålæg, jf. den foreslåede § 786 d i retsplejeloven, indføres en ordning med forudgående retskendelse svarende til, hvad der kendes i dag for indgreb i meddelelshemmeligheden.

For generel og udifferentieret samt målrettet personbestemt og geografisk registrering og opbevaring af trafikdata, der ikke iværksættes på grundlag af konkret begrundede pålæg men automatisk, jf. de foreslåede bestemmelser i retsplejelovens § 786 b, § 786 c, § 786 e og § 786 f, vil der som i dag være adgang til domstolsprøvelse, jf. grundlovens § 63.

Der henvises til pkt. 3.6.

Politiets adgang til den registrerede og opbevarede trafikdata vil reguleres af retsplejelovens kapitel 71 og 74 om hhv. indgreb i meddelelshemmeligheden m.v. og edition.

Det foreslås, at regler om adgang til registrerede og opbevarede oplysninger i retsplejelovens kapitel 71 og 74 ændres, så de er i overensstemmelse med EU-retten. Det vil bl.a. indebære, at det efter forslaget alene vil være muligt at få adgang til oplysninger, der er registreret efter registrerings- og opbevaringspligterne i de foreslåede §§ 786 b-786 e i retsplejeloven, hvis det sker med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed.

Editionsreglerne foreslås desuden ændret, således at der som ved indgreb i meddelelshemmeligheden vil skulle beskikkes en advokat for den, hvis oplysninger politiet anmoder om adgang til, ligesom der som udgangspunkt vil skulle ske underretning af denne person ved indgrebets afslutning.

Der henvises til pkt. 3.7.

Endelig foreslås det, at der skal kunne fastsættes regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af §§ 786 a-786 f eller pålæg eller regler udstedt i medfør heraf, herunder regler med krav om opbevaring på servere i EU for data registreret efter de foreslåede regler.

Der henvises til pkt. 3.9.

2. Lovforslagets baggrund og formål

2.1. EU-Domstolens praksis før La Quadrature du Net-dommen

Lovforslaget har til formål at bringe reglerne om registrering og opbevaring samt reglerne om adgang til registrerede og opbevarede oplysninger i overensstemmelse med EU-Domstolens praksis vedrørende fortolkningen af artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet).

E-databeskyttelsesdirektivet indeholder regler om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor. Det følger navnlig af artikel 5, stk. 1, at medlemsstaterne skal sikre kommunikationshjemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata (princippet om kommunikationshjemmelighed). Det fremgår dog 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. E-databeskyttelsesdirektivets artikel 15, stk. 1, er gennemført i dansk ret ved retsplejelovens § 786, stk. 4.

EU-Domstolen har afsagt flere domme, der angår fortolkningen af e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med artikel 7 (om respekt for privatlivet), artikel 8 (om beskyttelse af personoplysninger) og artikel 11 (om ytrings- og informationsfrihed) i EU’s charter om Grundlæggende Rettigheder (Chartret).

Ved dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12, Digital Rights (Digital Rights-dommen), erklærer EU-Domstolen direktiv 2006/24/EF (logningsdirektivet) for ugyldigt, bl.a. med henvisning til, at direktivet 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 forebyggelse, efterforskning eller strafferetlig forfølgning af 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 Chartrets artikel 7 om respekt for privatliv og artikel 8 om beskyttelse af personoplysninger.

Ved dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 (Tele2-dommen), fastslår EU-Domstolen, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret pligt til lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugeres samtlige midler til elektronisk kommunikation. Domstolen fastslår samtidig, at EU-retten 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. Hvad angår reglerne om sikkerheden vedrørende og beskyttelsen af de data, der lagres af udbydere af elektroniske kommunikationstjenester, fastslår EU-Domstolen endelig, at artikel 15, stk. 1, ikke gør det muligt for medlemsstaterne at fravige direktivets artikel 4, stk. 1 eller stk. 1a, og at den nationale lovgivning derfor skal foreskrive en lagring på EU's område og en irreversibel destruktion af disse data ved udløbet af lagringsperioden.

Ved dom af 2. oktober 2018 i sag C-207/16, Ministerio Fiscal (Ministerio Fiscal-dommen), fastslår EU-Domstolen bl.a., at 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 på indehaverne, indebærer et indgreb i indehavernes grundlæggende rettigheder.

der i Chartrets artikel 7 og 8, der ikke er så alvorligt, at adgangen skal begrænses til forebyggelse, efterforskning og retsforfølgning af strafbare forhold med henblik på bekæmpelse af grov kriminalitet.

2.2. La Quadrature du Net-dommen

Den 6. oktober 2020 afsagde EU-Domstolen 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. (La Quadrature du Net-dommen). Dommen vedrører de franske og belgiske logningsreglers forenelighed 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 m.v. 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.

Domstolen fastslår således for første gang, under hvilke betingelser medlemsstaterne har mulighed for at pålægge teleudbydere m.v. 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 m.v. 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 en 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).

Domstolen udelukker imidlertid 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 også anfører i bl.a. Tele2-dommen, hvorefter medlemsstaterne kan pålægge teleudbydere m.v. 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 grov kriminalitet, 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 lagre målrettet i områder med høj hyppighed af grov kriminalitet samt steder, hvor der er en forhøjet risiko for, at grov kriminalitet bliver planlagt eller begået. Det kan ifølge Domstolen navnlig være steder, der er kendetegnet ved et højt antal tilfælde af grov kriminalitet, steder, hvor der i særlig grad kan begås kriminalitet, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde og vejafgiftsområder.

Den målrettede lagring af disse data må kun ske, så længe det er strengt nødvendigt i lyset af formålet og de omstændigheder, der retfærdiggør lagringen. 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 (præmis 152-156). Dette må dog alene ske med henblik på at bekæmpe grov kriminalitet, herunder 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 myn-

dighedernes adgang til IP-adresserne skal være nøje reguleret i lovgivningen. Domstolens IP-adressebegreb er dog ikke klart defineret, særligt i forhold til de efterfølgende præmisser 157-159.

Domstolen anfører endvidere i præmis 140, at det kun er bekæmpelsen af grov kriminalitet, herunder 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 trafik- og lokaliseringsdata indebærer. Det er således kun de indgreb i de nævnte rettigheder, der ikke er alvorlige, som kan begrundes i formålet om forebyggelse, efterforskning og retsforfølgning af alle strafbare handlinger.

For så vidt angår oplysninger om identiteten på brugerne af elektroniske kommunikationsmidler fastslår Domstolen, at medlemsstaterne kan pålægge teleudbydere m.v. at lagre data vedrørende personers identitet med henblik på at forhindre eller efterforske alle strafbare handlinger.

Lagring af data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, kan ifølge Domstolen 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 m.v. 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, hvor det er nødvendigt at pålægge teleselskaberne at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger, herunder 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 pågældendes sociale eller professionelle omgangskreds.

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

2.3. EU-Domstolens praksis efter La Quadrature du Net-dommen

Ved dom af 2. marts 2021 i sag C-746/18, H.K. (H.K.-dommen) gentager EU-Domstolen, at EU-retten er til hinder for lovgivningsmæssige foranstaltninger, der i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafik- og lokaliseringsdata, og at det i overensstemmelse med proportionalitetsprincippet kun er bekæmpelsen af grov kriminalitet, herunder 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.

3. Hovedpunkterne i lovforslaget

3.1. Målrettet registrering og opbevaring af trafikdata

3.1.1. Gældende ret

3.1.1.1. 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.

Bestemmelsen blev foreslået med henblik på at styrke politiets efterforskningsmuligheder, jf. forarbejderne til lov nr. 378 af 6. juni 2002 (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 af 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 fremgår af 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 ”de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold”. Det fremgår endvidere, at der vil kunne opstilles regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger. Endvidere fremgår det, at det bør tilstræbes, at reglerne sikrer, at korrekt dansk realtid registreres.

De nærmere regler om registrering og opbevaring, herunder hvilke oplysninger udbyderne skal registrere, fremgår af logningsbekendtgørelsen, jf. pkt. 3.1.1.2.

De nærmere betingelser for, hvornår udbyderne af elektroniske kommunikationsnet eller -tjenester skal udlevere oplysningerne til politiet, fremgår navnlig af retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. pkt. 3.7. Udlevering af oplysningerne kræver som

udgangspunkt, at rettens kendelse i hvert enkelt tilfælde opnås forud for udleveringen. Udbyderen af elektroniske kommunikationsnet eller -tjenester 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 og opbevare oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold gælder, uanset karakteren af kriminalitet. Der er derfor efter gældende ret ikke særlige regler for registrering med henblik på beskyttelse af den nationale sikkerhed eller bekæmpelse af grov kriminalitet.

3.1.1.2. 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 registrering af oplysninger om såkaldt sessionsregistrering (logging af en række forbindelsesoplysninger om internettrafik) blev ophævet.

Det fremgår af logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester 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). Efter telelovens § 2, nr. 1, skal ved »udbyder« forstås den, som med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester omfattet af teleloven til rådighed for andre. Det fremgår af bemærkningerne til telelovens § 2, at enhver, der markedsfører og sælger produkter og elektroniske kommunikationsnet eller -tjenester omfattet af teleloven til andre, anses for at være udbyder med de rettigheder, dette giver blandt andet i relation til netadgang. Det vil sige, at alle virksomheder, som på kommercielt

grundlag betjener andre slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester med henblik på at formidle dele af disses teletrafik, er omfattet af dette begreb.

Det har ikke betydning, hvilke former for kommunikationsnet eller -tjenester, der bliver stillet til rådighed. Om udbyderen stiller fastnet-, mobil- og internetforbindelser eller trådløse forbindelser via hot spots til rådighed, betyder derfor ikke noget for, hvorvidt udbyderen er omfattet af udbyderbegrebet eller ej. Ligeledes har det ingen betydning, om udbyderen selv har anlagt eller lejer sig ind på infrastruktur.

Centralt i udbyderbegrebet er, om tjenesten stilles til rådighed med kommercielt formål. Det kommercielle formål foreligger, hvis eksempelvis en virksomhed sælger eller markedsfører et produkt for at opnå en direkte eller indirekte fortjeneste. Det er uden betydning, om aktiviteten reelt medfører en fortjeneste. Stiller et hotel eksempelvis et hot spot op i lobbyen eller internet/telefoni til rådighed på værelserne, uden at der opkræves særskilt betaling herfor, vil hotellet blive anset for udbyder, fordi udbuddet af forbindelsen sker for at gøre hotellet mere attraktivt og dermed med det formål at opnå en fortjeneste.

Det kommercielle formål foreligger desuden, hvis der er tale om en aktivitet, som sædvanligvis tilbydes eller efterspørges på markedsmæssige vilkår, uanset om den pågældende virksomhed, forening, myndighed m.v. i det konkrete tilfælde søger at opnå en fortjeneste. Hvis eksempelvis en kommune udlejer lokaler til erhverv, og i den sammenhæng stiller internetadgang til rådighed for lejere, vil kommunen være udbyder i det konkrete tilfælde, fordi udlejning af erhvervslokaler sædvanligvis foregår på markedsmæssige vilkår, og fordi udbud af internetadgang i erhvervslokaler typisk sker for at gøre lejemålet mere attraktivt.

Registrerings- og opbevaringspligten påhviler således alene kommercielle udbydere af kommunikationsnet eller -tjenester. Biblioteker, hospitaler, universiteter og folkeskoler, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter (lånere, patienter, studerende m.v.) vil således eksempelvis ikke være at anse for kommercielle udbydere af kommunikationsnet eller -tjenester.

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. bekendtgørelsens §§ 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 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). De nærmere regler om IP-adresser beskrives nedenfor under pkt. 3.3.

Efter logningsbekendtgørelsens § 6, stk. 1, skal udbyderne registrere oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester, herunder oplysninger om modtagende og afsendende e-mailadresser. Efter § 6, stk. 2, skal udbyderne registrere oplysninger om kommunikation foretaget ved brug af udbyderens egne internettelefoni-tjenester for de i § 5, stk. 1, nævnte oplysninger.

Udbyderne er i ingen tilfælde pålagt at 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.

Overtrædelse af logningsbekendtgørelsens §§ 4-6 samt § 9 straffes med bøde, jf. logningsbekendtgørelsens § 10, stk. 1. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel, jf. logningsbekendtgørelsens § 10, stk. 2.

3.1.1.3. Andre regler om behandling af loggede oplysninger m.v.

Udbydere af elektroniske kommunikationsnet eller -tjenester er undergivet tavshedspligt, jf. telelovens § 7, stk. 1, 1. pkt., hvorefter ejere af elektroniske kommunikationsnet og udbydere af elektroniske kommunikationsnet eller -tjenester og nummerafhængige interpersonelle kommunikationstjenester og deres ansatte og tidligere ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af elektroniske kommunikationsnet eller -tjenester og nummerafhængige interpersonelle kommunikationstjenester. Det følger af § 7, stk. 1, 2. pkt., at de nævnte ejere og udbydere skal træffe de foranstaltninger, der er nødvendige for at sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelige for uvedkommende. Overtrædelse af telelovens § 7, stk. 1, straffes med bøde, jf. lovens § 81, stk. 1, nr. 1.

Telelovens § 7, stk. 2, fastslår, at straffelovens §§ 152, 152 a og 152 d-152 f (bestemmelser om tavshedspligt) finder anvendelse for den, der virker eller har virket hos en ejer af elektroniske kommunikationsnet eller en udbyder af elektroniske kommunikationsnet eller -tjenester og nummerafhængige interpersonelle kommunikationsnet, eller som i øvrigt er eller har været beskæftiget med opgaver, der udføres efter aftale med disse.

Tavshedspligten er ikke til hinder for, at oplysninger kan kræves udleveret, hvis det eksempelvis følger af en afgørelse for retten om indgreb i meddelelshemmeligheden eller edition, jf. herom i pkt. 3.7 om adgang til registrerede data. I sådanne tilfælde er udlevering ikke "uberettiget".

Herudover gælder bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester (persondatasikkerhedsbekendtgørelsen). Bekendtgørelsen er udstedt med hjemmel i § 8, stk. 1 og 4, § 80 og § 81, stk. 2, i lov om elektroniske kommunikationsnet og -tjenester. Bekendtgørelsen trådte i kraft den 21. december 2020. I den forbindelse blev bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester ophævet.

Bekendtgørelsen indebærer bl.a., at udbydere af offentlige elektroniske kommunikationsnet eller -tjenester og nummeruafhængige interpersonelle kommunikationstjenester er forpligtet til at overholde en række krav, der skal sikre persondatasikkerheden. De skal bl.a. som udgangspunkt sikre, at trafikdata vedrørende abonnenter eller brugere slettes eller anonymiseres, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. bekendtgørelsens § 10, stk. 1. Der gælder visse undtagelser hertil og nærmere krav til behandlingen af trafikdata, jf. bekendtgørelsens § 10, stk. 2-5. Det følger desuden af persondatasikkerhedsbekendtgørelsens § 11, stk. 1, at udbydere af offentlige elektroniske kommunikationsnet eller -tjenester eller udbydere af nummeruafhængige interpersonelle kommunikationstjenester kun må behandle lokaliseringsdata bortset fra trafikdata i nærmere bestemte tilfælde, jf. bekendtgørelsens § 11, stk. 1, nr. 1 og 2. Der gælder i den forbindelse visse krav til bl.a. underretning, oplysning og samtykke, ligesom der er fastsat regler om, at behandling af lokaliseringsdata, bortset fra trafikdata, i henhold til stk. 1-3 kun må foretages af personer, som er ansat hos eller handler efter bemyndigelse fra udbyderen af nettet eller tjenesten eller fra den tredjemand, som leverer tillægstjenesten, jf. § 11, stk. 2-4.

Kravene følger af Kommissionens forordning (EU) nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation.

Bekendtgørelse nr. 1144 af 20. november 2006 om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden (sikkerhedsgodkendelse af personale i telebranchen) er udstedt med hjemmel i § 786, stk. 5 og 7, i retsplejeloven. Bekendtgørelsen trådte i kraft den 1. marts 2007.

Det følger af bekendtgørelsens § 1, stk. 1, at udbydere af elektroniske kommunikationsnet eller -tjenester skal sikre, at medarbejdere eller repræsentanter for udbyderen, der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden, jf. lov om rettens pleje kapitel 71, sikkerhedsgodkendes af Rigspolitiet til at håndtere klassificerede oplysninger. De sikkerhedsgodkendte medarbejdere eller repræsentanter for udbyderen skal overholde Rigspolitiets krav vedrørende sikkerhedsforskrifter om behandling, opbevaring eller destruktion af klassificerede oplysninger, jf. bekendtgørelsens § 1, stk. 2.

Overtrædelse af bekendtgørelsens § 1 straffes med bøde. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel, jf. bekendtgørelsens § 3.

Bekendtgørelse nr. 1145 af 20. november 2006 om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden (døgnbetjent kontaktpunkt) er udstedt med hjemmel i § 786, stk. 5 og 7, i retsplejeloven. Bekendtgørelsen trådte i kraft den 1. marts 2007.

Det følger af bekendtgørelsens § 1, stk. 1, at udbydere af elektroniske kommunikationsnet eller -tjenester skal etablere et døgnbetjent kontaktpunkt, der til enhver tid kan bistå politiet i forbindelse med iværksættelsen af indgreb i meddelelseshemmeligheden, jf. lov om rettens pleje kapitel 71. Oplysninger om det døgnbetjente kontaktpunkt skal meddeles Rigspolitiets Telecenter. Mindre udbydere kan af Rigspolitiet efter ansøgning gives tilladelse til at etablere en vagtordning, hvor politiet har adgang til at rette henvendelse til bestemte medarbejdere eller repræsentanter for udbyderen, der kan sørge for det videre fornødne i forbindelse med iværksættelsen af indgreb i meddelelseshemmeligheden. Oplysninger om vagtordningen skal meddeles Rigspolitiets Telecenter, jf. bekendtgørelsens § 1, stk. 2.

Etablering af et døgnbetjent kontaktpunkt eller vagtordning kan efter aftale med udbyderen af elektroniske kommunikationsnet eller -tjenester på dennes vegne foretages af en anden udbyder eller af en tredjemand, jf. bekendtgørelsens § 2.

Overtrædelse af bekendtgørelsens § 1 straffes med bøde. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel, jf. bekendtgørelsens § 4.

3.1.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder La Quadrature du Net-dommen af 6. oktober 2020, er beskrevet under pkt. 2.

La Quadrature du Net-dommen medfører behov for en ændring af retsplejeloovens § 786, stk. 4, således at ordningen bringes i overensstemmelse med EU-retten som fortolket af EU-Domstolen.

For så vidt angår målrettet registrering og opbevaring 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 lagring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, herunder forebyggelse af alvorlige trusler mod den offentlige sikkerhed og med henblik på beskyttelse af den nationale sikkerhed,
- at dette forudsætter, at en sådan lagring 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 lagringen,
- at lagringsforpligtelsen 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, herunder forhindre en alvorlig fare for den offentlige sikkerhed eller en risiko for den nationale sikkerhed (personbestemt målrettet registrering),
- at lagringsforpligtelsen kan fastsættes på baggrund af et geografisk kriterium, når det 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 registrering), og

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

3.1.3. Justitsministeriets overvejelser og den foreslåede ordning

Som udgangspunkt vil der i medfør af EU-Domstolens praksis, som er beskrevet under pkt. 2, 3.1.2 og 3.2.2, alene kunne iværksættes målrettet registrering og opbevaring af trafikdata. Kun i tilfælde, hvor der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig, vil der kunne iværksættes generel og udifferentieret registrering og opbevaring. Det foreslås på den baggrund, at der indføres en ordning med målrettet personbestemt (se pkt. 3.1.3.1) og geografisk (se pkt. 3.1.3.2) registrering og opbevaring. Det bemærkes i den forbindelse, at EU-Domstolen i *La Quadrature du Net*-dommen har peget på, at en ordning med målrettet registrering og opbevaring netop vil kunne tage udgangspunkt i kategorier af berørte personer eller et geografisk kriterium, jf. præmis 168.

3.1.3.1. Målrettet personbestemt registrering og opbevaring

Det foreslås, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage målrettet personbestemt registrering og opbevaring af trafikdata på baggrund af objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafikdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet, herunder forhindre en alvorlig fare for den offentlige sikkerhed eller en risiko for den nationale sikkerhed.

Det foreslås, at pligten til at foretage målrettet personbestemt registrering og opbevaring af trafikdata begrænses til at gælde udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden.

Der er således tale om en indskrænkelse af pligten i forhold til den bredere gruppe af udbydere, der bl.a. er omfattet af pligten til at foretage generel og udifferentieret registrering og opbevaring af trafikdata og oplysninger om en slutbrugers adgang til internettet efter forslaget til de nye §§ 786 e og 786

f i retsplejeloven, jf. lovforslagets § 1, nr. 9 ("udbydere af elektroniske kommunikationsnet eller -tjenester", jf. pkt. 3.2.3.1).

Begrebet "udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden" omfatter udbydere, der driver virksomhed omfattet af teleloven som deres hovedvirksomhed eller som en selvstændig del af virksomheden. Udbydere, der har mobiltelefoni, faksnettelefoni, bredbånd m.v. som deres hovedvirksomhed, vil således være omfattet af begrebet.

Som en ikkeaccessorisk del af virksomheden forstås, at udbuddet ikke kun er en accessorisk del af virksomheden. Et hotel, der for eksempel tilbyder sine kunder adgang til trådløst internet, vil således ikke være omfattet af begrebet, idet udbuddet i den forbindelse må anses for at være en integreret del af at leje hotelværelset.

Derimod vil der, hvis eksempelvis en dagligvarevirksomhed beslutter at udbyde internet- eller taletelefonitjenester til salg til kunderne, ikke nødvendigvis være tale om, at udbuddet af internet eller taletelefonitjenester alene er en accessorisk del af at handle med dagligvarevirksomheden, da udbuddet vil kunne udgøre en selvstændig del af virksomheden. Dagligvarevirksomheden vil i dette tilfælde kunne være omfattet af begrebet "udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden". Der vil være tale om en konkret vurdering.

Indskrænkelsen i udbyderbegrebet for så vidt angår den foreslåede målrettede registrering og opbevaring skyldes, at en anvendelse af det vide udbyderbegreb, jf. pkt. 3.1.3.3 i lovforslagets almindelige bemærkninger, ville føre til, at samtlige udbydere af elektroniske kommunikationsnet eller -tjenester, herunder f.eks. også restauranter, caféer, campingpladser og hoteller, der eksempelvis tilbyder adgang til et trådløst internet-hot spot, ville skulle have oplysninger om, hvilke personer og områder der vil skulle registreres og opbevares oplysninger for i medfør af de foreslåede §§ 786 b-d i retsplejeloven.

Størstedelen af disse oplysninger forudsættes pga. deres karakter alene videreformidlet til ansatte, der er sikkerhedsgodkendt til at håndtere efterforskningsfølsomme oplysninger om indgreb i meddelelseshemmeligheden

fra politiet. Hertil kommer, at der ikke findes en udtømmende liste over udbydere af elektroniske kommunikationsnet eller -tjenester, og det derfor vil være vanskeligt at få overblik over, hvem oplysningerne i givet fald ville skulle videreformidles til. På den baggrund foreslås udbyderbegrebet indsnævret for så vidt angår den foreslåede målrettede ordning. Der henvises i øvrigt til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Hvis de omfattede oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne.

Det forudsættes, at målrettet personbestemt registrering og opbevaring af trafikdata kobles til den pågældende persons unikke ID (f.eks. cpr-nummer). Det vil indebære, at der vil skulle ske registrering og opbevaring af trafikdata hidrørende fra alle kommunikationsmidler, som den pågældende person er registreret som abonnent for eller bruger af. Der henvises til pkt. 3.4.2.

EU-Domstolen har efter Justitsministeriets opfattelse sat en forholdsvis lav tærskel – jf. ordlyden ”kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet” i La Quadrature du Net-dommens præmis 148 – for kravet til, hvor underbygget grundlaget for beslutningen om, at en given person skal være omfattet af et pålæg om målrettet personbestemt registrering og opbevaring, skal være.

Det er på denne baggrund Justitsministeriets vurdering, at personer kan være omfattet af en pligt for udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, til at foretage målrettet personbestemt registrering, når visse objektive forhold tilsiger, at trafikdata om de pågældende – direkte eller indirekte – kan medvirke til at afdække en forbindelse til grov kriminalitet.

Ved ”grov kriminalitet” forstås samme kriminalitetskrav, som også foreslås at skulle gælde for udlevering af registrerings- og opbevaringspligtige oplysninger, jf. de foreslåede §§ 781 a og 804 a i retsplejeloven. Herefter vil grov kriminalitet blive karakteriseret som lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af

retsplejelovens § 781, stk. 2 eller 3, eller lovovertrædelser, som kan medføre strafforhøjelse efter straffelovens § 81 a. Der henvises til pkt. 3.7.3.

3.1.3.1.1. Måltrettet registrering og opbevaring for personer, der er dømt for grov kriminalitet

Det foreslås, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage måltrettet personbestemt registrering og opbevaring af trafikdata for personer, der er dømt for grov kriminalitet. For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

Personer, der er dømt for grov kriminalitet vil være i risiko for at recidivere til ny kriminalitet, herunder grov kriminalitet. Derudover må det antages, at disse personer til en vis grad har deres omgangskreds i kriminelle miljøer og dermed ofte vil have kontakt med andre kriminelle personer. Måltrettet personbestemt registrering og opbevaring af trafikdata vedrørende personer dømt for grov kriminalitet vil derfor i nogle tilfælde give politiet mulighed for at anvende registrerings- og opbevaringspligtige oplysninger i forbindelse med efterforskningen af eventuelle kriminelle forbindelser til grov kriminalitet, som disse personer måtte have. En forpligtelse for udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, til at foretage måltrettet personbestemt registrering og opbevaring for sådanne personer må derfor antages at kunne medvirke til opklare og retsforfølge grov kriminalitet.

Er personen dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 3 år, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som har medført strafforhøjelse efter straffelovens § 81 a, foreslås det, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, skal registrere trafikdata fra personen i 3 år.

Er personen dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 6 år, foreslås det, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, skal registrere trafikdata fra personen i 5 år.

Er personen dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 8 år, foreslås det, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, skal registrere trafikdata fra personen i 10 år.

Er den pågældende dømt for flere lovovertrædelser ved samme dom, vil der skulle tages udgangspunkt i den højeste strafferamme. Er personen dømt for en lovovertrædelse i straffelovens kapitel 12 og 13, der har en strafferamme på mindst 6 år, vil der efter lovforslaget skulle registreres trafikdata for vedkommende i 5 år. Er personen dømt for en lovovertrædelse i straffelovens kapitel 12 og 13, der har en strafferamme på mindst 8 år, vil der efter lovforslaget skulle registreres trafikdata for vedkommende i 10 år.

Det foreslås, at hvis den pågældende er idømt en ubetinget frihedsstraf, regnes den periode, som trafikdata fra den pågældende registreres for (3, 5 eller 10 år), fra tidspunktet for endelig løsladelse fra afsoning. Prøveløslades den pågældende, regnes perioden fra tidspunktet for prøveløsladelse. Genindsættes den pågældende til afsoning (f.eks. pga. manglende overholdelse af prøveløsladelsesvilkårene) fortsætter registreringsperioden under afsoningen uden afbrydelse og regnes fortsat fra prøveløsladelsestidspunktet. Er den pågældende person idømt en betinget frihedsstraf, regnes perioden fra endelig dom. Er den pågældende idømt anden strafferetlig retsfølge efter straffelovens §§ 68-70, regnes perioden fra endelig ophævelse af denne retsfølge. Dog regnes perioden fra endelig dom, hvis den pågældende er dømt til ambulant behandling, der ikke medfører eller kan medføre indlæggelse i institution.

Selvom registreringsperioden således først løber fra løsladelsestidspunktet mv., og der derfor som udgangspunkt ikke vil ske registrering og opbevaring under afsoningen, kan der efter en konkret vurdering iværksættes registrering og opbevaring også under afsoning (se nedenfor vedrørende målrettet registrering og opbevaring på baggrund af konkret begrundede pålæg).

Hvis den pågældende inden for registreringsperioden på ny dømmes for grov kriminalitet, som vil medføre, at der vil skulle registreres og opbevares oplysninger om den pågældende, vil der løbe en selvstændig registreringsperiode for denne registrering fra prøveløsladelse m.v., mens den igangværende opbevaring kan fortsætte, indtil den fastsatte frist. I disse tilfælde vil registrerings- og opbevaringsperioden muligvis kunne løbe under en afsoning. Der lægges ikke med lovforslaget op til, at der skal være mulighed for at slå registreringsperioder sammen.

Det bemærkes i forlængelse heraf, at det vil kræve ny systemteknisk understøttelse at håndtere en automatiseret iværksættelse af målrettet registrering og opbevaring af trafikdata fra de omfattede personer. Der henvises til pkt. 3.1.3.4.

3.1.3.1.2. Målrettet registrering og opbevaring for kommunikationsapparater og personer, der har været genstand for visse indgreb i meddelelseshemmeligheden

Det foreslås desuden, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata fra kommunikationsapparater og personer, der har været genstand for indgreb i meddelelseshemmeligheden i medfør af retsplejelovens § 780, stk. 1, nr. 1 (telefonaflytning) eller nr. 3 (teleoplysning). For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

Er indgrebet iværksat på et specifikt telefonnummer el. lign., vil registreringen af trafikdata også skulle iværksættes for den person, telefonnummeret el. lign. tilhører, dvs. at registreringen og opbevaringen også omfatter trafikdata fra eventuelle andre kommunikationsmidler eller abonnementer, som vedkommende er indehaver af eller senere vil blive indehaver af. Indehaver vil i den forbindelse skulle forstås som den, der efter gældende ret ville skulle underrettes om indgrebet i medfør af retsplejelovens § 788, dvs. indehaveren af telefonabonnementet eller telefonen alt afhængig af, om det er telefonnummeret eller IMEI-nummeret, der har dannet grundlag for indgrebet, jf. nærmere herom om de gældende regler i pkt. 3.7.1.2.

Det forudsættes i den forbindelse, at registrering og opbevaring af trafikdata for personer, der har været genstand for et af de omfattede indgreb, kobles til den pågældende persons unikke ID (f.eks. cpr-nummer). Det vil indebære, at der vil skulle ske registrering og opbevaring af trafikdata hidrørende fra alle kommunikationsmidler, som den pågældende person er registreret som abonnent for eller bruger af. Der henvises til pkt. 3.4.2.

Justitsministeriet har i forbindelse med overvejelserne om forslaget lagt vægt på, at indgreb i meddelelseshemmeligheden i form af telefonaflytning eller teleoplysning i medfør af retsplejelovens § 780, stk. 1, nr. 1 og 3, som ikke foreslås ændret, kun kan iværksættes, hvis det telefonnummer eller den person, som kendelsen omhandler, har en direkte eller indirekte forbindelse til grov kriminalitet. Det skyldes, at det efter retsplejelovens § 781, stk. 1, nr. 1, er en betingelse for at foretage indgreb i meddelelseshemmeligheden, at der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser til eller fra en mistænkt. Hertil kommer, at indgreb i medfør af retsplejelovens § 780, stk. 1, nr. 1 og 3, kræver, at der indhentes en retskendelse og således er undergivet domstolskontrol.

Det foreslås, at længden af registreringsperioden skal være 1 år fra det tidspunkt, indgrebet afsluttes. Indgreb i medfør af § 780, stk. 1, nr. 1, betragtes som afsluttet, når politiet inden udløbet af fristen anmoder udbyderen om, at tage aflytningen ned, eller når indgrebet udløber. For så vidt angår indhentelse af fremadrettet teleoplysning, jf. § 780, stk. 1, nr. 3, dvs. oplysninger om kommunikation, der finder sted løbende og i realtid, jf. pkt. 3.7.1.2.1, betragtes indgrebet som afsluttet, når politiet inden udløbet af fristen for indgrebet anmoder udbyderen om at nedtage indgrebet, eller når indgrebet udløber, mens det for indhentelse af historiske teleoplysninger vil anses for afsluttet på tidspunktet for indhentelse af kendelsen herom.

Det følger af retsplejelovens § 786, stk. 2, at indehaveren af en telefon eller andet kommunikationsapparat kan give samtykke til foretagelse af teleoplysning. Indgreb efter retsplejelovens § 780, stk. 1, nr. 3, anvendes således kun, når indehaveren af kommunikationsapparatet ikke har givet samtykke. Det forudsættes, at der i forbindelse med indhentelse af et sådant samtykke også vil kunne indhentes samtykke til den efterfølgende tidsbegrænsede registrering og opbevaring af trafikdata. Det vil i den forbindelse være et krav, at samtykket er klart og utvetydigt og kommer fra den person, registrerings- og opbevaringspligten vedrører. Samtykket vil til enhver tid kunne trækkes tilbage.

Hvis et kommunikationsapparat eller en person inden for registreringsperioden på ny bliver genstand for et indgreb i meddelelshemmeligheden, der vil medføre, at der vil skulle registreres og opbevares oplysninger om det pågældende kommunikationsapparat eller den pågældende person, vil der løbe en selvstændig registreringsperiode for denne registrering, mens den igangværende registrering og opbevaring kan fortsætte indtil den fastsatte frist. Der lægges ikke med lovforslaget op til, at der skal være mulighed for at slå registreringsperioder sammen.

3.1.3.2. Målrettet geografisk registrering og opbevaring

Det foreslås, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage målrettet geografisk registrering og opbevaring på grundlag af objektive og ikke-diskriminerende forhold, der tilsiger, at der i et givet område er en forhøjet risiko for, at der planlægges eller begås grov kriminalitet. For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

3.1.3.2.1. Målrettet registrering og opbevaring i områder med forhøjet risiko for, at der planlægges eller begås grov kriminalitet

Det er vurderingen, at der vil være en forhøjet risiko for, at der planlægges eller begås grov kriminalitet i områder på 3 km gange 3 km, hvor antallet af anmeldelser om grov kriminalitet begået i området udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Det er endvidere vurderingen, at der vil være en forhøjet risiko for, at der planlægges grov kriminalitet i områder på 3 km gange 3 km, hvor antallet af beboere dømt for grov kriminalitet udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Den foreslåede størrelse på områder á 3 km gange 3 km er fastsat ud fra en vurdering af, at det ved områder af denne størrelse vurderes muligt at etablere en ordning, som kan implementeres i samspil mellem myndighederne og udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, som skal udpege de master, der er nødvendige

for at dække området. Samtidig er det vurderingen, at den praktiske implementering af målrettet registrering og opbevaring af trafikdata vedrørende områder af denne størrelse vil være i overensstemmelse med EU-rettens krav om alene af foretage registrering og opbevaring i det omfang, det er strengt nødvendigt.

Det foreslås på den baggrund, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på områder på 3 km gange 3 km, hvor:

- 1) antallet af anmeldelser af lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, eller
- 2) antallet af beboere dømt for lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

Det foreslås desuden, at justitsministeren efter forhandling med erhvervsministeren vil kunne fastsætte nærmere regler om geografisk målrettet registrering og opbevaring af trafikdata.

3.1.3.2.2. Målrettet registrering og opbevaring i særligt sikringskritiske områder

Det er desuden vurderingen, at der er områder, hvor der er særlige beskyttelseshensyn, der kan begrunde, at området anses for at være særligt sikringskritisk, og at der på den baggrund kan være behov for at foretage registrering og opbevaring af trafikdata vedrørende sådanne områder. Eksempelvis på baggrund af en vurdering af, at der er tale om et trafikknudepunkt, som en stor mængde personer jævnligt passerer igennem, at der i området kan befinde sig personer med et særligt beskyttelsesbehov, eller at der er tale om et område, der på grundlag af sin funktion i sig selv er særligt sikringskritisk.

Det foreslås derfor, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage målrettet geografisk registrering og opbevaring af trafikdata på særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, Marienborg Slot, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser. Eksemplerne er ikke udtømmende.

For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

3.1.3.3. Målrettet registrering og opbevaring på baggrund af konkret begrundede pålæg

Det foreslås desuden, at der kan meddeles udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, pålæg om at foretage målrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, som politiet har grund til at antage har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

For så vidt angår begrebet ”udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden” henvises til pkt. 3.1.3.1.

Med forslaget vil der således konkret – efter rettens kendelse – kunne meddeles pålæg om registrering og opbevaring af trafikdata fra kommunikationsapparater og personer, som politiet har grund til at antage har forbindelse til grov kriminalitet, uden at der har været tilstrækkeligt grundlag for at domfælde eller at iværksætte de omfattede indgreb i meddelelshemmeligheden mod pågældende.

Der vil desuden – efter rettens kendelse – kunne meddeles pålæg om registrering af trafikdata for bestemte områder, som politiet har grund til at antage har forbindelse til grov kriminalitet, uden at området er omfattet af den foreslåede § 786 c, stk. 1 og 2, i retsplejeloven.

Det foreslåede krav om, at der skal være grund til at antage, at kommunikationsapparater, personer eller bestemte områder har en forbindelse til grov kriminalitet vil medføre, at kravet for at foretage målrettet registrering og opbevaring af trafikdata efter den foreslåede § 786 d i retsplejeloven vil være lavere end det krav, der gælder for at foretage indgreb i meddelelshemmeligheden efter den gældende § 781, stk. 1, nr. 1. Dette skal ses i lyset af, at der på tidspunktet for iværksættelse af registrering og opbevaring af trafikdata ikke nødvendigvis vil være en nærmere konkretiseret mistanke om, at en bestemt person har begået eller vil begå en lovovertrædelse, eller at der er eller vil blive begået lovovertrædelser på et bestemt område. Der vil derfor også kunne meddeles pålæg om registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, når politiet har grund til at antage, at der er en forbindelse til planlægning af grov kriminalitet.

Politiet vil efter en konkret vurdering f.eks. kunne anmode retten om at træffe afgørelse om meddelelse af pålæg om registrering og opbevaring af trafikdata fra:

- kommunikationsapparater, som politiet har grund til at antage benyttes eller har været benyttet i forbindelse med kriminelle aktiviteter, uanset at brugeren af apparatet ikke konkret kan identificeres,
- mistænkte personer, der er, eller har været, genstand for tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet, og som ikke er omfattet af muligheden for at registrere og opbevare

trafikdata fra personer, der har været genstand for indgreb efter retsplejelovens § 780, stk. 1, nr. 1 eller 3,

- personer, der er undergivet systematisk, politimæssig monitoring, eksempelvis inden for rocker- og bandeområdet, herunder randpersoner fra rocker-/bandemiljøet,
- personer, der har været i kontakt med personer, der er eller har været genstand for et tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet,
- afsonere,
- forurettede og
- personer med nære relationer til personer, der har forbindelse til grov kriminalitet, som f.eks. ægtefæller eller samlevende.

Politiet vil desuden efter en konkret vurdering kunne anmode retten om at træffe afgørelse om meddelelse af pålæg om registrering og opbevaring af trafikdata for bestemte områder, hvor der midlertidigt er grund til at antage, at der er en forhøjet risiko for, at grov kriminalitet begås eller planlægges i forbindelse med større forsamlinger, områder for statsbesøg, festivaler. Det kan f.eks. være terrorrelaterede sager.

Kommunikationsapparater, personer eller bestemte områder, der hidtil har været registreret og opbevaret trafikdata for efter en af de andre foreslåede hjemler relateret til målrettet personbestemt eller geografisk registrering og opbevaring, vil også kunne blive genstand for et konkret begrundet pålæg om registrering og opbevaring af trafikdata. I så fald vil det på lige fod med øvrige konkret begrundede pålæg være en betingelse, at politiet har grund til at antage, at kommunikationsapparatet, personen eller området har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelse eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Eksemplerne er ikke udtømmende.

Det vil i alle tilfælde være et krav, at politiet har grund til at antage, at det kommunikationsapparat, den person eller det område, som et pålæg om registrering og opbevaring af trafikdata påtænkes rettet imod, har en direkte eller indirekte forbindelse til grov kriminalitet.

For så vidt angår målrettet geografisk registrering og opbevaring på baggrund af konkret begrundede pålæg bemærkes det, at størrelsen af det bestemte område vil afhænge af den konkrete forbindelse til grov kriminalitet. Hvis der eksempelvis er mistanke om et forestående bandedrab eller mistanke om et forestående terrorangreb, vil området omfattet af det konkret begrundede pålæg kunne udstrækkes til at omfatte hele det nødvendige område, f.eks. til en hel bydel eller en landsdel. Det forudsættes, at domstolene som led i proportionalitetsvurderingen vil tage højde for, at registrering og opbevaring af trafikdata afgrænses til det strengt nødvendige under hensyntagen til kriminalitetens art, og hvad der er teknisk muligt.

Det bemærkes endvidere, at det vil være et krav for meddelelse af konkret begrundede pålæg om registrering og opbevaring af trafikdata, at politiet indhenter rettens kendelse herom, jf. pkt. 3.6. Registreringsperioden regnes fra tidspunktet for pålæggets udstedelse.

Et pålæg om målrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, som politiet har grund til at antage har en forbindelse til grov kriminalitet, skal være skriftligt og skal angive hjemlen for pålæggets udstedelse, samt hvilket apparat eller hvilken person eller hvilket bestemt område (f.eks. relevante koordinater) registreringen og opbevaringen af trafikdata er rettet imod. I det omfang pålægget angår en bestemt person, kan retten i kendelsen for pålægget angive de eventuelle kommunikationsmidler, som den pågældende benytter uden at være registreret som bruger heraf. Det skal endvidere angives i pålægget, hvilket tidsrum pålægget om registrering og opbevaring af trafikdata gælder for. Tidsrummet skal være så kort som muligt og må ikke overstige 6 måneder ad gangen. Tidsrummet vil kunne forlænges, men højst med 6 måneder ad gangen. Forlængelsen vil skulle ske ved kendelse, jf. nærmere i pkt. 3.6.3.2.

Det følger 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. Overtrædelse af telelovens § 10, stk. 4, kan efter de gældende regler straffes med bøde, jf. telelovens § 81, stk. 1, nr. 1. På tilsvarende vis foreslås det, at der vil kunne pålægges bødestraf, hvis udbydere, som med et kommercielt for-

mål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, uden lovlig grund afviser at efterkomme et pålæg om iværksættelse af målrettet registrering og opbevaring, eller hvis iværksættelsen af pålægget ikke sker straks.

Det bemærkes, at det ikke vil udgøre en overtrædelse af de sektorspecifikke regler i bl.a. teleloven, hvis en udbyder, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, i overensstemmelse med et pålæg fra politiet har foretaget registrering og opbevaring, og pålægget senere f.eks. måtte blive underkendt, jf. nærmere nedenfor om prøvelse.

Der er ikke adgang til, at en udbyder, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, foretager en retlig efterprøvelse af, om betingelserne konkret er opfyldt. Ansvar for, at betingelserne for at påbegynde registrering og opbevaring er opfyldt, ligger således alene hos de myndigheder, der er kompetente til at pålægge registrering og opbevaring. Foretager udbyderen behandling af en eller flere personoplysninger i form af registrering og opbevaring på baggrund af den retlige forpligtelse, som et pålæg om registrering og opbevaring indebærer, påhviler det alene udbyderen at kunne dokumentere, at et sådant pålæg er udstedt. Såfremt et pålæg konkret måtte give anledning hertil, f.eks. pga. dets omfang, er der imidlertid ikke noget til hinder for, at udbyderen søger pålæggets udstrækning bekræftet hos politiet. Politiets bekræftelse heraf vil i den forbindelse være tilstrækkelig dokumentation for, at udbyderen har sikret den fornødne dokumentation af grundlaget for den iværksatte registrering og opbevaring.

3.1.3.4. Generelt

Det foreslås, at registrerings- og opbevaringspligten for så vidt angår de foreslåede ordninger med målrettet personbestemt og geografisk registrering og opbevaring vil skulle omfatte de data, der er registrerings- og opbevaringspligtige i dag. Det vil sige de data, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som ”teletrafik” (trafikdata). Visse lokaliseringsdata, som udgør trafikdata i forbindelse med telefoni- og sms/mms-kommunikation, er også i dag registrerings- og opbevaringspligtige, idet de anses for omfattet af forpligtelsen i retsplejelovens

§ 786, stk. 4, eller regler fastsat i medfør heraf. Det gælder oplysninger om den eller de celler, en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen. Disse data vil efter lovforslaget også fremadrettet være registrerings- og opbevaringspligtige.

Det foreslås således, at målrettet registrering og opbevaring vil gælde alle typer trafikdata.

Begrebet trafikdata skal forstås i overensstemmelse med e-databeskyttelsesdirektivets artikel 2, litra b og c. Ved trafikdata forstås data, som behandles med henblik på overførsel af kommunikation i et elektronisk kommunikationsnet eller debitering heraf.

Ved trafikdata forstås nærmere:

- 1) opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 2) opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 3) ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 4) kvittering for modtagelse af meddelelser,
- 5) identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre),
- 6) den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,
- 7) tidspunktet for kommunikationens start og afslutning,
- 8) oplysninger om afsendende e-mailadresse og
- 9) oplysninger om modtagende e-mailadresse.

Det bemærkes, at det i dag også påhviler udbydere af elektroniske kommunikationsnet eller -tjenester at registrere og opbevare oplysninger om tidspunktet for første aktivering af anonyme tjenester (taletidskort). Som følge af forslaget om krav om registrering af nummeroplysningsdata for uregistrerede taletidskort vil der dog fra lovens ikrafttræden ikke længere kunne købes nye anonyme taletidskort. Der henvises til pkt. 3.4.2. På den baggrund lægges der op til ikke at lade oplysninger om tidspunktet for første aktivering af anonyme tjenester (taletidskort) omfatte af pligten til registrering og opbevaring.

Med benævnelsen af identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre) i opremsningen ovenfor (nr. 5), sigtes der til oplysninger om identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre), når de genereres i forbindelse med trafik (som trafikdata, der er registrerings- og opbevaringspligtige i medfør af de foreslåede §§ 786 a-786 e). Det bemærkes imidlertid, at identiteten på det benyttede kommunikationsudstyr (f.eks. IMSI- og IMEI-numre) vil kunne udleveres efter den foreslåede § 804 b, stk. 1, hvis sådanne oplysninger ikke er registreret og opbevaret som trafikdata i medfør af de foreslåede §§ 786 a-786 e. Det vil således være en forudsætning for udlevering efter den foreslåede § 804 b, stk. 1, at udbyderne af elektroniske kommunikationsnet eller -tjenester er i besiddelse af oplysningerne på andet grundlag. Der henvises til pkt. 3.7.4.

Det bemærkes desuden, at udbyderne af elektroniske kommunikationsnet eller -tjenester herudover for en begrænset periode råder over yderligere lokaliseringsdata i egne systemer til brug for fejlretning. Politiet vil i dag kunne hastesikre og få adgang til disse data efter retsplejelovens regler herom. Det gælder dels lokaliseringsdata, der udgør trafikdata i forbindelse med internetforbrug, dels lokaliseringsdata, der ikke udgør trafikdata, fra tændte telefoner, der ikke anvendes aktivt. Der lægges med lovforslaget op til, at disse yderligere lokaliseringsdata fremover fortsat *ikke* skal være registrerings- og opbevaringspligtige. Politiet vil derfor fortsat kunne få adgang til sådanne data efter de gældende regler om edition i det omfang, udbyderne af elektroniske kommunikationsnet eller -tjenester er i besiddelse heraf. Det samme gælder trafikdata, der ikke gøres registrerings- og opbevaringspligtig efter den foreslåede ordning med målrettet registrering og opbevaring. Dvs. trafikdata, der ikke vedrører kommunikationsapparater, personer eller områder omfattet af ordningen med målrettet registrering og opbevaring. Det bemærkes i den forbindelse, at udbyderne af elektroniske kommunikationsnet eller -tjenester har oplyst, at de som udgangspunkt sletter oplysninger, der ikke er registrerings- og opbevaringspligtige, efter ca. 14 dage. Forslaget indebærer, at der efter de gældende regler om edition kan opnås adgang til oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, mens oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, vil skulle tilgås efter de foreslåede regler om adgang til oplysninger registreret og opbevaret efter de foreslåede §§ 786 a-786 e i

retsplejeloven, hvorefter der kun vil kunne opnås adgang til oplysningerne, hvis anmodningen sker med henblik på at bekæmpe grov kriminalitet.

Det bemærkes endvidere, at med benævnelsen af oplysninger om afsendende e-mailadresse og modtagende e-mailadresse i opremsningen ovenfor (nr. 8 og 9), menes oplysninger om modtagende og afsendende e-mailadresser fra udbyderens egne e-mailtjenester.

Endelig bemærkes det, at det med den foreslåede model vil påhvile udbyderne at kunne adskille oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, fra oplysninger, der ikke er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, således at det er muligt også ved politiets adgang til data at tage højde for, om der er tale om oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, eller ej.

Efterforskningen af sager om grov kriminalitet kan have en international dimension og vil ofte strække sig over længere perioder, ligesom grove kriminelle handlinger eller planlægningen heraf også vil kunne strække sig over længere perioder. Politiet har endvidere erfaring med, at større sager om grov kriminalitet, der efterforskes over længere tid, vil kunne kaste lys over ældre forhold, hvor det viser sig, at der er brug for teleoplysninger tilbage i tid. Endvidere vil de sager om national sikkerhed, 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 m.v., herunder efterforskningen af sådanne sager, ofte have en kompleksitet og et tidsmæssigt perspektiv, der kan strække sig over lang tid.

Det foreslås på den baggrund, at data registreret i medfør af de foreslåede regler om målrettet personbestemt og geografisk registrering og opbevaring skal opbevares i 1 år.

Det vil kunne variere over tid, hvor i landet der er en forhøjet risiko for, at der planlægges eller begås grov kriminalitet m.v., eller hvor i landet, der er særlige beskyttelseshensyn, der kan begrunde, at området anses for at være særligt sikringskritisk. Den nærmere registrering og opbevaring af trafikdata for områder, hvor der er en sådan forhøjet risiko, vil således skulle tilpasses løbende ud fra en vurdering af det aktuelle kriminalitetsbillede.

Det foreslås på den baggrund, at myndighederne årligt skal udarbejde en oversigt over områder omfattet af de foreslåede § 786 c, stk. 1 (områder med et større antal anmeldelser om grov kriminalitet og områder med et større antal beboere dømt for grov kriminalitet) og 2 (særligt sikringskritiske områder). Af oversigten vil skulle fremgå tilstrækkelige oplysninger til så præcist som muligt at udpege de oplistede omfattede geografiske områder, eksempelvis ved angivelse af præcise koordinater. Oversigten vil skulle videreformidles til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, med henblik på iværksættelse af målrettet registrering og opbevaring på de oplistede områder.

Oplysningerne på oversigten vil præcist angive, hvilke geografiske områder der i det givne år vil skulle foretages målrettet geografisk registrering og opbevaring vedrørende. Sådanne oplysninger vil, hvis de offentliggøres, kunne medføre en betydelig forhøjelse af risikoen for omgåselse, idet det ud fra oplysningerne også vil være muligt at sammenstykke et billede af, hvor der ikke foretages målrettet geografisk registrering og opbevaring af trafikdata. Det vil kunne have en negativ effekt på de retshåndhævende myndigheders mulighed for at efterforske og retsforfølge grov kriminalitet.

Desuden vil der af oversigten kunne fremgå informationer om områder, der vil kunne give et indblik i konkrete igangværende efterforskninger, hvilket også vil kunne have en negativ betydning for de retshåndhævende myndigheders mulighed for at efterforske og retsforfølge grov kriminalitet. Der vil endvidere kunne indgå oplysninger, hvor hensynet til statens sikkerhed tilsiger, at de ikke kan offentliggøres.

Herudover vil myndighederne skulle videreformidle retskendelser med konkrete pålæg om målrettet registrering og opbevaring for konkrete geografiske områder indhentet efter den foreslåede § 786 d i retsplejeloven til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden. For oplysninger om konkrete områder, hvor der på baggrund af konkrete pålæg vil skulle ske målrettet geografisk registrering og opbevaring af trafikdata, gælder de samme betragtninger om muligheden for at efterforske og retsforfølge grov kriminalitet, som gælder oplysningerne på den årlige oversigt over geografiske områder.

Oplysningerne på oversigten over geografiske områder og oplysninger om de konkret begrundede pålæg om målrettet geografisk registrering og opbevaring af trafikdata vil derfor ikke blive offentliggjort.

Myndighederne vil desuden skulle videreformidle oplysninger om, hvilke personer der skal foretages målrettet personbestemt registrering og opbevaring af trafikdata for efter de foreslåede regler i § 786 b i retsplejeloven til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, med henblik på iværksættelse af målrettet registrering og opbevaring af trafikdata for de omfattede personer. Oplysningerne skal være tilstrækkelige til, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, kan iværksætte målrettet personbestemt registrering og opbevaring af trafikdata for de pågældende personer.

Myndighederne vil også skulle videreformidle retskendelser med konkret begrundede pålæg om målrettet registrering og opbevaring af trafikdata for konkrete personer indhentet efter den foreslåede § 786 d i retsplejeloven til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden.

På samme måde som oplysninger om de konkrete pålæg om målrettet geografisk registrering og opbevaring af trafikdata vil oplysninger om personer omfattet af den foreslåede § 786 b, stk. 4, i retsplejeloven og oplysninger om konkret begrundede pålæg om målrettet personbestemt registrering og opbevaring af trafikdata efter den foreslåedes § 786 d i retsplejeloven kunne give et indblik i igangværende efterforskninger, hvilket vil kunne have en negativ betydning for politiets efterforskningsmuligheder. Der vil endvidere kunne indgå oplysninger, hvor hensynet til statens sikkerhed tilsiger, at de ikke kan offentliggøres.

I forlængelse heraf forudsættes det, at oplysninger om de omfattede geografiske områder og personer samt oplysningerne om de konkret begrundede pålæg vedrørende personer og områder alene videreformidles til ansatte hos udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk

del af virksomheden, der er sikkerhedsgodkendt til at håndtere sådanne oplysninger om indgreb i meddelelshemmeligheden fra politiet.

Det forudsættes endvidere, at

- oplysninger på den årlige oversigt over geografiske områder, der vil skulle foretages målrettet geografisk registrering og opbevaring af trafikdata for, jf. den foreslåede § 786 c i retsplejeloven,
- oplysninger om personer, der skal foretages målrettet personbestemt registrering og opbevaring af trafikdata for, jf. den foreslåede § 786 b, stk. 4, og
- oplysninger om konkret begrundede pålæg om målrettet geografisk og personbestemt registrering og opbevaring af trafikdata, jf. den foreslåede § 786 d

vil kunne undtages fra aktindsigt. Der kan i den forbindelse henvises til § 19, stk. 1, i lov om offentlighed i forvaltningen (offentlighedsloven), hvorefter retten til aktindsigt ikke omfatter sager inden for strafferetsplejen. Hvis de nævnte oplysninger ikke indgår i en sag inden for strafferetsplejen, kan der desuden henvises til offentlighedslovens § 30, nr. 1, som fastsætter, at retten til aktindsigt ikke omfatter oplysninger om enkeltpersoners private, herunder økonomiske, forhold, offentlighedslovens § 31, hvorefter retten til aktindsigt kan begrænses, i det omfang det er af væsentlig betydning for statens sikkerhed eller rigets forsvar, samt offentlighedslovens § 33, nr. 1, hvorefter retten til aktindsigt kan begrænses, i det omfang det er nødvendigt til beskyttelse af væsentlige hensyn til bl.a. forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Det forudsættes i forlængelse heraf, at de nævnte oplysninger ikke vil kunne kræves udleveret til brug for en retssag, jf. retsplejeloven § 41 d, stk. 5, nr. 2 og 6, samt retsplejelovens § 169, stk. 2, 3. pkt.

Registrerings- og opbevaringspligten for udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, vil for så vidt angår de foreslåede ordninger med målrettet personbestemt og geografisk registrering og opbevaring efter forslaget gælde fra det tidspunkt, hvor udbyderne har modtaget tilstrækkelige oplysninger om de omfattede personer og områder fra myndighederne til at iværksætte registrering og opbevaring målrettet de pågældende personer og områder. For så vidt angår konkret begrundede pålæg om målrettet registrering og opbevaring indhentet efter

den foreslåede § 786 d i retsplejeloven vil dette være ved udbydernes modtagelse af den indhentede retskendelse.

For så vidt angår den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata bemærkes det, at master tilhørende udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, er placeret forskelligt. Områder, der geografisk er placeret i nærheden af et område på 3 gange 3 km, hvor der vil skulle foretages målrettet geografisk registrering og opbevaring, vil derfor også, pga. disse tekniske forhold, i et større eller mindre omfang kunne blive omfattet af den registrering og opbevaring, udbyderne iværksætter – afhængig af antallet af masterne og deres placering. Det forudsættes i den forbindelse, at udbyderne iværksætter registreringen og opbevaringen af trafikdata, så registreringen alene omfatter det område, der er strengt nødvendigt. Det påhviler i den forbindelse udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at udpege de fornødne master, således at det angivne område dækkes fuldstændigt. Det forudsættes i den forbindelse, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, ved udpegningen af de fornødne master tager højde for bygningsmassen og andre forhold, der typisk vil kunne forårsage såkaldte mastespring. Det vil bl.a. indebære, at det typisk vil være nødvendigt at medtage master uden for området på 3 km gange 3 km, da telefoner vil være mere tilbøjelige til at springe på master, der er placeret længere væk, såfremt disse er mindre belastede af trafikdata end de master, der befinder sig tættest ved telefonen. Er dette tilfældet, vil de oplysninger, der registreres og opbevares, være omfattet af den målrettede geografiske registrering og opbevaring. Det betyder, at politiet og anklagemyndigheden vil kunne få adgang til disse trafikdata, og at disse oplysninger på samme vis som øvrige oplysninger, der registreres og opbevares som følge af en af de foreslåede registrerings- og opbevaringspligter, kan anvendes i efterforskninger og som bevis i straffesager. Det skal ses i lyset af, at det ikke er muligt at frasortere data inden for de enkelte cellers rækkevidde, som stammer fra telefoner, der reelt har befundet sig uden for de udpegede områder.

Den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata og den foreslåede ordning med målrettet geografisk registrering og opbevaring af trafikdata for så vidt angår det foreslåede § 786

c, stk. 1, nr. 2, (områder med en overhyppighed af beboere dømt for grov kriminalitet), vil kræve udvikling af it-systemunderstøttelse hos bl.a. Rigspolitiet med henblik på en automatiseret proces.

Der vil være behov for at foretage en grundig foranalyse forud for selve systemudviklingen til understøttelse af den foreslåede målrettede registrering og opbevaring, idet der vil være tale om et komplekst it-projekt. It-systemudviklingen vil bl.a. skulle bygge oven på it-systemer fra flere forskellige myndigheder (herunder politiet og kriminalforsorgen) og telebranchen. Foranalysen ventes tidligst at foreligge i 2023. Herefter vil Rigspolitiet kunne levere et skøn over, hvornår it-systemunderstøttelsen vil kunne ventes etableret og sat i drift. Det forudsættes, at udviklingsarbejdet sker under dialog med telebranchen, således at det sikres, at den kommende it-systemunderstøttelse i Rigspolitiet er kompatibel med den it-systemunderstøttelse, ordningen forudsætter for så vidt angår udbyderne, som med et kommercielt formål udbyder elektroniske kommunikationsnet og –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden.

Da en sådan it-systemunderstøttelse ikke vil kunne være færdigudviklet på tidspunktet for lovens ikrafttrædelse, foreslås det, at justitsministeren i en overgangsperiode – dvs. perioden fra lovens ikrafttræden og indtil det tidspunkt, hvor Rigspolitiets it-løsning m.v. er etableret og klar til at blive sat i drift – vil kunne fastsætte nærmere regler om registrering og opbevaring af trafikdata for så vidt angår den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata. Det forudsættes, at bemyndigelsen udnyttes til at fastsætte regler om bl.a. politiets adgang til at pålægge registrering og opbevaring af trafikdata baseret på politiets konkrete anmodninger. Der lægges i den forbindelse ikke op til at bemyndige justitsministeren til at fastsætte andre betingelser for den målrettede registrering og opbevaring af trafikdata end dem, som fremgår af de foreslåede §§ 786 b og 786 d i retsplejeloven.

Det bemærkes, at udmøntningen af de foreslåede regler om målrettet personbestemt og geografisk registrering og opbevaring vil være forbundet med en risiko for eventuelle fejl enten i form af, at der registreres og opbevares oplysninger om personer eller områder, der ikke er omfattet af den foreslåede ordning, eller i form af, at der ikke registreres oplysninger for alle personer eller områder, der er omfattet af ordningen. Det skyldes bl.a., at

udmøntningen vil være afhængig af en række ældre it-systemer og overbygninger herpå. Der vil også være risiko for fejl i overgangsperioden, hvor der vil være tale om at udmønte reglerne i en manuel løsning.

For så vidt angår domstolsprøvelse foreslås det, at der for registrering og opbevaring af trafikdata på grundlag af konkret begrundede pålæg, jf. den foreslåede § 786 d i retsplejeloven, indføres en ordning med forudgående retskendelse svarende til, hvad der kendes i dag for indgreb i meddelelshemmeligheden.

For målrettet personbestemt og geografisk registrering og opbevaring af trafikdata, der ikke iværksættes på grundlag af konkret begrundede pålæg men automatisk, jf. de foreslåede bestemmelser i retsplejelovens §§ 786 b og 786 c, vil der som i dag være adgang til domstolsprøvelse, jf. grundlovens § 63.

Vedrørende domstolsprøvelse henvises i øvrigt til pkt. 3.6.

3.2. Generel og udifferentieret registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed

3.2.1. Gældende ret

Der henvises til beskrivelsen ovenfor under pkt. 3.1.1 vedrørende retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen. Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786, stk. 4, for teleudbydere til at registrere og opbevare oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold ikke skelner mellem de forskellige kriminalitetsformer. Der er derfor efter gældende ret ikke særlige regler for registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed eller bekæmpelse af grov kriminalitet.

3.2.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder La Quadrature du Net-dommen af 6. oktober 2020, er beskrevet under pkt. 2.

La Quadrature du Net-dommen nødvendiggør en ændring af retsplejelovens § 786, stk. 4, således at ordningen er i fuld overensstemmelse med EU-retten som fortolket af EU-Domstolen.

For så vidt angår registrering og opbevaring med henblik på beskyttelse af den nationale sikkerhed er de relevante dele af La Quadrature du Net-dommen præmis 134-139. Det fremgår heraf navnlig,

- at der kan fastsættes nationale regler, der foreskriver generel og udifferentieret lagring 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, som må anses for at være reel og aktuel eller forudsigelig,
- 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 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 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.

3.2.3. Justitsministeriets overvejelser og den foreslåede ordning

3.2.3.1. Alvorlig trussel mod Danmarks nationale sikkerhed

Det er Justitsministeriets opfattelse, at oplysninger om antallet og karakteren af verserende eller afgjorte straffesager om overtrædelse af straffelovens kapitel 12 og 13 kan indgå som et af flere elementer i vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig.

Det vil således indgå som et væsentligt moment ved vurderingen, om der er foretaget sigtelser, sket varetægtsfængsling eller rejst tiltale for forhold omfattet af straffelovens kapitel 12 og 13, ligesom domfældelser, hvorved der er dømt for overtrædelse af de bestemmelser, der hører under straffelovens kapitel 12 eller 13, vil kunne tillægges betydelig vægt ved vurderingen.

Et andet element, som kan indgå i vurderingen af, om der foreligger en trussel mod den nationale sikkerhed, er ”Vurderingen af Terrortruslen mod Danmark” (VTD), som årligt udarbejdes af Center for Terroranalyse (CTA). VTD’en er CTA’s samlede vurdering af terrortruslen mod Danmark og danske interesser i udlandet. Vurderingen 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.

VTD’en indeholder en samlet 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 til og/eller intention om at begå et terrorangreb, og om planlægning af et terrorangreb i det kommende år er sandsynlig.

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.

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.
Minimal	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt.

Seneste VTD blev udgivet den 31. marts 2021. Det fremgår heraf, at CTA vurderer, at terrortruslen mod Danmark er alvorlig. Det fremgår af tidligere vurderinger af terrortruslen, at CTA også tidligere har vurderet, at truslen mod Danmark er alvorlig, jf. CTA's vurderinger i årene fra 2014-2020. Siden 2014 har CTA brugt terrortrusselsniveauerne og definitionerne gengivet ovenfor i figur 1, herunder begrebet "alvorlig", som en indikation på et specifikt defineret trusselsniveau, dog således, at det laveste terrortrusselsniveau indtil seneste VTD udgivet den 31. marts 2021, var benævnt "ingen", mens det nu benævnes "minimal". Definitionen for niveauet er imidlertid fortsat den samme.

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 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 krænkelse 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.

Justitsministeriet vurderer på den baggrund, at VTD'en kan indgå som et af flere elementer i vurderingen af, hvorvidt der foreligger en alvorlig trussel mod den nationale sikkerhed, der er reel og aktuel eller forudsigelig.

Justitsministeriet har desuden lagt vægt på, at VTD'en er tilstrækkelig dynamisk i karakter til, at vurderingen af, om der er en alvorlig trussel mod den nationale sikkerhed, ikke ved inddragelse heraf vil få en systematisk karakter. Der henvises til, at der tidligere har været perioder, hvor truslen mod Danmark har været vurderet anderledes af CTA, end det er tilfældet i dag. Hertil kommer, 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 høje niveau ("alvorlig").

Ud over dokumentation vedrørende antallet og karakteren af verserende eller afgjorte straffesager om overtrædelse af straffelovens kapitel 12 og 13 og VTD'en kan også en række andre uklassificerede analyseprodukter udgivet af Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste eller Center for Cybersikkerhed indgå i vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed. Det kunne f.eks. være Center for Cybersikkerheds årlige "Trusselsvurdering 2020: Cybertruslen mod Danmark", men også andre relevante trusselsvurderinger vil kunne indgå.

Vurderingen af, om der foreligger en alvorlig trussel mod den nationale sikkerhed vil skulle 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 på baggrund af en gennemgang af aktuelle straffesager omhandlende overtrædelser af bestemmelserne i straffelovens kapitel 12 og 13, herunder både verserende sager og sager, hvori der er sket domfældelse, samt på baggrund af VTD'en 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, 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.

Det foreslås på den baggrund, at justitsministeren bemyndiges til efter forhandling med erhvervsministeren at fastsætte regler om, at det påhviler udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

Det foreslås, at udtrykket ”udbydere af elektroniske kommunikationsnet eller -tjenester forstås i overensstemmelse med samme udtryk i logningsbekendtgørelsen. Der henvises til pkt. 3.1.1.2.

Hvis de omfattede oplysninger kan registreres af flere udbydere, skal oplysningerne registreres og opbevares af mindst én af udbyderne.

3.2.3.2. Tidsmæssig udstrækning m.v.

Justitsministeriet har overvejet, hvordan det kan sikres, at den generelle og udifferentierede registrering og opbevaring af trafikdata tidsmæssigt begrænses til det strengt nødvendige, således at registreringen og opbevaringen ikke får en systematisk karakter.

Det er Justitsministeriets vurdering, at en tidsmæssig udstrækning for generel og udifferentieret registrering og opbevaring på op til 1 år fra udstedelsen af en bekendtgørelse herom vil være proportional i de tilfælde, hvor det antages, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed som beskrevet ovenfor.

Det foreslås på den baggrund, at udbydere af elektroniske kommunikationsnet eller -tjenesters registreringspligt højst vil kunne fastsættes for en periode på 1 år ad gangen. Den tidsmæssige udstrækning skal begrænses til det strengt nødvendige, og udstrækningen kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt. Det forudsættes også, at fastsatte regler ophæves, hvis der opstår grundlag for at antage, at de ikke længere kan opretholdes. Det forudsættes også, at udbyderne af elektroniske kommunikationsnet eller -tjenester med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet personbestemt og geografisk registrering og opbevaring.

Det foreslås i forlængelse heraf, at oplysninger, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, vil skulle opbevares i 1 år fra registreringstidspunktet, også efter overgangen til målrettet registrering og opbevaring. Det skal ses i lyset af, at oplysninger, der er registreret og opbevaret som følge af en gældende pligt til generel og udifferentieret registrering og opbevaring, vil være registreret på lovligt grundlag, og at sådanne oplysninger derfor vil kunne opbevares i 1 år efter selve registreringen med henblik på efterforskning og retsforfølgning af grov kriminalitet. Det bemærkes, at det vil være et krav for, at politiet og anklagemyndigheden kan få adgang til sådanne oplysninger, at det sker med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed. Oplysninger registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, der er indhentet af politiet og anklagemyndigheden inden opbevaringsperioden for de pågældende oplysninger er udløbet, vil også efter udløbet af opbevaringsperioden kunne anvendes i efterforskningen og som bevis i straffesager.

Gyldigheden af regler udstedt i medfør af bemyndigelsen kan prøves, jf. grundlovens § 63. Det forudsættes, at grundlaget for vurderingen af, at der foreligger en alvorlig trussel mod Danmarks nationale sikkerhed, der nødvendiggør fastsættelse af regler om generel og udifferentieret registrering og opbevaring af trafikdata, offentliggøres ved udstedelsen af reglerne. Vedrørende domstolsprøvelsen henvises i øvrigt til pkt. 3.6.

3.2.3.3. Omfang af oplysninger og kommunikationsmidler

Det foreslås, at registrerings- og opbevaringspligten vil skulle omfatte de data, der er registrerings- og opbevaringspligtige i dag. Der henvises til pkt. 3.1.3.4.

3.3. Registrering og opbevaring af oplysninger om en brugers adgang til internettet

3.3.1 Gældende ret

Der henvises til beskrivelsen ovenfor under pkt. 3.1.1 vedrørende retsplejelovens § 786, stk. 4, og logningsbekendtgørelsen.

Efter logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, skal en udbyder af elektroniske kommunikationsnet eller -tjenester registrere oplysninger om en brugers adgang til internettet, herunder den tildelte brugeridentitet (nr. 1), den brugeridentitet og det tele-

fonnummer, som er tildelt kommunika-tioner, der indgår i et offentligt elektronisk kommunikationsnet (nr. 2), navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse (herefter IP-adresse), en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet (nr. 3) og tidspunktet for kommunikationens start og afslutning (nr. 4).

Begrebet ”brugeridentitet” skal ikke forstås indskrænkende, hvilket kan udledes af vejledning nr. 74 af 28. september 2006 til logningsbekendtgørelsen, der beskriver begrebet. Med tildelt brugeridentitet, jf. § 5, stk. 1, nr. 1, vil normalt forstås den tildelte internetprotokol-adresse (IP-adresse), en slutbruger gør brug af ved anvendelse af internettet. Begrebet omfatter herudover også andre oplysninger, der identificerer en slutbruger over for udbyderen. Det vil f.eks. være kundenummer, abonnementsnummer eller andre oplysninger. I praksis vil brugeridentiteten både omfatte den tildelte IP-adresse og evt. portnummer.

Med den brugeridentitet og det telefonnummer, som er tildelt kommunika-tioner, der indgår i et offentligt elektronisk kommunikationsnet, jf. § 5, stk. 1, nr. 2, fremgår det af vejledningen, at bestemmelsen f.eks. sigter på situationer, hvor en slutbruger tildeles en IP-adresse til brug ved den pågældende session og herefter ringer til en anden bruger via det offentlige elektroniske kommunikationsnet. I den forbindelse tildeles slutbrugeren et telefonnummer eller et andet identifikationsnummer. Udbyderne af elektroniske kommunikationsnet eller -tjenester skal i sådanne situationer registrere oplysninger om de til slutbrugeren tildelte identiteter, numre og IP-adresser. Der er derfor et overlap for så vidt angår brugeridentitet.

Det fremgår af logningsbekendtgørelsens § 5, stk. 2, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, der udbyder trådløs adgang til internettet, endvidere skal registrere oplysninger om det lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr.

Det fremgår af vejledningen til logningsbekendtgørelsen, at § 5, stk. 2, medfører, at oplysninger om et hot spots præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr skal registreres. Det betyder, at en udbyder af internetadgang via et hot spot skal

registrere oplysninger om en slutbrugers adgang til internettet, og at udbyderen samtidig skal registrere oplysninger om, hvor det pågældende hot spot geografisk er placeret.

Ved trådløs adgang til internettet (hot spots) forstås f.eks. netværk, der giver slutbrugere trådløs adgang til internettet på offentlige steder, eksempelvis banegårde og lufthavne. Der etableres som oftest trådløs adgang for slutbrugeren til internettet på baggrund af identiteten på det benyttede kommunikationsudstyr – f.eks. i form af en MAC-adresse – og et kundenummer. Udbyderen af trådløs adgang til internettet skal registrere oplysninger om identiteten på det benyttede kommunikationsudstyr, en slutbruger anvender i forbindelse med tilkobling til routeren, samt den IP-adresse den pågældende slutbruger blev tildelt som led i kommunikationen.

Udlevering af oplysninger om en slutbrugers adgang til internettet, jf. logningsbekendtgørelsens § 5, udleveres efter retsplejelovens regler om edition henholdsvis telelovens § 13, jf. pkt. 3.7.1.

3.3.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder La Quadrature du Net-dommen af 6. oktober 2020, er beskrevet under pkt. 2.

For så vidt angår registrering og opbevaring af IP-adresser er de relevante dele af dommen præmis 152-156. Det fremgår heraf bl.a.,

- at der kan fastsættes lovgivningsmæssige foranstaltninger, der foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, såfremt det kan begrundes af hensyn til bekæmpelsen af grov kriminalitet, herunder forebyggelsen af alvorlige trusler mod den offentlige sikkerhed og beskyttelsen af den nationale sikkerhed, og at det desuden er en forudsætning, at denne mulighed er betinget af en streng overholdelse af de materielle og proceduremæssige betingelser, der skal gælde for brugen af disse data,
- at lagringsperioden 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.

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

- at data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, principielt ikke kan kvalificeres som et alvorligt indgreb i grundlæggende rettigheder, og at lagring 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 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 lagring.

3.3.3. Justitsministeriets overvejelser og den foreslåede ordning

Politiet har behov for at kunne afdække, hvilke slutbrugere der benytter bestemte IP-adresser på givne tidspunkter, idet sådanne oplysninger er helt afgørende i forbindelse med efterforskningen af en lang række sager. 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 kriminalitet begået online, f.eks. hacking, digitale sexkrænkelser og distribution af materiale om seksuelt misbrug af mindreårige m.v., tilsiger generelt, at politiets behov for entydigt og effektivt at kunne fastlægge identiteten på en slutbruger af en given IP-adresse fortsat vil have en central betydning.

Det fremgår af EU-Domstolens præmis 152 i La Quadrature du Net-dommen, at IP-adresser genereres uden at være knyttet til en bestemt kommunikation og hovedsageligt tjener til – gennem udbyderen – at identificere den fysiske person, der ejer det terminaludstyr, hvorfra en kommunikation via internettet foretages. For så vidt det kun er IP-adresserne på kilden til kommunikationen og ikke IP-adresserne på modtageren af kommunikationen, der registreres og opbevares, afslører IP-adresser ikke som sådan nogen oplysninger om de tredjemænd, der har været i kontakt med personen, der har foretaget kommunikationen. EU-Domstolen anfører derfor, at denne kategori af data er mindre følsomme end andre former for trafikdata.

Det fremgår derimod af præmis 153, at eftersom IP-adresser kan anvendes til bl.a. at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter, gør disse oplysninger det imidlertid muligt at skabe en detaljeret profil af denne internetbruger. Den lagring og analyse af de nævnte IP-adresser, som en sådan sporing kræver, udgør således alvorlige indgreb i internetbrugerens grundlæggende rettigheder, som er sikrede ved chartrets artikel 7 og 8.

I præmis 154 i omtales i forbindelse med spørgsmålet om registrering og opbevaring af IP-adresser, at IP-adressen, hvorfra en lovovertrædelse er begået på internettet, kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som var tildelt denne adresse på det tidspunkt, hvor den pågældende overtrædelse blev begået. Det anføres videre, at dette bl.a. kan »være tilfældet for særligt alvorlige lovovertrædelser på området for børnepornografi, såsom erhvervelse, udbredelse, transmission eller tilrådighedsstillelse på internettet 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 (...)«.

Det fremgår herudover af præmis 156, at henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som denne lagring indebærer, er det kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der i lighed med beskyttelsen af den nationale sikkerhed kan begrunde dette indgreb. Lagringsperioden må endvidere ikke overstige, hvad der er strengt nødvendigt for at nå det forfulgte formål. Endelig skal en foranstaltning af denne art 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.

Det fremgår derefter af præmis 157-159 om civile identitetsoplysninger, at hvad angår de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, gør disse data det ikke i sig selv muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode, hvilket 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. Det indgreb, som en lagring af disse data indebærer, kan således principielt ikke kvalificeres som alvorligt. Registrering og opbevaring af 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, hvortil artikel 15, stk. 1, første punktum, i direktiv 2002/58 henviser.

Justitsministeriet bemærker på den baggrund, at begrebet 'IP-adresser' ikke er entydigt defineret af EU-Domstolen.

Som det fremgår af præmis 152, fremhæver Domstolen, at det er definerende for IP-adresser, at de kan identificere den fysiske person, der ejer terminaludstyr, hvorfra en kommunikation via internettet foretages. En sådan definition af IP-adresser er bred, da den omfatter alle de sammenhænge, hvor IP-adresser anvendes.

I den efterfølgende præmis 153 fremhæver Domstolen derimod, at IP-adresser bl.a. kan bruges til at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter.

En sporing som beskrevet i præmis 153 vil efter Justitsministeriets opfattelse kræve registrering og opbevaring af sessioner (sessionslogging, som blev afskaffet i Danmark ved ikrafttræden af bekendtgørelse nr. 660 af 19. juni 2014 om ændring af bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)). Ved sessionslogging forstås den situation, hvor en slutbruger sender eller modtager data på internettet, og en udbyder registrerer oplysninger om internet-sessionens initierende og afsluttende pakke, herunder oplysninger om afsendende og modtagende IP-adresse, afsendende og modtagende portnummer samt transportprotokol, hver gang en slutbruger tilgår f.eks. en server eller kommunikerer direkte over internettet med en anden slutbruger.

Ovenstående umiddelbart modstridende præmisser skal endvidere ses i sammenhæng med præmis 157-159 om civile identitetsoplysninger. Det skyldes, at de data, som udgør IP-adresser, der ikke er omfattet af registrering og opbevaring af sessioner, som beskrevet i præmis 153, vil opfylde definitionen i præmis 157. Det skyldes, at disse IP-adresser m.v. alene vedrører

identiteten på brugerne af elektroniske kommunikationsmidler, og at disse data ikke i sig selv gør det muligt at få kendskab til datoen og tidspunktet for samt varigheden og modtagerne af den kommunikation, der er foretaget, og heller ikke de steder, hvorfra denne kommunikation har fundet sted, eller oplysning om, hvor ofte denne kommunikation har været foretaget med visse personer i en bestemt periode, hvilket 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.

Det er derfor Justitsministeriets opfattelse, at det er uklart, hvorvidt EU-Domstolens præmis 152-156 i La Quadrature du Net-dommen omfatter registrering og opbevaring af IP-adresser helt generelt, eller kun i tilfælde, hvor der er tale om registrering og opbevaring af sessioner, som beskrevet i præmis 153.

Da behovet for entydigt og effektivt at kunne fastlægge identiteten på en slutbruger af en given IP-adresse fortsat vil have en central betydning for politiets efterforskning, og da disse oplysninger ikke tilvejebringer nogen form for oplysninger om den foretagne kommunikation og dermed om en persons privatliv, er det Justitsministeriets vurdering, at EU-Domstolens præmis 152-156 alene angår IP-adresser i forbindelse med registrering og opbevaring af sessioner. Registrering og opbevaring af IP-adresser, der alene opfylder beskrivelsen i EU-Domstolens præmis 157, kan derfor opbevares og anvendes til brug for efterforskning af almindelig kriminalitet.

Det er på den baggrund Justitsministeriets vurdering, at de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 1, der foreskriver, at udbydere af elektroniske kommunikationsnet eller -tjenester skal foretage generel og udifferentieret registrering af oplysninger om en slutbrugers adgang til internettet (herunder IP-adresser), er i overensstemmelse med La Quadrature du Net-dommen. Det skyldes, at de danske regler ikke omfatter registrering og opbevaring af sessioner, men alene registrering og opbevaring af identitetsoplysninger på slutbrugerens adgang til internettet. Det bemærkes, at såfremt der indføres regler om registrering og opbevaring af sessioner, som beskrevet i præmis 153, vil disse regler kun være i overensstemmelse med La Quadrature du Net-dommen, hvis de opfylder præmis 152-156. Efter Justitsministeriets opfattelse kan disse præmisser b.la. kun efterleves derved, at adgang til sådanne oplysninger betinges af, at udleveringen sker med henblik på bekæmpelse af grov kriminalitet.

Udlevering af oplysninger om en brugers adgang til internettet efter logningsbekendtgørelsens § 5, sker i dag efter retsplejelovens regler om edition. Det er Justitsministeriets vurdering, at dette vil være i overensstemmelse med EU-Domstolens praksis, herunder La Quadrature du Net-dommen.

Det er desuden Justitsministeriets vurdering, at en opbevaringsperiode på 1 år kan anses for begrænset til det, der er strengt nødvendigt for at nå det forfulgte formål, og derfor er i overensstemmelse med EU-Domstolens krav i La Quadrature du Net-dommen. Det skyldes for det første, at sager om kriminalitet på internettet ofte er komplekse og derfor tager lang tid at efterforske, bl.a. fordi der ofte er en international dimension, som f.eks. kan nødvendiggøre kontakt til udenlandske selskaber eller myndigheder, før indhentning af oplysninger om IP-adresse kan søges indhentet fra en dansk udbyder af elektroniske kommunikationsnet eller -tjenester. Det skyldes for det andet, at der i sager om organiseret kriminalitet kan være behov for opbevaring og registrering af brugeridentiteter over længere tid, idet disse sagstyper ofte involverer en større mængde kommunikationsenheder, som computere og mobiltelefoner, som skal beslaglægges og undersøges med henblik på IT-tekniske spor, såsom IP-adresser på bagmænd.

Det er Justitsministeriets vurdering, at de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 2, der foreskriver, at ud over internetoplysninger, der skal registreres efter § 5, stk. 1, skal oplysninger om et hot spots præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr registreres, ikke er i overensstemmelse med La Quadrature du Net-dommens præmis 157-159. Derfor omfatter den foreslåede ordning ikke en videreførelse af de nugældende danske regler i logningsbekendtgørelsens § 5, stk. 2.

Det er endelig Justitsministeriets opfattelse, at det, bl.a. på baggrund af den teknologiske udvikling, er nødvendigt med en præcisering af de nugældende regler om adgang til oplysninger om en slutbrugers adgang til internettet (herunder IP-adresser), således at det er klart, hvad der skal registreres og opbevares, og hvad der kan gives adgang til.

For entydig identifikation af slutbrugerens adgang til internettet er det nødvendigt, at der foruden registrering og opbevaring af selve den IP-adresse, der er anvendt ved adgangen til internettet, også vil kunne ske registrering

og opbevaring af det såkaldte portnummer ("source port number"), som udbydere af elektroniske kommunikationsnet eller -tjenester m.v. tildeler slutbrugeren for at identificere trafikken til og fra den enkelte slutbruger samt andre identificerende oplysninger, som udbydere af elektroniske kommunikationsnet eller -tjenester tildeler slutbrugeren ved adgang til internettet. Det skyldes, at et større antal brugere typisk anvender den samme IP-adresse samtidig, hvorfor en IP-adresse alene således ikke kan tjene til at identificere den fysiske person, der kommunikerer via internettet. Portnummeret er derfor, sammen med IP-adressen og tidspunktet, der behandles nedenfor, afgørende for at kunne fastlægge identitet på en slutbrugers adgang til internettet. Andre identificerende oplysninger vil på samme måde være nødvendige at registrere og opbevare, for at brugeren entydigt kan identificeres. Det er f.eks. tilfældet, hvor udbydere af elektroniske kommunikationsnet eller -tjenester anvender Carrier-grade Network Address Translation (NAT), hvor udbyderen forener endnu flere brugeres adgang til internettet på endnu færre IP-adresser.

Endvidere vil der også skulle ske registrering og opbevaring af oplysninger om det tidspunkt, hvor en slutbruger blev tildelt en given IP-adresse, portnummer eller andre identificerende oplysninger, som udbydere af elektroniske kommunikationsnet eller -tjenester tildeler slutbrugeren ved adgang til internettet. Det skyldes, at flere slutbrugere kan anvende de samme IP-adresser, portnumre og evt. andre identificerende oplysninger, men aldrig på samme tidspunkt. Derfor forudsætter en entydig identifikation af slutbrugeren og registrering af de tidspunkter, hvor en slutbruger tildeles en given IP-adresse, portnummer eller andre identificerende oplysninger. Tidspunktet bliver derfor sammen med IP-adressen, portnummeret og evt. andre identificerende oplysninger afgørende for at kunne fastlægge identitet på en slutbrugers adgang til internettet.

Retsplejelovens § 786, stk. 4, som logningsbekendtgørelsens § 5, stk. 1, er udstedt i medfør af, foreslås ophævet. Det vil derfor være nødvendigt at indføre en hjemmel i retsplejeloven for fortsat at kunne registrere og opbevare oplysninger om en slutbrugers adgang til internettet.

Der foreslås derfor indført en forpligtelse i retsplejeloven, hvorefter udbydere af elektroniske kommunikationsnet eller -tjenester skal foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet.

Det foreslås, at udtrykket ”udbydere af elektroniske kommunikationsnet eller -tjenester” forstås i overensstemmelse med samme udtryk i logningsbekendtgørelsen. Der henvises til pkt. 3.2.3.1.

Det foreslås endvidere, at de nærmere regler om sådan registrering og opbevaring kan fastsættes ved bekendtgørelse. En sådan bekendtgørelse kan omfatte nærmere regler om, hvilke oplysninger udbydere af elektroniske kommunikationsnet eller -tjenester skal registrere, for at slutbrugeren entydigt kan identificeres. Det kan bl.a. være regler om registrering af brugeridentiteter, herunder IP-adresse, portnummer og andre identificerende oplysninger, som udbydere af elektroniske kommunikationsnet eller -tjenester tildeler slutbrugeren ved adgang til internettet, samt regler om registrering af tidspunktet for tildelingen af brugeridentitet. Endvidere vil der kunne fastsættes regler om identifikation af abonnenten over for udbyderen, f.eks. telefonnummer eller anden identifikationsnummer, samt navn og adresse på abonnenten og den forventede bruger. Det forudsættes, at bestemmelserne gøres teknologineutrale og klare.

Det foreslås, at oplysninger registreret efter den foreslåede pligt til generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet skal opbevares 1 år.

3.4. Registrering og verificering af nummeroplysningsdata

3.4.1 Gældende ret

Det følger af bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, som er udstedt i medfør af § 31, stk. 3, i lov nr. 128 om elektroniske kommunikationsnet og -tjenester af 7. februar 2014 (teleloven) med senere ændringer, at datasælgeren bl.a. skal indsamle og registrere nummeroplysningsdata. Nummeroplysningsdata, som datasælgeren skal indsamle og registrere, er specificeret i bekendtgørelsens bilag 1.

Ved en datasælger forstås en udbyder af elektroniske kommunikationsnet eller -tjenester, der videretildeler 8-cifrede abonnentnumre til slutbrugere, jf. § 2, stk. 2, i bekendtgørelsen om nummeroplysningsdatabaser.

Nummeroplysningsdata er i § 31, stk. 2, i teleloven defineret som abonnentnumre, der er tildelt slutbrugere, indeholdende navn, adresse, eventuelle oplysninger om stilling, abonnentnummeret og den kategori af tjeneste, abonnentnummeret anvendes til.

Bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser fastsætter ikke krav om verificering af de nummeroplysningsdata, som indsamles og registreres.

3.4.2. Justitsministeriets overvejelser og den foreslåede ordning

Med indførelsen af en ordning om målrettet personbestemt registrering og opbevaring af trafikdata vil det efter Justitsministeriets opfattelse være afgørende, at der i videst muligt omfang kan ske en entydig identifikation af brugeren af et givet kommunikationsmiddel. Dels for i videst mulig omfang at undgå, at der sker uforvarende registrering og opbevaring af forkerte personers trafikdata, dels for så vidt muligt at sikre, at der af hensyn til bekæmpelse af grov kriminalitet også kan findes frem til de personer, der efter loven kan iværksættes registrering og opbevaring på.

Efter gældende ret er der ikke krav om, at udbydere af elektroniske kommunikationsnet eller -tjenester verificerer oplysningerne, som de indsamler og registrerer efter bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, jf. pkt. 3.4.1.

Det foreslås derfor, at der fastsættes en bemyndigelse for justitsministeren til, efter forhandling med klima-, energi- og forsyningsministeren, at kunne udstede regler om registrering og verificering, hvorved udbydere af elektroniske kommunikationsnet eller -tjenester vil kunne blive pålagt at verificere nummeroplysningsdata, som registreres og opbevares til brug for nummeroplysningsdatabasen, særligt med det formål, at 118-databasen, som politiet har adgang til, opnår en datakvalitet, der kan understøtte målrettet personbestemt registrering og opbevaring af trafikdata.

Det foreslås, at udtrykket ”udbydere af elektroniske kommunikationsnet eller -tjenester” forstås i overensstemmelse med samme udtryk i logningsbekendtgørelsen. Der henvises til pkt. 3.2.3.1.

Formålet med den foreslåede bemyndigelse vil således være, at der herigenom i bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser vil kunne fastsættes regler med nærmere krav til, hvornår og hvordan verificering skal ske, således at der opnås større sikkerhed for, at det er de korrekte oplysninger, der fremgår af 118-databasen.

Forslaget skal ses i sammenhæng med den foreslåede ændring af definitionen af nummeroplysningsdata i telelovens § 31, stk. 2, hvor det foreslås, at

der foretages en ændring af § 31, stk. 2, i teleloven, som indeholder definitionen af nummeroplysningsdata, således at nummeroplysningsdata, ud over de i forvejen angivne data, også omfatter unikt ID og eventuelle oplysninger om bruger. Der henvises til pkt. 3.8.

Med den foreslåede ændring af definitionen af nummeroplysningsdata og den foreslåede indførelse af mulighed for, at justitsministeren efter forhandling med klima-, energi- og forsyningsministeren kan fastsætte et registrerings- og verificeringskrav, lægges der op til, at udbydere af elektroniske kommunikationsnet eller -tjenester, ud over en indsamling og registrering af gældende nummeroplysningsdata, skal indsamle og registrere unikt ID og eventuelle oplysninger om bruger og herunder verificere slutbrugerens unikke ID. Endvidere foreslås det med ordningen, at udbydere af elektroniske kommunikationsnet eller -tjenester skal foretage en dokumentation af verificeringen, ligesom det foreslås, at slutbrugeren ikke må opnå adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget. Endeligt foreslås det, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter.

Der stilles med den foreslåede ordning ikke krav til, hvordan verificeringen skal foretages. Verificering vil eksempelvis kunne ske gennem en ny systemunderstøttet adgang til opslag i Det Centrale Personregister (CPR), hvorved det oplyste CPR-nummer kontrolleres i CPR-systemet for at verificere, at det af slutbrugeren oplyste er korrekt. Hvis slutbrugeren ikke har et CPR-nummer, kan verificeringen af de af slutbrugeren oplyste oplysninger i stedet ske ved, at slutbrugeren fremviser billedlegitimation i form af et pas eller nationalt civilt identitetskort. Udbyderen kan herved kontrollere, at passet eller det nationale identitetskort, hvor fødselsdato og hhv. pasnummer eller personnummer vil fremgå, sammen med billede-ID af slutbrugeren, stemmer overens med den person, som slutbrugeren til udbyderen oplyser at være. For personer med et CPR-nummer vil udbydere af elektroniske kommunikationsnet eller -tjenester også kunne kombinere et opslag i CPR med forevisning af billede-ID. Det afgørende er, at der foretages en verificering af slutbrugerens unikke ID. Erhvervskunder registreres med et CVR-nummer, som kan verificeres ved opslag i CVR-registeret (som er offentligt tilgængeligt). For erhvervskunder uden CVR-nummer kan verificeringen være opslag i det selskabsregister, erhvervskunden er registreret i. Det bemærkes, at den foreslåede ordning med verificering ikke kan ude-

lukke alle tilfælde, hvor en slutbruger forsætligt afgiver oplysninger til udbyderen af elektroniske kommunikationsnet eller -tjenester, der kan verificeres, men ikke er korrekte. F.eks. ved identitetstyveri, hvor andres personlige oplysninger bliver misbrugt ved, at en person bruger oplysningerne uberettiget i forbindelse med indsamling og registrering af nummeroplysningsdata.

Der stilles heller ikke med den foreslåede ordning krav til, hvordan udbyderne skal foretage dokumentation af verificeringen. Kravet vil eksempelvis kunne opfyldes ved, at udbyderen opbevarer en kopi af billedlegitimationen eller i deres system registrerer, at verificering er foretaget, og hvordan det er foretaget, således at dette fremgår i udbyderens system. Energistyrelsen vil i medfør af telelovens § 32 kunne føre tilsyn med, at udbyderne har dokumentation for at have foretaget verificering.

Endvidere foreslås det, at der fastsættes regler om, at udbyderne fremadrettet ikke må give slutbrugeren adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget. Dette for at sikre, at verificeringen foretages straks med indsamlingen og registreringen, da verificeringen er afgørende for, at de oplysninger, som videregives til forsyningspligtudbydernes landsdækkende nummeroplysningsdatabase (118-databasen), er korrekte og for at sikre, at det er muligt for politiet hurtigt at kunne iværksætte registrering og opbevaring af trafikdata for en person, som måtte være omfattet af personbestemt målrettet registrering og opbevaring, og som eksempelvis opretter et nyt abonnement.

Desuden foreslås det, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter omfattet af bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser. Det vil betyde, at uregistrerede taletidskort fremadrettet ikke vil kunne sælges. Det er Justitsministeriets opfattelse, at dette kan medvirke til at minimere den væsentlige omgåelsesrisiko, som brugen af uregistrerede taletidskort udgør, og som allerede i dag udnyttes af organiserede kriminelle m.v.

Det foreslås også, at der fastsættes overgangsbestemmelser, således at udbyderne kan nå at tilvejebringe den nødvendige systemunderstøttelse for verificering af kunder på tidspunktet for forpligtelsens indtrædelse.

Endeligt foreslås det, at udbyderne også skal indsamle og registrere unikt ID for alle eksisterende abonnenter. Derfor forudsættes det, at der fastsættes regler vedrørende en overgangsordning, således at udbyderne inden en nærmere bestemt periode skal have foretaget den fornødne registrering af eksisterende kunder. Det forudsættes dog, at disse regler ikke vil omfatte krav om indsamling og registrering af unikt ID på eksisterende abonnenter på fastnet- og IP-telefoni, hvor kravet alene forudsættes at være fremadrettet.

3.5. Hastesikring

3.5.1. 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 er at sikre, at politiet kan udstede pålæg om 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). Et pålæg om hastesikring omfatter dermed også oplysninger, der er registrerings- og opbevaringspligtige efter retsplejelovens § 786, stk. 4.

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. Det fremgår samme sted af bemærkningerne, at bestemmelsen indebærer, at politiet i de tilfælde, hvor der anvendes flere udbydere af telenet eller teletjenester, sættes i stand til at identificere og pålægge hver enkelt udbyder af telenet eller teletjenester at hastesikre data. Som eksempel kan nævnes tilfælde, hvor en person distribuerer børnepornografisk materiale ved hjælp af flere internetudbydere.

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. Der kan endvidere pålægge selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens kapitel 5.

De nærmere betingelser for, hvornår udbydere af elektroniske kommunikationsnet eller -tjenester skal udlevere oplysningerne til politiet, fremgår af retsplejelovens kapitel 71 og 74 om indgreb i meddelelshemmeligheden

og edition, jf. nærmere herom pkt. 3.7. En udlevering af de pågældende elektroniske data til politiet vil således skulle ske efter retsplejelovens § 781, stk. 1-3, for så vidt angår indholdsdata og trafikdata og § 804, stk. 1, for så vidt angår øvrige elektroniske data, f.eks. kundeoplysninger, jf. bemærkningerne til § 2, nr. 2, i lovforslag nr. L 55 som fremsat, jf. Folketingstidende 2003-04, tillæg A, s. 1827.

Det bemærkes, at den gældende forpligtelse efter retsplejelovens § 786 a for udbydere af elektroniske kommunikationsnet eller -tjenester 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, herunder beskyttelsen af den nationale sikkerhed.

3.5.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder La Quadrature du Net-dommen, er beskrevet under pkt. 2.

For så vidt angår hastesikring af elektronisk data er de relevante dele af La Quadrature du Net-dommen præmis 160-165. Det fremgår heraf bl.a.,

- at medlemsstaterne kan fastsætte national lovgivning, der muliggør, at der i konkrete tilfælde kan pålægges teleudbydere m.v. 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 teleudbydere m.v., 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 teleudbydere m.v. 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, hvis oplysninger kaster lys over forbrydelsen, såsom data vedrørende offeret eller den sociale eller professionelle omgangskreds, og

- at en sådan hurtig lagring udelukkende kan ske for at efterforske grov kriminalitet, herunder angreb mod den nationale sikkerhed, hvis de strafbare handlinger eller disse angreb allerede har kunnet konstateres, såvel som i den situation, hvor der efter en objektiv undersøgelse af samtlige relevante omstændigheder foreligger rimelig grund til at mistænke, at der er begået sådanne strafbare handlinger eller angreb.

3.5.3. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan en ordning med hastesikring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed, kan indrettes. Ved hastesikring forstås et indgreb, der pålægger udbyderne at sikre og opbevare data, som de råder over, som ellers ville være særligt udsat for at gå tabt eller blive ændret ("hurtig lagring" i La Quadrature du Net-dommen).

I den nuværende § 786 a, stk. 1, er alene "trafikdata" direkte nævnt. Det foreslås, at stk. 1 ændres, således at "trafikdata" ændres til "trafik- og lokaliseringsdata". Ændringen har ikke til formål at ændre på de data, der er omfattet af bestemmelsen. Der tilsigtes alene en tydeliggørelse af, at bestemmelsen også omhandler lokaliseringsdata, uanset om disse er omfattet af registrerings- og opbevaringspligten i medfør af § 786 b, 786 c, 786 d, eller 786 e.

Politiet vil skulle vurdere, hvilken tidsmæssig udstrækning pålægget skal have. Ved et pålægs tidsmæssige udstrækning forstås den periode, som udbyderne forpligtes til at opbevare de pågældende data i. Det fremgår af La Quadrature du Net-dommen, at varigheden af denne datalagring skal begrænses til det "strengt nødvendige". Det er Justitsministeriets opfattelse, at bestemmelsen i retsplejelovens § 786 a, stk. 2, allerede opfylder dette krav derved, at den stiller krav om, at perioden skal være "så kort som mulig".

Det fremgår desuden af dommen, at sikringsperioden gerne må forlænges, når det er begrundet i omstændighederne og det formål, der forfølges. Det foreslås derfor, at 4. pkt. i retsplejelovens § 786 a, stk. 2, om, at et pålæg ikke kan forlænges, skal udgå, således at et pålæg inden for de 90 dage kan forlænges. Samtidig foreslås det med et nyt 4. pkt. indført, at et pålæg efterfølgende kan opretholdes. Det er Justitsministeriets opfattelse, at dette ikke vil stride imod Europarådets konvention om IT-kriminalitet, artikel 16.

Justitsministeriet har herved lagt vægt på, at det allerede fremgår af konventionen, at parterne (medlemslandene) kan bestemme, at et sådant pålæg efterfølgende kan opretholdes. Pålægget vil således kunne opretholdes efter de 90 dage. Det vil i den forbindelse fortsat gøre sig gældende, at sikringsperioden skal være så kort som mulig og ikke kan overstige 90 dage ad gangen.

Politiets adgang til at pålægge hastesikring af trafik- og lokaliseringsdata, som udbyderne råder over, vil alene kunne anvendes, når det sker af hensyn til bekæmpelse af grov kriminalitet, herunder beskyttelsen af den nationale sikkerhed.

Det bemærkes i den forbindelse, at det følger af artikel 16, stk. 4, i Europarådets konvention om IT-kriminalitet (CETS nr. 185), at artikel 14 og 15 skal gælde for de beføjelser og procedurer, der er nævnt i artikel 16. Det følger endvidere af artikel 15, stk. 1, at enhver part skal sikre, at der for fastsættelse, gennemførelse og anvendelse af de pågældende beføjelser og procedurer gælder de efter partens nationale lovgivning gældende betingelser og retssikkerhedsgarantier, som på behørig vis skal sikre iagttagelse af menneskerettigheder og frihedsrettigheder, herunder rettigheder ifølge forpligtelser, som parten har påtaget sig i henhold til Europarådets konvention om beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder fra 1950, FN's konvention om borgerlige og politiske rettigheder fra 1966 samt andre gældende internationale menneskerettighedsdokumenter, og som skal inkorporere reglen om proportionalitet. Justitsministeriet har tidligere vurderet, at indsættelsen af et kriminalitetskrav ikke vil være foreneligt med artikel 16 i Europarådets konvention om IT-kriminalitet (CETS nr. 185). Det skyldes navnlig hensynet til, at pålæg om hastesikring skal være anvendeligt som et redskab allerede tidligt i efterforskningsfasen. Justitsministeriet forudsatte samtidig, at adgangen til at meddele pålæg om hastesikring ikke ville blive benyttet, hvis det på forhånd måtte stå klart for politiet, at oplysningerne ikke ville kunne udleveres som følge af, at betingelserne herfor i retsplejeloven ikke ville være opfyldt. Der henvises til pkt. 7.3.3 i de almindelige bemærkninger til lovforslag nr. L 55 af 5. november 2003, jf. Folketingstidende 2003-04, tillæg A, s. 1812 ff.

Det foreslås imidlertid, for at bringe bestemmelsen i overensstemmelse med EU-Domstolens nyeste praksis, at der i retsplejelovens § 786 a om hastesikring indføres et kriminalitetskrav, således at hastesikring af trafik- og loka-

liseringsdata kun må foretages, hvis efterforskningen angår grov kriminalitet, herunder beskyttelse af den nationale sikkerhed. Herefter vil et pålæg om hastesikring af trafik- og lokaliseringsdata kunne benyttes af hensyn til bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed, herunder hvor disse handlinger, eller forsøg herpå, allerede er konstateret, eller hvor der ud fra en objektiv vurdering af omstændighederne er en rimelig formodning om, at sådan grov kriminalitet eller handlinger er begået, forsøges eller planlægges. Det er dog ikke et krav, at oplysningerne vedrører personer, der konkret er mistænkt for at have begået grov kriminalitet, herunder et angreb mod den nationale sikkerhed, men oplysningerne skal på grundlag af objektive og ikke-diskriminerende forhold kunne bidrage til opklaringen af en sådan handling eller angreb mod den nationale sikkerhed, såsom 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 bemærkes, at § 786 a, stk. 1, som nævnt ovenfor også omfatter øvrige elektroniske data. Herved forstås også indholdsdata og kundeoplysninger. La Quadrature du Net-dommen omhandler for så vidt angår hastesikring de trafik- og lokaliseringsdata, som enten registreres og opbevares efter artikel 5, 6 og 9 i direktiv 2002/58, eller som registreres og opbevares på baggrund af en forpligtelse for teleudbyderne fastsat i medfør af artikel 15 i direktivet, jf. ovenfor.

Justitsministeriet har på den baggrund overvejet, om der i medfør af La Quadrature du Net-dommen også skal gælde et kriminalitetskrav for indholdsdata. Som ovenfor nævnt er bestemmelsen om hastesikring indsat i retsplejeloven på baggrund af Europarådets konvention om IT-kriminalitet (CETS nr. 185), som EU-Domstolen i La Quadrature du Net-dommen også henviser til (præmis 162). EU-Domstolen er dermed opmærksom på konventionen, herunder dens formål, men forholder sig alene til, at hastesikring af trafik- og lokaliseringsdata kun må ske til bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed. På den baggrund er det Justitsministeriets opfattelse, at det oprindelige formål med Europarådets konvention om IT-kriminalitet (CETS nr. 185) må stå ved magt, og der således ikke skal indføres et kriminalitetskrav for hastesikring af elektroniske data, herunder indholdsdata, bortset fra trafik- og lokaliseringsdata.

Efter Justitsministeriets opfattelse ændrer La Quadrature du Net-dommen ikke på, at bestemmelsen om hastesikring kan bruges til politiets efterforskning generelt, men der vil for trafik- og lokaliseringsdata skulle gælde et krav om, at hastesikring kun kan ske til brug for efterforskning af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed.

Hastesikring af trafik- og lokaliseringsdata vil kunne anvendes, når der er en rimelig formodning om, at der er begået eller vil blive begået grov kriminalitet m.v. Råder udbydere af elektroniske kommunikationsnet eller -tjenester konkret over data, der kan bidrage til opklaringen af grov kriminalitet m.v., vil disse således også kunne omfattes af et pålæg om hastesikring, uanset hvor gamle de er.

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.

Justitsministeriets finder på den baggrund, at der ikke ved pålæg om hastesikring bør stilles strenge krav til, i hvor høj grad disse hastesikrede oplysninger 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 forudgående godkendelse af, at der kan gives adgang hertil efter de øvrige regler i retsplejeloven. Eksempelvis vil det forhold, at der på et bestemt geografisk område er konstateret grov kriminalitet m.v. i sig selv være nok til, at der kan pålægges hastesikring af data med tilknytning til området.

Politiet vil endvidere også for at hastesikre trafik- og lokaliseringsdata indledningsvis skulle vurdere, om den pågældende sag konkret udgør grov kriminalitet m.v., herunder forsøg herpå, 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 grov kriminalitet m.v., f.eks. ved større ulykkestilfælde eller større uvarslede hændelser.

3.6. Domstolsprøvelse

3.6.1. Gældende ret

Der findes ikke i dag særlige regler om domstolsprøvelse af den registrering og opbevaring, der foretages efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf.

Domstolene kan imidlertid efter grundlovens § 63 prøve, om lovgivningens betingelser for registrering og opbevaring af de omfattede oplysninger er opfyldt, herunder også om dette er i overensstemmelse med EU-retten. Et sådant søgsmål kan anlægges i civilprocessens former.

Politiets adgang til de registrerede data sker efter retsplejelovens regler om indgreb i meddelelshemmeligheden eller om edition, afhængigt af hvilke oplysninger der er tale om. Disse regler er nærmere beskrevet i pkt. 3.7. Visse oplysninger kan politiet kræve udleveret efter telelovens § 13, der er nærmere beskrevet i pkt. 3.7.1.5.

3.6.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder La Quadrature du Net-dommen, er beskrevet under pkt. 2.

For så vidt angår domstolsprøvelse er de relevante dele af La Quadrature du Net-dommen præmis 139 og 163. Det fremgår heraf bl.a.,

- at henset til alvoren af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som følger af en generel og udifferentieret datalagringsforanstaltning, er det vigtigt at sikre, at anvendelsen af denne foranstaltning rent faktisk begrænses til de situationer, hvor der foreligger en alvorlig trussel mod den nationale sikkerhed, såsom de situationer, der er omhandlet i dommens præmis 135 og 136. Det er i denne henseende væsentligt, at en afgørelse, hvorved udbyderne af elektroniske kommunikationstjenester pålægges at foretage en sådan lagring af data, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og
- at for så vidt angår hastesikring står det, henset til den nødvendige afvejning af de omhandlede rettigheder og interesser, der er nævnt i dommens præmis 130, medlemsstaterne frit for at fastsætte muligheden for ved en afgørelse fra den kompetente myndighed, som er

underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som de råder over.

3.6.3. Justitsministeriets overvejelser og den foreslåede ordning

Det er Justitsministeriets vurdering, at den almindelige domstolsprøvelse af øvrighedsmyndighedens grænser, jf. grundlovens § 63, er tilstrækkelig effektiv i forhold til oplysninger, der registreres og opbevares generelt og udifferentieret, dvs. generel og udifferentieret registrering og opbevaring med henblik på beskyttelse mod en alvorlig trussel mod den nationale sikkerhed samt generel og udifferentieret registrering og opbevaring af IP-adresser, jf. nærmere pkt. 3.2 og 3.3. Det er desuden Justitsministeriets opfattelse, at tilsvarende gælder i forhold til oplysninger, der registreres og opbevares målrettet i medfør af klare og objektive kriterier, jf. nærmere pkt. 3.1.

Kendetegnende for den generelle og udifferentierede registrering og opbevaring, der er omtalt i pkt. 3.2 og 3.3 og de dele af den målrettede registrering og opbevaring, som ikke iværksættes på baggrund af konkret begrundede pålæg, der er beskrevet i pkt. 3.1, er, at der ikke skal foretages en vurdering af registreringen og opbevaringen af trafikdata i forhold til eksempelvis en konkret person eller et konkret område. Det vil med de foreslåede bestemmelser være objektivt konstaterbart, hvornår der kan foretages registrering og opbevaring af de pågældende oplysninger.

Det vil således være tydeligt, hvornår der sker en generel og udifferentieret registrering og opbevaring på baggrund af en alvorlig trussel mod den nationale sikkerhed, idet dette vil fastsættes ved bekendtgørelser. Det vil efter forslaget endvidere gælde, at udbyderne af elektroniske kommunikationsnet eller -tjenesters pligt til at registrere oplysninger generelt og udifferentieret fastsat i medfør af den foreslåede § 786 e, stk. 1, i retsplejeloven højst vil kunne fastsættes for en periode på 1 år ad gangen.

Herudover vil det være tydeligt, at der vil ske målrettet registrering og opbevaring af trafikdata for personer som er dømt for grov kriminalitet, eller som har været genstand for et af de omfattede indgreb i meddelelseshemmeligheden, idet der er fastsat objektivt konstaterbare og klare kriterier for iværksættelse af registrering og opbevaring af trafikdata for så vidt angår disse dele af den målrettede personbestemte ordning.

Det bemærkes i den forbindelse, at der ved behandlingen af en anmodning om aflytning eller teleoplysning vil være en indgrebsadvokat til stede, jf. retsplejelovens § 784. Der vil desuden som udgangspunkt skulle gives underretning om indgrebet til indehaveren af den pågældende telefon, jf. retsplejelovens § 788.

Det vil desuden være tydeligt, at der vil ske målrettet geografisk registrering og opbevaring i nærmere bestemte områder på 3 km gange 3 km, hvor antallet af anmeldelser om og beboere dømt for grov kriminalitet udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit de sidste 3 år. Det samme vil gælde for så vidt angår de særligt sikringskritiske områder. Der henvises dog til det under pkt. 3.1.3.2 anførte om såkaldte mastespring m.v.

Det er Justitsministeriets vurdering, at en prøvelse af, om de foreslåede ordninger er i overensstemmelse med bl.a. EU-retten, mest hensigtsmæssigt sker inden for de almindelige rammer for domstolenes kontrol med øvrighedsmyndighedens grænser, hvilket normalt vil være et civilt søgsmål anlagt mod den relevante myndighed – i dette tilfælde Justitsministeriet.

Ud fra samme betragtninger er det desuden Justitsministeriets opfattelse, at der for ordningerne med generel og udifferentieret registrering og opbevaring samt for de nævnte dele af ordningerne med målrettet registrering og opbevaring ikke vil være behov for at foretage underretning af de pågældende. Der henvises i den forbindelse til det ovenfor anførte om, at det – på baggrund af de objektive og klare kriterier, der foreslås fastsat i loven for disse ordninger – vil være almindeligt kendt, at der i de omfattede tilfælde vil foretages registrering og opbevaring af trafikdata.

Det er imidlertid Justitsministeriets opfattelse, at der bør være adgang til særlig domstolsprøvelse for de personer, hvis oplysninger gøres til genstand for målrettet registrering og opbevaring som følge af konkret begrundede pålæg om registrering og opbevaring, jf. pkt. 3.1. For denne del af ordningen gælder det, at den, hvis oplysninger gøres til genstand for registrering og opbevaring, ikke ud fra loven vil have mulighed for at vide, at registreringen og opbevaringen finder sted, og at de pågældende dermed ikke vil have mulighed for at få varetaget deres retlige interesser i registreringsperioden.

Det er på den baggrund Justitsministeriets vurdering, at den almindelige domstolskontrol med øvrighedsmyndighedens grænser ikke vil være en effektiv domstolsprøvelse af den registrering og opbevaring af trafikdata, der iværksættes på baggrund af, at politiet har grund til at antage, at en given

person eller et givet område har en forbindelse til grov kriminalitet. Justitsministeriet vurderer, at der i stedet bør indføres en domstolskontrol, der svarer til den, der kendes fra retsplejelovens regler om indgreb i meddelelshemmeligheden m.v.

Det er herudover Justitsministeriets vurdering, at der som i dag generelt bør være en domstolskontrol i forbindelse med, at politiet ønsker adgang til de registrerede og opbevarede oplysninger. Adgangen hertil vil efter forslaget – som i dag – skulle ske efter retsplejelovens regler om indgreb i meddelelshemmeligheden eller om edition afhængigt af, hvilke oplysninger der er tale om. Dog med den forskel, at det for så vidt angår oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, vil være en betingelse for at få adgang til sådanne oplysninger, at det sker med henblik på bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed. Der henvises til pkt. 3.7.

3.6.3.1. Domstolsprøvelse af ordningen med generel og udifferentieret registrering og opbevaring samt de dele af ordningen med målrettet registrering og opbevaring, der sker på baggrund af objektive og klare kriterier fastsat i loven

Der foreslås ikke indført særlige regler om domstolsprøvelse hverken for så vidt angår den generelle og udifferentierede registrering og opbevaring eller den målrettede registrering og opbevaring på baggrund af objektive og klare kriterier fastsat i loven. Kontrollen med denne registrering og opbevaring vil skulle ske efter den almindelige adgang til domstolsprøvelse, jf. grundlovens § 63.

Den almindelige domstolsprøvelse af øvrighedsmyndighedens grænser vil navnlig være relevant i forbindelse med en prøvelse af, om ordningen med generel og udifferentieret registrering og opbevaring med henblik på beskyttelse mod en alvorlig trussel mod den nationale sikkerhed er i overensstemmelse med bl.a. EU-retten.

Den almindelige domstolskontrol med øvrighedsmyndighedens grænser vil normalt finde sted som et civilt søgsmål anlagt mod den relevante myndighed. Det vil afhænge af de almindelige civilprocessuelle regler, om et søgsmål kan anlægges, herunder navnlig reglerne om partshabilitet og retlig interesse.

Det bemærkes i den forbindelse, at det forudsættes, at de bagvedliggende klassificerede oplysninger, der ligger til grund for VTD'en og andre relevante analyseprodukter, herunder oplysninger om visse verserende og afgjorte straffesager, ikke vil kunne kræves udleveret til brug for en retssag, jf. retsplejeloven § 41 d, stk. 5, nr. 2 og 6, samt retsplejelovens § 169, stk. 2, 3. pkt.

Det bemærkes i forlængelse heraf, at de bagvedliggende klassificerede oplysninger i øvrigt forudsættes at kunne undtages fra aktindsigt efter bl.a. offentlighedslovens § 31, i det omfang det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Herudover forudsættes det, at bagvedliggende oplysninger, herunder klassificerede oplysninger, om hvilke det gælder, at efterforskningshensyn tilsiger, at de ikke kan videregives, vil kunne undtages efter bl.a. offentlighedslovens § 33, nr. 1.

Det vil på den baggrund navnlig være trusselsvurderingen, herunder den offentliggjorte VTD, andre relevante offentliggjorte analyseprodukter og eventuelle relevante oplysninger om offentlige straffesager om straffelovens kapitel 12 og 13, og ikke bagvedliggende klassificerede oplysninger og analyser, der vil kunne indgå i vurderingen af, om betingelserne for at foretage generel og udifferentieret registrering og opbevaring af trafikdata er opfyldt.

Det vil i sidste ende være retten, som afgør, hvilken bevismæssig vægt bl.a. trusselsvurderingen, VTD'en, andre analyseprodukter og oplysninger om visse verserende og afgjorte straffesager m.v. skal tillægges i den enkelte sag, jf. princippet om den fri bevisbedømmelse.

Retten vil på grundlag af det, der er passeret under forhandlingerne og bevisførelsen, afgøre, hvilke faktiske omstændigheder der skal lægges til grund for sagens pådømmelse, jf. retsplejelovens § 344. Der vil i den forbindelse kunne være en risiko for, at retten vurderer, at de oplysninger, der er fremlagt under sagens behandling, ikke er tilstrækkelige til at vurdere, om f.eks. betingelserne for at foretage generel og udifferentieret registrering og opbevaring af trafikdata er opfyldt.

Såfremt retten under en sag måtte komme frem til, at betingelserne for en generel og udifferentieret registrering og opbevaring af trafikdata ikke er opfyldt, vil dette ikke være til hinder for, at den med lovforslaget foreslåede ordning for målrettet registrering og opbevaring af trafikdata iværksættes i muligt omfang, jf. pkt. 3.1.3.4.

Indbringes et søgsmål om, hvorvidt den foreslåede ordning om generel og udifferentieret registrering og opbevaring er i overensstemmelse med EU-retten m.v., vil der kunne opstå spørgsmål om, hvorvidt disse regler i perioden mellem indbringelse af søgsmålet og en eventuel præjudiciel forelæggelse for EU-Domstolen om dette spørgsmål vil kunne anvendes i straffesager og under efterforskning.

Det bemærkes i den forbindelse, at det fremgår af afsnittet om anvendelse af teledata i straffesager i Rigsadvokatmeddelelsen af 25. august 2020, at teledata, herunder registrerede 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.

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

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

Herudover vil der i overensstemmelse med det såkaldte ”ligestillingsprincip” være adgang til kontradiktion samt fuld transparens i processen. Det følger således af ”kontradiktionsprincippet”, at forsvareren under hovedforhandlingen på lige fod med anklageren vil kunne foretage dokumentation af registrerede og opbevarede oplysninger og stille spørgsmål til vidner m.v. Retten vil endvidere være berettiget og forpligtet til at stille spørgsmål til vidner, som afhøres, når som helst der i sandhedens interesse er grund til dette.

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

Endvidere må det antages, at lovligheden af registrerings- og opbevaringsforpligtelsen ikke har haft betydning for bevisets værdi, uanset at oplysningerne ikke ville være indhentet, hvis de foreslåede regler var underkendt ved domstolene.

I forlængelse heraf er det Justitsministeriets vurdering, at det ikke vil være i strid med artikel 47 i Chartret eller artikel 6 i Den Europæiske Menneskerettighedskonvention, at de foreslåede regler om generel og udifferentieret registrering og opbevaring fortsat anvendes i straffesager og under efterforskning i en periode mellem en eventuel indbringelse af søgsmål om reglernes overensstemmelse med EU-retten m.v., og indtil EU-Domstolen har besvaret et eventuelt præjudicielt spørgsmål herom.

3.6.3.2. Domstolsprøvelse af konkret begrundede pålæg efter den foreslåede § 786 d i retsplejeloven

Det foreslås, at målrettet registrering og opbevaring af trafikdata på grundlag af konkret begrundede pålæg, jf. den foreslåede § 786 d i retsplejeloven, undergives en forudgående domstolskontrol svarende til den, der i dag gælder for indgreb i meddelelshemmeligheden, jf. retsplejelovens § 783. Tilsvarende regler gælder eksempelvis for observation og teleobservation, jf. henvisningen til retsplejelovens § 783 i § 791 a, stk. 8, samt ved dataaflæsning, jf. § 791 b, stk. 3. De gældende regler om forudgående domstolskontrol ved indgreb i meddelelshemmeligheden er beskrevet i pkt. 3.7.1.2.

Politiet vil efter forslaget – forud for, at der foretages registrering og opbevaring af et kommunikationsapparat, en person eller et bestemt område på grundlag af en konkret vurdering – skulle indhente en retskendelse. Efter omstændighederne vil politiet kunne meddele udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, et pålæg om registrering og opbevaring uden forudgående domstolskontrol, såfremt øjemedet ellers ville forspildes, jf. § 783, stk. 4, 1. pkt., der foreslås gjort anvendelig på registrering og opbevaring på baggrund af en konkret begrundede pålæg. I sådanne tilfælde vil politiet skulle indbringe spørgsmålet for retten snarest muligt og senest inden 24 timer fra indgrebets iværksættelse, jf. stk. 4, 2. pkt.

Ved rettens kendelse skal det fastsættes, inden for hvilket tidsrum indgrebet kan foretages, jf. § 783, stk. 3, 1. pkt. Efter den gældende § 783, stk. 3, 2.

pkt., skal tidsrummet skal være så kort som muligt og må ikke overstige 4 uger, jf. stk. 3, 2. pkt. Tidsrummet kan forlænges ved kendelse, men højst med 4 uger ad gangen, jf. stk. 3, 3. og 4. pkt.

Disse regler foreslås ikke videreført, for så vidt angår den foreslåede § 785 d. I stedet foreslås det, at tidsrummet for registrering af trafikdata skal være så kort som muligt og ikke må overstige 6 måneder ad gangen. Tidsrummet vil kunne forlænges, men højst med 6 måneder ad gangen. Forlængelsen vil skulle ske ved kendelse.

Dette skal ses i lyset af, at det indgreb, som består i registrering og opbevaring af trafikdata, alt andet lige må anses for mindre indgribende end f.eks. et indgreb i meddelelshemmeligheden som aflytning, hvor indgrebet også omfatter al indholdet af en elektronisk kommunikation. Der er således ikke på samme måde som ved eksempelvis aflytning af en person tale om en krænkelse af det væsentligste indhold af de grundlæggende rettigheder fastslået i Chartrets artikel 7 og 8, jf. Tele2-dommens præmis 101.

Registrering og opbevaring af trafikdata kan imidlertid have en indvirkning på brugen af de elektroniske kommunikationsmidler og følgelig på brugerne af disse midlers udøvelse af deres ytringsfrihed, som er sikret ved Chartrets artikel 11, jf. Tele2-dommens præmis 101. Der vil derfor være behov for, at tidsrummet for de konkret begrundede pålæg ikke går videre, end hvad der er strengt nødvendigt, jf. Tele2-dommens præmis 108.

Der vil være mange forskellige situationer, der vil kunne resultere i et konkret begrundet pålæg om registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller områder med forbindelse til grov kriminalitet. Der kan både være tale om kommunikationsapparater, personer og områder med en relativt stærk forbindelse til grov kriminalitet, og der kan være tale om kommunikationsapparater, personer og områder med en mere indirekte forbindelse til grov kriminalitet. Der bør derfor efter Justitsministeriets opfattelse være mulighed for at fastsætte, at et konkret begrundet pålæg skal gælde i op til 6 måneder. Ved vurderingen af, hvor længe tidsrummet for pålægget skal være, vil der kunne lægges vægt på de konkrete omstændigheder i sagen. Er der eksempelvis tale om, at der i forbindelse med et tidsbegrænset arrangement (eksempelvis en fodboldkamp, en festival el. lign.) anmodes om registrering og opbevaring af trafikdata i et nærmere bestemt område, vil tidsrummet skulle fastsættes, så det indsnævres til det strengt nødvendige i relation til det pågældende arrangement. Det

samme vil kunne gøre sig gældende i tilfælde, hvor politiet får kendskab til forestående kriminelle handlinger, som politiet har en rimelig formodning om, vil blive begået af bestemte personer inden for et kortere tidsrum. Er der tale om et konkret begrundet pålæg vedrørende en person, som ønskes registreret og opbevaret trafikdata for, fordi der er grund til at antage, at vedkommende har en forbindelse til et større netværk, der forsøges optrevlet, vil der imidlertid som udgangspunkt foreligge omstændigheder, der tilsiger, at tidsrummet fastsættes til 6 måneder. Tilsvarende kan gøre sig gældende, hvis der er tale om et konkret begrundet pålæg vedrørende et område, hvor politiet med henblik på bekæmpelse af grov kriminalitet har interesse i at følge området i en længere periode, fordi der er grund til at antage, at det område har en forbindelse til grov kriminalitet.

Det konkrete tidsrum vedrører kun den periode, hvori registreringen af trafikdata kan finde sted, og ændrer ikke ved, at de oplysninger, der er registreret i perioden, efter forslaget skal opbevares i 1 år efter indgrebets afslutning.

Justitsministeriet vurderer, at interesserne for den eller de personer, hvis oplysninger er genstand for registrering og opbevaring på baggrund af en konkret vurdering, kan varetages på samme måde, som gælder i dag vedrørende personer, der er genstand for indgreb i meddelelseshemmeligheden. Det vil sige, at der skal beskikkes en advokat for den eller de personer, som indgrebet vedrører, inden retten træffer afgørelse om registrering og opbevaring på baggrund af en konkret vurdering, jf. retsplejelovens §§ 784-785. Disse regler giver endvidere mulighed for, efter sagens karakter, at beskikke en advokat fra den særlige kreds af advokater, der er omtalt i § 784, stk. 1, 2. pkt. Tilsvarende vil henvisningen til reglerne om beskikkede forsvarer i kapitel 66 indebære, at reglerne om forsvarers adgang til aktindsigt vil finde anvendelse, jf. § 729 a, stk. 2 og 3. Advokaten vil derfor have adgang til det materiale, som politiet har tilvejebragt til brug for sagen, jf. § 729 a, stk. 3, 1. pkt. Advokatens adgang til materiale vil, som forsvarerens adgang, kunne begrænses med henvisning til eksempelvis hensynet til fremmede magter, statens sikkerhed eller sagens opklaring, jf. § 729 c, stk. 1, nr. 1-3. De gældende regler herom er beskrevet i pkt. 3.7.1.2.

Særligt for registrering og opbevaring på baggrund af konkret begrundede pålæg vedrørende bestemte personer bemærkes det, at der som udgangspunkt vil skulle beskikkes en advokat for den eller de personer, hvis oplysninger gøres til genstand for registrering og opbevaring. Advokaten kan gøre

indsigelser, hvis advokaten ikke mener, at der er grundlag for at foretage målrettet personbestemt registrering og opbevaring. Eksempelvis hvis advokaten mener, at den konkrete person ikke har en forbindelse til grov kriminalitet, eller at indgrebet er uproportionalt, jf. de foreslåede § 786 d, stk. 1, og § 786 d, stk. 2, 3. pkt., jf. § 782, stk. 1.

Særligt for så vidt angår registrering og opbevaring på baggrund af konkret begrundede pålæg vedrørende bestemte områder bemærkes det, at det vil være tilstrækkeligt at beskikke én advokat, der varetager interesserne for alle de personer, der vil blive berørt af denne registrering og opbevaring. Det er kendetegnet for denne form for registrering og opbevaring, at den ikke foretages på baggrund af en konkret vurdering af den enkelte persons forhold, men sker på baggrund af en konkret vurdering af forholdene i et nærmere bestemt område, jf. ovenfor i pkt. 3.1.3.2. Disse forhold vil gøre sig gældende for alle de personer, der befinder sig i området.

Advokaten kan også her gøre indsigelse, hvis advokaten er af den opfattelse, at det pågældende område, ikke har en forbindelse til grov kriminalitet, jf. den foreslåede § 786 d, stk. 1, eller hvis indgrebet er uproportionalt, fordi registreringen og opbevaringen f.eks. dækker for stort et område i forhold til, hvad forbindelsen til grov kriminalitet kan bære, jf. den foreslåede § 786 d, stk. 2, 3. pkt., jf. § 782, stk. 1.

Reglerne om underretning, jf. retsplejelovens § 788 foreslås ikke overført til pålæg om registrering og opbevaring på baggrund af konkret begrundede pålæg.

Det vil ofte være centralt for efterforskningen, at registrering og opbevaring foretaget i medfør af den foreslåede § 786 d, ikke bliver kendt for de personer, den vedrører. Disse personers interesser vil være varetaget ved den foreslåede advokatbeskikkelse.

Der vil fortsat skulle ske underretning af de relevante personer i forbindelse med, at politiet får adgang til oplysningerne, jf. retsplejelovens § 788, stk. 1-3, hvis ikke der er grundlag for at undlade underretning, jf. § 788, stk. 4. Underretning kan eksempelvis undlades, hvis det 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 meddelelshemmeligheden. Med lovforslagets § 1, nr. 13, foreslås et nyt stk. 9 i retsplejelovens § 806, hvorefter bl.a. reglerne om underretning i §

788 gøres anvendelige også i tilfælde, hvor adgangen til den registrerede og opbevarede data sker efter reglerne om edition. Der henvises til pkt. 3.7.3.3.4 og til bemærkningerne til lovforslagets § 1, nr. 13.

Udbyderne af elektroniske kommunikationsnet eller -tjenester skal efter gældende ret ikke orienteres om retsmøder vedrørende indgreb i meddelelseshemmeligheden. Denne retsstilling foreslås overført til afgørelser, der træffes efter den foreslåede § 786 d i retsplejeloven; og udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, vil derfor heller ikke skulle orienteres om retsmøder, der foretages med henblik på at træffe afgørelser efter den foreslåede § 786 d. Dette adskiller sig fra situationer, hvor et indgreb foretages efter reglerne om edition i lovens kapitel 74, hvor der skal ske underretning af udbyderne af elektroniske kommunikationsnet eller -tjenester efter retsplejelovens § 806, stk. 9, medmindre retten bestemmer, at der ikke skal gives underretning, jf. § 748, stk. 5 og 6. Der henvises til pkt. 3.7.1.2.

Justitsministeriet har også overvejet, om der skal indføres et krav om forudgående retskendelse i forbindelse med hastesikring. Det er Justitsministeriets vurdering, at der i EU-Domstolens praksis stilles krav om en effektiv prøvelse af hastesikring, men at denne ikke behøver at være forudgående, jf. La Quadrature du Net-dommens præmis 163. Oplysninger, som er sikret i medfør af reglerne om hastesikring, vil politiet efter gældende ret kunne få adgang til efter de relevante regler i retsplejeloven. Denne adgang vil som hovedregel kræve forudgående retskendelse. Der henvises til pkt. 3.7 vedrørende adgang til oplysninger.

3.7. Adgang til registrerede og opbevarede data

3.7.1. Gældende ret

3.7.1.1. Indledning

Politiets adgang til trafikdata samt oplysninger om brugeridentitet sker i dag efter retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden m.v. eller reglerne om edition i retsplejelovens kapitel 74 afhængig af, hvilke typer oplysninger der er tale om. Endvidere findes der, som gennemgået under pkt. 3.4.1, regler om udlevering af basale oplysninger om en slutbruger i telelovens § 13.

Reglerne om indgreb i meddelelseshemmeligheden og om edition anvendes både på oplysninger, som udbyderne er forpligtede til at registrere og opbevare i medfør af logningsbekendtgørelsen, jf. pkt. 3.1.1, og på andre oplysninger (ikke-registreringspligtige), f.eks. når en telefon signalerer til mobilnetværket, selv om telefonen ikke aktivt anvendes på det pågældende tidspunkt (lokaliseringsdata som udbydere af elektroniske kommunikationsnet eller -tjenester er i besiddelse af hensyn til fejlretning m.v., ofte kaldet »allerede registreret lokaliseringsdata«).

3.7.1.2. Teleoplysning

3.7.1.2.1. Anvendelse

Retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden m.v. blev indsat ved lov nr. 227 af 6. juni 1985, der bygger på Strafferetsplejeudvalgets betænkning nr. 1023/1984. Kapitel 71 er ændret flere gange siden 1985.

Det følger af retsplejelovens § 780, stk. 1, nr. 3, at politiet kan foretage indgreb i meddelelseshemmeligheden ved at indhente oplysninger om, hvilke telefoner eller andre tilsvarende kommunikationsapparater, der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning).

Retsplejelovens § 780, stk. 1, nr. 3, omfatter både oplysninger om kommunikation, der har været foretaget (historiske oplysninger), samt kommunikation, der vil blive foretaget i fremtiden. Det fremgår således af bestemmelsens forarbejder, at der ikke er tilsigtet nogen realitetsændring i forhold til den tidligere § 788, stk. 1, i retsplejeloven, hvoraf det fremgik, at vedkommende telefonadministration skulle meddele politiet oplysninger om, hvilke telefoner der i et bestemt tidsrum »sættes eller har været sat« i forbindelse med en bestemt telefon. Der henvises til betænkning nr. 1023/1984, s. 210.

Retsplejelovens § 780, stk. 1, nr. 3, er efter sin ordlyd ikke begrænset til bestemte typer af oplysninger. 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.

Teleoplysning bliver af politiet i praksis typisk anvendt til at klarlægge, hvilke kommunikationsapparater der har kommunikeret med hinanden i et bestemt tidsrum. Teleoplysning omfatter eksempelvis navne, telefonnumre,

IMEI-numre, IMSI-numre eller andre oplysninger om, hvilke kommunikationsapparater der har været sat i forbindelse med hinanden. Derimod er oplysninger om, hvilken slutbruger der er indehaver af et bestemt telefonnummer, en bestemt IP-adresse, et bestemt IMEI- eller IMSI-nummer etc. ikke omfattet af reglerne om teleoplysning, men kan indhentes efter retsplejelovens regler om edition eller efter telelovens § 13, hvorefter udbydere af elektroniske kommunikationsnet eller -tjenester på begæring af politiet skal udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester. Afgørende er i den forbindelse, om oplysningerne angiver, hvilke kommunikationsapparater der er sat eller sættes i forbindelse med hinanden. Er dette tilfældet, skal reglerne om teleoplysning anvendes.

Udlevering af oplysninger om, hvilke telefoner eller tilsvarende kommunikationsapparater der har taget kontakt til en bestemt telefon m.v., udgør ikke et indgreb i meddelelshemmeligheden, 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 således pålægges at udlevere sådanne oplysninger, uden at betingelserne for at foretage indgreb i meddelelshemmeligheden skal være opfyldt, jf. retsplejelovens § 786, stk. 2.

Når anklagemyndigheden indhenter kendelse om indgreb i meddelelshemmeligheden i form af fremadrettet teleoplysning efter retsplejelovens § 780, stk. 1, nr. 3, omfatter kendelsen om teleoplysning i praksis både oplysninger om, hvilke kommunikationsapparater der sættes i forbindelse med hinanden, samt hvilke sendemaster og masteceller de registres på (masteoplysninger). En kendelse om aflytning efter retsplejelovens § 780, stk. 1, nr. 1, vil i praksis også omfatte teleoplysning og masteoplysning.

Når anklagemyndigheden indhenter kendelse om indgreb i meddelelshemmeligheden i form af bagudrettet (historisk) teleoplysning sker dette i praksis efter retsplejelovens § 780, stk. 1, nr. 3, samt lovens § 804 om edition. Kendelsen vil omfatte både oplysninger om, hvilke kommunikationsapparater der har været sat i forbindelse med hinanden, samt hvilke sendemaster og masteceller de har været registreret på.

3.7.1.2.2. Kriminalitetskrav

De almindelige betingelser for at foretage indgreb i meddelelseshemmeligheden, herunder i form af teleoplysning, findes i retsplejelovens § 781, stk. 1.

Det følger af denne bestemmelse, at indgreb i meddelelseshemmeligheden kun må foretages, såfremt 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 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 (kriminalitetskravet). Disse lovovertrædelser er dels afgrænset ved en generel henvisning til alle lovovertrædelser med en bestemt strafferamme dels specificeret ved henvisning til bestemte kapitler i straffeloven eller til bestemte 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 kapitel 12 eller 13 eller en overtrædelse af straffelovens § 124, stk. 2 (befrielse af en anholdt eller fængslet m.v.), § 125 (hjælp til at unddrage nogen fra forfølgning for en forbrydelse m.v.), § 127, stk. 1 (unddragelse af krigstjeneste m.v.), § 233, stk. 1 (rufferi), § 235 (besiddelse og udbredelse af børnepornografisk materiale), § 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, er 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 nedsettelse 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 visse former for indgreb i meddelelseshemmeligheden, uanset det almindelige kriminalitetskrav i § 781, stk. 1, nr. 3, ikke er opfyldt, såfremt betingelserne i § 781, stk. 1, nr. 1 og 2, i øvrigt er opfyldt.

Efter retsplejelovens § 781, stk. 2, kan fredskrænkelser som omhandlet i straffelovens § 263, stk. 1 (hacking), således begrunde indgreb i meddelelseshemmeligheden i form af telefonaflytning eller teleoplysning, jf. § 780, stk. 1, hhv. nr. 1 og nr. 3, uanset om kriminalitetskravet i § 781, stk. 1, er opfyldt. Strafferammen i straffelovens § 263, stk. 1, går fra bøde til fængsel indtil 1 år og 6 måneder.

Efter retsplejelovens § 781, stk. 3, nr. 1, kan teleoplysning foretages, hvis mistanken angår en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, uanset om kriminalitetskravet i § 781, stk. 1, er opfyldt. Efter retsplejelovens § 781, stk. 3, nr. 2, kan teleoplysning endvidere foretages, hvis mistanken angår en overtrædelse af straffelovens § 279 a om databedrageri, eller § 293, stk. 1, om brugstyveri ved anvendelse af en telekommunikationstjeneste, uanset om kriminalitetskravet i § 781, stk. 1, nr. 3, er opfyldt.

Retsplejelovens § 781, stk. 3, nr. 3-5, oplister en række overtrædelser af forskellige EU-regler om forbud mod insiderhandel og markedsmanipulation på forskellige områder, der kan begrunde teleoplysning, f.eks. markedsmisbrugsforordningen.

Vedrørende retsplejelovens § 781, stk. 1, nr. 5, skal det bemærkes, at de deri nævnte artikler i CO₂-auktioneringsforordningen er udgået med artikel 1, nr. 33, i Kommissionens delegerede forordning (EU) 2019/1868 af 28. august 2019 om ændring af forordning (EU) nr. 1031/2010. Det fremgår af betragtning nr. 9 i præamblen til Kommissionens forordning, at eftersom markedsmisbrugsforordningen finder direkte anvendelse på auktioner over emissionskvoter, er bestemmelserne om markedsmisbrug i CO₂-auktioneringsforordningens blevet overflødige og bør slettes.

Det er kendetegnende for de lovovertrædelser, der er særskilt nævnt i retsplejelovens § 781, stk. 1, nr. 3, samt § 781, stk. 2 og 3, at de kan være vanskelige at efterforske, hvis ikke der er adgang til indgreb i meddelelseshemmeligheden, eller at indgreb i meddelelseshemmeligheden er et relevant el-

ler hensigtsmæssigt efterforskningsmiddel. For så vidt angår lovovertrædelserne i § 781, stk. 3, nr. 3-5, er der tale om lovovertrædelser, der består i forskellige overtrædelser af EU-forordninger om forbud mod insiderhandel og uretmæssig videregivelse af intern viden samt forbud mod markedsmissbrug. Det følger af de forskellige EU-forordninger, at myndighederne i overensstemmelse med national lovgivning bl.a. skal tillægges beføjelser til at kræve at få udleveret fortegnelse over datatrafik.

3.7.1.2.3. Proportionalitetskrav m.v.

Teleoplysning må, ligesom andre indgreb i meddelelshemmeligheden, 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 lovovertrædelserne i øvrigt er omfattet af kriminalitetskravet i § 781.

Retsplejelovens § 782, stk. 2, fastslår, at der ikke må foretages telefonaflytning, anden aflytning, brevåbning og brevstandsning med hensyn til den mistænkte forbindelse med personer, som efter reglerne i § 170 er udelukket fra at afgive forklaring som vidne. Teleoplysning og udvidet teleoplysning er udtrykkeligt ikke medtaget i denne undtagelsesregel, og disse indgreb kan derfor godt foretages med hensyn til mistænkte forbindelse med de nævnte personer. Dette forhold er omtalt nærmere i pkt. 3.10.

Indgreb i meddelelshemmeligheden sker efter rettens kendelse, jf. retsplejelovens § 783, stk. 1, 1. pkt. I kendelsen skal angives det telefonnummer, som indgrebet angår, jf. stk. 1, 2. pkt. Indgreb kan finde sted ikke blot med henvisning til bestemte telefonnumre, men også bestemte telefonapparater identificeret ved et såkaldt IMEI-nummer (telefonapparatnummer), jf. fra retspraksis Vestre Landsrets kendelse af 22. juni 1998 i sag nr. S-1654-98, gengivet i *Ugeskrift for Retsvæsen 1998, s. 1412 f.*

I kendelsen fastsættes det tidsrum, inden for hvilket indgrebet kan foretages, jf. § 783, stk. 3. Tidsrummet skal være så kort som muligt og må ikke overstige 4 uger. Tidsrummet kan forlænges, men højst 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 giver tilladelse til, at der kan foretages 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, 1. pkt. Angår efterforskningen en overtrædelse af straffelovens kapitel 12 eller 13, beskikkes advokaten fra den særlige kreds af advokater. 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. retsplejelovens § 785, stk. 1. Det fremgår af retsplejelovens § 785, stk. 1, 2. pkt., at advokaten er berettiget til at få udleveret genparter af materialet. Finder politiet, at materialet er af særlig fortrolig karakter, og at genpart heraf derfor ikke bør udleveres, skal spørgsmålet herom på begæring af advokaten af politiet indbringes for retten, jf. stk. 1, 3. pkt. Advokaten må ikke give de modtagne oplysninger videre til andre eller uden politiets samtykke sætte sig i forbindelse med den, over for hvem indgrebet er begæret foretaget, jf. stk. 1, 4. pkt.

Det fremgår videre af retsplejelovens § 785, stk. 2, at bl.a. bestemmelserne om beskikkede forsvarer i lovens kapitel 66 om sigtede og hans forsvarer finder tilsvarende anvendelse på den beskikkede advokat. Dette indebærer bl.a., at den beskikkede advokat har krav på aktindsigt, jf. reglerne i retsplejelovens § 729 a, stk. 2 og 3, men at retten efter anmodning fra politiet kan bestemme, at reglerne om aktindsigt fraviges, hvis det er påkrævet af hensyn til bl.a. fremmede magter, statens sikkerhed eller sagens opklaring, jf. retsplejelovens § 729 c, stk. 1, nr. 1-3.

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. retsplejelovens § 788, stk. 4, 1. pkt.

Underretning ved telefonaflytning og teleoplysning skal gives til indehaveren af den pågældende telefon eller kommunikationsapparat, der har været genstand for indgrebet, jf. retsplejelovens § 788, stk. 2, nr. 1. Dvs., at det typisk vil være indehaveren af abonnementet, der skal underrettes. Der henvises til betænkning nr. 1023/1984, s. 117.

3.7.1.3. 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 er 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«).

Indførelsen af bestemmelsen i retsplejelovens § 780, stk. 1, nr. 4, om udvidet teleoplysning er i bemærkningerne til lovforslaget begrundet i Højesterets kendelse af 7. maj 1997 i sag nr. 457/1996, gengivet i *Ugeskrift for Retsvæsen*, 1997, s. 1021 f.

Det fremgår af forarbejderne, at udvidet teleoplysning ikke specifikt vedrører masteoplysninger, men at bestemmelsen er formuleret, så den tager højde for den teknologiske udvikling og vedrører oplysninger, 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.

Udvidet teleoplysning omfatter oplysninger om, hvilke telefoner der inden for et nærmere angivet område har været sat eller sættes i forbindelse med andre telefoner. Telefonerne skal have været i aktiv brug til f.eks. tale, sms og mms for at fremgå af udvidet teleoplysning.

Som anført ovenfor under pkt. 3.7.1.2 følger det af retsplejelovens § 781, stk. 1, at indgreb i meddelelshemmeligheden kun må foretages, hvis 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 indgrebet må antages at være af afgørende betydning for efterforsk-

ningen (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 (kriminalitetskravet).

Det følger imidlertid af § 781, stk. 5, at udvidet teleoplysning efter § 780, stk. 1, nr. 4, kun kan foretages, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller betydelige samfundsværdier. Det følger endvidere af bestemmelsen, at udvidet teleoplysning kan foretages, uanset at betingelsen i stk. 1, nr. 1 (mistankekravet), ikke er opfyldt.

Reglerne om proportionalitet, retskendelse, advokatbeskikkelse, og bistandspligt fra teleselskaberne, gælder også for indgreb i meddelelshemmeligheden i form af udvidet teleoplysning. Der henvises til pkt. 3.7.1.2.

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

3.7.1.4. Edition

3.7.1.4.1. Anvendelse

Retsplejelovens kapitel 74 om beslaglæggelse og edition blev indsat ved lov nr. 229 af 21. april 1999, og editionsreglerne er i det væsentlige uændrede siden dengang. Ved lov nr. 124 af 30. januar 2021 blev indsat § 806, stk. 7, i retsplejeloven, der gav politiet mulighed for at træffe visse afgørelser om edition uden forudgående retskendelse.

Efter retsplejelovens § 804, stk. 1, kan der som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller krænkelser 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 konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

»Genstand« er ikke begrænset til fysiske genstande. Editionspligten kan efter forarbejderne omfatte eksempelvis pligt til at udlevere en fotokopi eller en udskrift af et »EDB-register«, jf. bemærkningerne til § 804 i lovforslag nr. L 41 af 8. oktober 1998, jf. Folketingstidende 1998-99, tillæg A, s. 875. »Genstand« kan også omfatte oplysninger om, hvilke sendemaster og masteceller eller lignende telefonen eller kommunikationsapparatet har været sat i forbindelse med. Hvis et teleselskab er i besiddelse af sådanne allerede lagrede (historiske) oplysninger, eksempelvis som følge af reglerne om registrering og opbevaring, kan disse oplysninger kræves udleveret efter reglerne om edition. Denne retstilling blev lagt til grund ved Højesterets kendelse af 22. juli 2009 i sag nr. 419/2008, gengivet i *Ugeskrift for Retsvæsen*, 2009, s. 2610 ff., der vedrørte allerede lagrede masteoplysninger. Hvis oplysningerne, der ønskes udleveret, tillige angår, hvilke kommunikationsapparater der har været sat i forbindelse med hinanden, skal reglerne om teleoplysning anvendes, jf. pkt. 3.7.1.2.

Forskelligt fra almindelige masteoplysninger er oplysninger om, hvilke sendemaster en telefon eller kommunikationsapparat har signaleret til (allerede registreret lokaliseringsdata) uden at have været aktiv på den pågældende mast. Sådanne oplysninger er ikke omfattet af registreringspligten efter gældende ret. Trafikdata i forbindelse med internetforbrug er heller ikke registreringspligtigt efter den gældende § 786, stk. 4, og regler fastsat i medfør heraf. Hvis teleselskaberne er i besiddelse af sådanne oplysninger, kan de kræves udleveret efter reglerne om edition.

Retsplejelovens regler om edition anvendes endvidere, hvis der er tale om udlevering af historiske masteoplysninger for et bestemt område eller en bestemt adresse, jf. Østre Landsrets kendelse af 3. marts 2017 i sag nr. S-584-17, gengivet i *Ugeskrift for Retsvæsen* 2017, s. 1934 f. Hvis der samtidig anmodes om oplysninger om, hvilke kommunikationsapparater i et område der sættes i forbindelse med andre kommunikationsapparater, anvendes reglerne om udvidet teleoplysning, jf. pkt. 3.7.1.3.

Edition kan ligeledes bruges til at få udleveret oplysninger om brugerens identitet. Eksempelvis kan oplysninger om, hvilken abonnent der er indehaver af et bestemt telefonnummer, en bestemt IP-adresse, et bestemt IMEI-nummer eller IMSI-nummer etc., kræves udleveret efter reglerne om edition eller efter reglen i telelovens § 13, hvis udbyderne af elektroniske kommunikationsnet eller -tjenester er i besiddelse af oplysninger herom på andet grundlag end en registrerings- og opbevaringspligt. Der henvises til Vestre

Landsrets kendelse af 3. november 2004 i sag nr. S-2473-04, gengivet i *Ugeskrift for Retsvæsen* 2005, s.777 f., og til Østre Landsrets kendelse af 11. september 2006 i sag nr. S-2688-0 6, gengivet i *Ugeskrift for Retsvæsen* 2007.22 f.

3.7.1.4.2. Kriminalitetskrav

Kriminalitetskravet 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, eller en krænkelse som nævnt i § 2, stk. 2, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, jf. retsplejelovens § 804, stk. 1, 1. pkt.

Det lave kriminalitetskrav skal ses i lyset af editionsreglernes sammenhæng med vidnereglerne. Retsplejelovens regler om edition er udarbejdet med det udgangspunkt, at der ikke bør være grund til hemmeligholdelse af flere oplysninger efter reglerne om edition end efter reglerne om vidneforklaring. Den almindelige vidnepligt gælder i alle sager og ikke kun i sager vedrørende lovovertrædelser af en vis grovhed, jf. § 168, stk. 1. Der henvises til betænkning nr. 316/1962, s. 91 f., og betænkning nr. 1223/1991, s. 32.

Det fremgår af forarbejderne til retsplejelovens § 804, stk. 1, 1. pkt., at henvisningen til § 2, stk. 2, nr. 1, i lov om tilhold, opholdsforbud og bortvisning indebærer, at edition kan ske med henblik på at vurdere, om betingelserne for at meddele tilhold er opfyldt. Det fremgår videre af forarbejderne, at edition bør kunne foretages, når der foreligger gentagne krænkelse, eller når der foreligger en enkelt krænkelse af en sådan grovhed, at krænkelsen i sig selv kan give grundlag for tilhold. Der henvises til betænkning nr. 1023/1984, s. 95, samt til pkt. 3.7.3.1 i de almindelige bemærkninger til lovforslag nr. L 10 af 9. november 2011, jf. Folketingstidende 2011-12, tillæg A, s. 26.

3.7.4.4.3. Tavshedspligt, proportionalitet m.v.

Oplysninger omfattet af en tavshedspligt skal som udgangspunkt udleveres ved et pålæg om edition. Der gælder dog en undtagelse for visse professioner, herunder præster i folkekirken eller andre trossamfund, læger, forsvarere, retsmæglere og advokater. For andre professioner skal et editionspålæg efterkommes, uanset en eventuel tavshedspligt. Dette gælder, uanset om tavshedspligten følger af loven eller af aftale, vedtægter eller en branchesædvane eller lignende. For de professioner, der ikke er omfattet af stk. 1,

men er undergivet en tavshedspligt i medfør af lovgivningen, har retten mulighed for konkret at bestemme, at de alligevel ikke er forpligtede til at udlevere oplysninger omfattet af tavshedspligten, jf. retsplejelovens § 804, stk. 4, jf. § 170, stk. 3.

Hvis en fysisk eller juridisk person for at efterkomme et editionspålæg er nødt til at udlevere oplysninger, der er omfattet af en tavshedspligt, kan der ikke straffes for overtrædelse af tavshedspligten. Der er heller ikke pligt til at betale erstatning for et tab, der måtte være lidt herved. Udlevering af oplysninger anses i sådanne tilfælde for at være berettiget, og der er derfor ikke tale om et brud på tavshedspligten. Udbyderne af elektroniske kommunikationsnet eller -tjenesters tavshedspligt er beskrevet nærmere i pkt. 3.1.1.4.

Det følger af retsplejelovens § 805, stk. 1, at et pålæg om edition ikke må meddeles, hvis indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre. Ifølge bestemmelsens forarbejder lovfæster den det almindelige proportionalitetsprincip, der antages at gælde ved alle straffeprocessuelle tvangsindgreb. Der henvises til bemærkningerne til retsplejelovens § 805 i lovforslag nr. L 41 af 8. oktober 1998, jf. Folketingstidende 1998-99, tillæg A, s. 876.

Herudover skal der foretages en afvejning af kravet på hemmeligholdelse over for hensynet til retshåndhævelsen, dvs. afvejning af hensynet til at få udleveret oplysninger til brug for efterforskning af straffesager over for brugernes krav på hemmeligholdelse, sådan som dette er sikret i e-databeskyttelsesdirektivet og i EU's charter om grundlæggende rettigheder, jf. Østre Landsrets kendelse af 7. maj 2018 i sag nr. B-2451-17 og B-2458-17, gengivet i *Ugeskrift for Retsvæsen 2019, s. 2019 ff.* Sagen er afgjort efter civilprocessens regler om edition, jf. retsplejelovens § 299, men de hensyn, der ifølge landsretten begrundes kravet på hemmeligholdelse, gælder også i strafferetsplejen. Det må derfor antages, at en tilsvarende afvejning skal foretages, hvis edition begæres efter strafferetsplejens regler om edition.

Afgørelse om pålæg om edition træffes af retten efter politiets begæring, jf. retsplejelovens § 806, stk. 1 og 2. Hvis indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om edition, jf. § 806, stk. 4, 1. pkt. 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. pkt. For bankoplysninger m.v. kan en afgørelse om edition træffes af politiet uden forudgående retskendelse, jf. retsplejelovens § 806, stk. 7.

Efter retsplejelovens § 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.

Retsplejelovens § 806, stk. 9 og 10, indeholder regler om kontradiktion, for så vidt angår den, pålægget om edition retter sig imod, hvilket vil være udbyderen af elektroniske kommunikationsnet eller -tjenester. Manglende iagttagelse af kontradiktionspligten kan medføre, at begæring om edition ikke imødekommes, jf. eksempelvis en afgørelse fra Vestre Landsret af 14. april 1977 i sag nr. I-727/1977, gengivet i Ugeskrift for Retsvæsen 1977, s. 736. I sagen opretholdt landsretten en afgørelse, hvor byretten havde afvist et editionspålæg vedrørende udlevering af kontooplysninger, da de banker, der havde rådighed over oplysningerne, ikke havde haft lejlighed til at udtale sig. Der er imidlertid ingen pligt til at underrette den, der måtte være genstand for oplysningerne, eksempelvis ejeren af en telefon, for hvilken der bliver registreret og opbevaret trafikdata.

Hvis der er en forsvarer for en sigtet i sagen, skal denne underrettes om retsmødet vedrørende editionsspørgsmålet og have mulighed for at overvære mødet, jf. retsplejelovens § 748, stk. 2, 1. pkt. Retten kan dog efter politiets begæring bestemme, at reglen om underretning kan fraviges, hvis hensynet til fremmed magter, til statens sikkerhed eller til sagens opklaring eller tredjemand undtagelsesvis gør det påkrævet, jf. bestemmelsens 3. og 4. pkt. Forsvareren må kun med rettens samtykke videregive oplysninger, han har modtaget i retsmødet, jf. stk. 2, 5. pkt. Manglende iagttagelse af kontradiktionsreglen i forhold til forsvareren kan også medføre, at der ikke meddeles pålæg om edition, eller at et allerede meddelt pålæg må ophæves, jf. eksempelvis Vestre Landsrets afgørelse af 7. januar 1988 i sag nr. 8, *gengivet i Ugeskrift for Retsvæsen 1988, s. 408/1*.

3.7.1.5 Telelovens § 13

Det følger af telelovens § 13, at udbydere af elektroniske kommunikationsnet eller -tjenester 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, som blev indsat ved lov nr. 545 af 8. juni 2006. Det fremgår af de specielle bemærkninger til denne bestemmelse, jf. forslag nr. L 219 af 31. marts 2006 til lov om ændring af lov om konkurrence- og forbrugerforhold på telemarkedet, lov om radiofrekvenser og lov om radio- og teleterminaludstyr og elektromagnetiske forhold, Folketingstidende 2005-06, tillæg A, 7335f, 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.

Udbyderne af elektroniske kommunikationsnet eller -tjenester er ikke efter telelovens § 13 forpligtede til at registrere og gemme oplysninger, ud over hvad der allerede følger af telelovens § 31, stk. 2 og 3, om afgivelse af nummeroplysningsdata, men forpligtes alene til at udlevere oplysninger, som udbyderen i øvrigt måtte være i umiddelbar besiddelse af om en slutbrugers adgang til kommunikationsnet eller -tjenester.

Det skal bemærkes, at oplysninger, som udbyderne af elektroniske kommunikationsnet eller -tjenester alene ligger inde med som følge af en registrerings- og opbevaringspligt, kun kan udleveres efter reglerne i retsplejeloven.

Det bemærkes i forarbejderne til telelovens § 13, at der er både tale om navn til nummer og nummer til navn oplysninger. Det bemærkes endvidere, at bestemmelsen alene omfatter statiske oplysninger, idet registrering af dynamiske IP-adresser m.v. vil ske i medfør af registreringsforpligtelsen i retsplejelovens § 786, stk. 4. Udlevering af dynamiske IP-adresser m.v. sker efter retsplejelovens bestemmelser om edition.

Det bemærkes desuden, at de oplistede eksempler i forarbejderne til telelovens § 13 er eksempler på de typer af oplysninger, der på tidspunktet for

forarbejdernes forfættelse kunne identificere en slutbrugers adgang til kommunikationsnet eller -tjenester for alle elektroniske kommunikationsformer, herunder en slutbrugers adgang til internettet. Der vil som følge af den almindelige teknologiske udvikling kunne opstå nye typer af oplysninger, der kan betegnes som oplysninger om en slutbrugers adgang til kommunikationsnet eller -tjenester, og som kan tjene til at identificere en bestemt slutbruger.

Telelovens § 13 blev indsat på baggrund af overvejelser om det danske samfunds beredskab og indsats mod terrorhandlinger, men bestemmelsen har efter dens ordlyd og forarbejder intet kriminalitetskrav m.v. Den nugældende bestemmelse kan således anvendes til brug for politiets efterforskning af ethvert strafbart forhold, men også som led i politiets øvrige opgavevaretagelse, jf. politilovens § 2.

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

Hvis en udbyder af elektroniske kommunikationsnet eller -tjenester ikke efterkommer politiets begæring i medfør af telelovens § 13, kan de pålægges bødestraf, jf. telelovens § 81, stk. 1, nr. 1.

3.7.2. EU-Domstolens praksis

EU-Domstolens udtalelser vedrørende registrering af trafik- og lokaliseringsdata i La Quadrature du Net-dommen er omtalt i pkt. 3.1.2 og 3.2.2. For så vidt angår EU-Domstolens behandling af spørgsmålet om adgangen til lagret data i dommen, henvises til 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.«

Det må således lægges til grund, at der efter EU-Domstolens opfattelse i princippet kun må gives adgang til registrerings- og opbevaringspligtig trafikdata med henblik på at efterforske og retsforfølge en strafbar overtrædelse, hvis den strafbare overtrædelse vedrører det hensyn, der er baggrunden for, at teleudbyderne m.v. er pålagt at registrere og opbevare de pågældende data, idet der dog kan gives adgang til registrerede og opbevarede trafikdata med henblik på at beskytte den nationale sikkerhed, selv om registrerings- og opbevaringsforpligtelsen 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 kan begrunde, at politiet og anklagemyndigheden kan få adgang til registrerings- og opbevaringspligtige trafikdata. EU-Domstolen tager derimod ikke eksplicit stilling til, om hensynet til at efterforske og retsforfølge grov kriminalitet kan begrunde, at politiet og anklagemyndigheden kan få adgang til trafikdata, der er lagret med henblik på at beskytte den nationale sikkerhed.

Domstolen henviser dog i præmis 166 til dommens 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-dommen og det her opstillede proportionalitetskrav, må dette efter Justitsministeriets opfattelse fortolkes således, at Domstolen herved – fortsat – har den opfattelse, at det indgreb i de grundlæggende rettigheder, som teleudbyderes pligt til at registrere og opbevare trafikdata og offentlige myndigheders adgang hertil udgør, kan begrundes i hensynet til forebyggelse, efterforskning 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.

Justitsministeriet vurderer således – under en væsentlig procesrisiko, som kan aktualiseres ved de nye reglers ikrafttræden, i lyset af præmis 166 i La Quadrature du Net-dommen – at dommen ikke er til hinder for, at medlemsstaterne kan give politiet og anklagemyndigheden adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af 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 politiet og anklagemyndigheden adgang til sådanne registrerede og opbevarede trafikdata.

Den ovenfor omtalte procesrisiko vil kunne foreligge i en situation, hvor spørgsmålet om lovligheden af f.eks. registreringen eller indhentelsen af oplysninger fører til, at retten vurderer, at spørgsmålet om, hvorvidt de pågældende oplysninger kan anvendes som bevis i straffesager, skal forelægges præjudicielt for EU-Domstolen. En sådan præjudiciel forelæggelse vil potentielt kunne medføre, at straffesager, hvor loggede oplysninger indgår, og

er nødvendige at dokumentere som led i bevisførelsen, ikke vil kunne afvikles. Det vil kunne føre til en sagsophobning i straffesagskæden, ligesom det i en periode vil kunne hindre effektiv strafforfølgning af en lang række kriminalitetstyper.

EU-Domstolens dom af 2. marts 2021 i H.K.-sagen har ikke endeligt afgjort spørgsmålet om adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet. 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 trafik-data 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).«

Herudover skal Justitsministeriet bemærke, 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 i La Quadrature du Net-dommen, at adgangen til registrerede og opbevarede 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 registreringen og opbevaringen af oplysningerne.

Desuden bemærkes det, at den franske Conseil d'État i opfølgning af EU-Domstolens dom i La Quadrature du Net-sagen, som Conseil d'État havde forelagt præjudicielt for EU-Domstolen, i sin afgørelse af 21. april 2021 har fastslået, at den eksisterende trussel mod den nationale sikkerhed i Frankrig kan begrunde en pligt for teleudbydere til generel og udfifferentieret at registrere og opbevare trafik- og lokaliseringsdata på nuværende tidspunkt, og at de franske efterforskningsmyndigheder kan få adgang hertil med henblik på bekæmpelse af alvorlig kriminalitet.

3.7.3. Justitsministeriets overvejelser

3.7.3.1. *Generelle overvejelser i lyset af den nyeste EU-praksis*

Adgangen til oplysninger, som udbydere af elektroniske kommunikationsnet eller -tjenester indsamler, registrerer og opbevarer 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, jf. omtalen af bekendtgørelsen i pkt. 3.7.1.2, er et helt centralt efterforskningsværktøj for politiet i forbindelse med efterforskningen af kriminalitet, ligesom det kan være afgørende for anklagemyndighedens strafforfølgning af tiltalte ved domstolene.

Politiet anvender oplysninger fra udbydere af elektroniske kommunikationsnet eller -tjenester på forskellige stadier af efterforskningen. I den indledende fase kan det navnlig være aktuelt at analysere oplysninger om relevante personers kommunikation og på den baggrund danne et overblik over personernes kommunikationsmønstre og færden. Det gør det muligt at målrette den efterfølgende efterforskningsmæssige indsats, herunder udelukke

personer fra efterforskningen, hvis de vurderes ikke at have relevans for sagen.

Oplysninger registreret og opbevaret af udbydere af elektroniske kommunikationsnet eller -tjenester kan navnlig være med til at målrette politiets indsamling af andre beviser, herunder videoovervågning, på et tidligt stadie af efterforskningen, 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 disse oplysninger også bidrage til at opspore den mistænkte. En analyse af indhentede oplysninger fra udbydere af elektroniske kommunikationsnet eller -tjenester kan også resultere i nye spor i efterforskningen eller kaste lys over andre forhold, der gør det nødvendigt at indhente yderligere oplysninger fra udbydere. Ved efterforskning i lukkede, kriminelle miljøer, f.eks. i sager vedrørende organiseret narkotika- eller bandekriminalitet, kan oplysningerne – typisk i første omgang vedrørende personer, som politiet ikke har kendt til eller haft fokus på – bidrage til, at mistænkte kan kædes sammen, og at kriminelle netværk optrevles. På tilsvarende vis anvendes disse oplysninger til at afkræfte, om mistænkte har relationer til kriminelle netværk eller grupperinger.

Udvidet teleoplysning anvendes særligt i sager, hvor et antal ukendte personer, der mistænkes for at have begået en alvorlig forbrydelse, vurderes at have kommunikeret med hinanden umiddelbart før, under 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. Udvidet teleoplysning kan have stor betydning ved efterforskning af grov kriminalitet som f.eks. terror, drab, røveri m.v. og i forbindelse med målrettede eftersøgninger i denne sammenhæng.

Det er på den baggrund Justitsministeriets vurdering, at politiet og anklagemyndigheden fortsat i videst muligt omfang bør have adgang til registrerede og opbevarede trafikdata inden for rammerne af EU-retten, herunder særligt La Quadrature du Net-dommen. Justitsministeriet finder imidlertid i lyset af dommens præmis 166, at der er behov for, at reglerne om adgang til oplysninger ved indgreb i meddelelseshemmeligheden og edition ændres.

La Quadrature du Net-dommen aktualiserer efter Justitsministeriets opfattelse et behov for at foretage en nærmere vurdering af, hvad der i national

ret må betegnes som »grov kriminalitet« i relation til udlevering af trafik- og lokaliseringsdata, som defineret af Domstolen.

Justitsministeriet har noteret sig, at EU-Domstolen i La Quadrature du Net-dommen ikke præciserer, hvad der skal forstås ved »grov kriminalitet« eller »den nationale sikkerhed«. Der må derfor efter Justitsministeriets opfattelse tilkomme medlemsstaterne et vist skøn med hensyn til, hvordan disse begreber skal forstås. Dette skøn vil skulle udøves under hensyntagen til de forpligtelser, der følger af EU-traktatens artikel 4, stk. 3, om loyalt samarbejde, herunder navnlig at EU-retlige forpligtelser, ikke må stilles dårligere end tilsvarende, national ret (ækvivalensprincippet), og at EU-retlige forpligtelser i alle tilfælde, skal gennemføres effektivt (effektivitetsprincippet).

Efter Justitsministeriets opfattelse kan lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, tk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, eller krænkelser eller overtrædelser som omfattet af retsplejelovens § 781, stk. 2 eller 3, anses for grov kriminalitet.

Justitsministeriet mener desuden, at overtrædelser, der kan medføre straf-forhøjelse efter straffelovens § 81 a må betragtes som grov kriminalitet, hvis de begås under sådanne omstændigheder, at § 81 a kan bringes i anvendelse. Efter § 81 a, stk. 1, kan den straf, der er foreskrevet i straffeloven § 119, § 123, § 192 a og § 244, § 244, jf. § 247, § 245, § 245, jf. § 247, § 246, jf. § 245, § 246, jf. § 245, jf. § 247, § 252, stk. 1, § 260, stk. 1, § 261, stk. 1 og 2, § 266, § 285, stk. 1, jf. § 281, § 286, stk. 1, jf. § 281, og § 288, forhøjes indtil det dobbelte, hvis lovovertrædelser har baggrund i eller er egnet til at fremkalde en konflikt mellem grupper af personer, hvor der som led i konflikten enten anvendes skydevåben eller anvendes våben eller eksplosivstoffer, som på grund af deres særdeles farlige karakter er egnet til at forvolde betydelig skade, eller begås brandstiftelse omfattet af denne lovs § 180. Mange af disse forbrydelser vil i forvejen have en strafferamme med et maksimum på 3 års fængsel eller derover, men bestemmelsen vil være relevant eksempelvis ved overtrædelser af § 260 (ulovlig tvang). Justitsministeriet har ved vurderingen lagt vægt på, at § 81 a omfatter nogle meget kvalificerede omstændigheder, hvor lovovertrædelser måske isoleret set ikke er så alvorlig, men kan være med til at fremkalde eller opretholde farlige situationer, f.eks. bandekonflikter, hvor der anvendes skydevåben el. lign.

Kriminalitetskravet vil gælde ved adgang til alle oplysninger, der er registreret og opbevaret i medfør af de foreslåede forpligtelser til generel og udifferentieret registrering og opbevaring af trafikdata og til målrettet registrering og opbevaring af trafikdata (pkt. 3.1, 3.4 og 3.2). Kravet vil endvidere gælde ved adgang til alle oplysninger, der er hastesikret efter de foreslåede regler om hastesikring (pkt. 3.5).

Det foreslåede kriminalitetskrav vil i nogle tilfælde indebære en lempelse i forhold til, hvad der gælder for teleoplysning og udvidet teleoplysning i dag, mens der vil være tale om et skærpet kriminalitetskrav for så vidt angår pålæg om edition. Dette skal ses i lyset af behovet for en ensrettet regulering af registrerings- og opbevaringspligtige oplysninger og EU-Domstolens dertilhørende krav om grov kriminalitet.

Justitsministeriet har ved vurderingen af det foreslåede kriminalitetskrav lagt vægt på karakteren af de lovovertrædelser, der vil falde inden for ordningen, og som bl.a. indebærer, at de fleste lovovertrædelser i straffelovens kapitel 25 (seksualforbrydelser) og kapitel 26 (forbrydelser mod liv og lemme) vil være omfattet af adgangen til loggede oplysninger. Der henvises til pkt. 3.7.3.3 og 3.7.4 og til de specielle bemærkninger til lovforslagets § 1, nr. 2 og 4. Der er således efter Justitsministeriets opfattelse tale om lovovertrædelser, der i almindelighed vil have en sådan grovhed, at pligt til registrering og opbevaring samt anvendelsen heraf må anses for proportional.

Et kriminalitetskrav på mere end 3 år vil medføre, at lovovertrædelser som eksempelvis vold (straffelovens § 244, stk. 1), psykisk vold (straffelovens § 243) og videregivelse af private oplysninger m.v. under skærpende omstændigheder (straffelovens § 264 d, stk. 2), ikke vil være medtaget.

Ligeledes indebærer et kriminalitetskrav på 3 år, at tyveri (straffelovens § 276) og indbrudstyveri (straffelovens § 276 a) falder uden for, medmindre der er tale om tyveri og indbrudstyveri af særlig grov beskaffenhed. Det samme gør sig gældende for narkotikakriminalitet omfattet af lov om euforiserende stoffer, uden at lovovertrædelserne samtidig er omfattet af straffelovens § 191.

Det bemærkes desuden, at lovovertrædelser, der har en strafferamme på mere end 2 år, efter fast praksis optages i straffeloven, der regulerer de groveste lovovertrædelser. Et kriminalitetskrav på 3 år vil derfor ligge over,

hvad der sædvanligvis kræves for at en lovovertrædelse optages i straffeloven i stedet for særlovgivningen. Kravet vil dermed medføre, at speciallovsovertrædelser kun sjældent vil blive omfattet af ordningen.

Endelig skal det bemærkes, at et kriminalitetskrav på 3 år eller derover svarer til, hvad der gælder i artikel 2, stk. 2, i Rådets rammeafgørelse nr. 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurene for overgivelse mellem medlemsstaterne. Efter denne bestemmelse kan en række nærmere angivne kategorier af lovovertrædelser medføre fuldbyrdelse på grundlag af en europæisk arrestordre uden kontrol af dobbelt strafbarhed, hvis lovovertrædelserne kan straffes med frihedsstraf af en maksimal varighed på mindst 3 år.

Udover ved efterforskning af lovovertrædelser, der kan straffes med fængsel i 3 år eller derover, skal adgang til registrerings- og opbevaringspligtige oplysninger også kunne ske såfremt betingelserne i § 781 i øvrigt er opfyldt, eksempelvis hvis der er tale om en efterforskning efter straffelovens kapitel 12 eller 13 eller en af de krænkelser eller overtrædelser, der er særskilt fremhævet i § 781, stk. 1, 2 eller 3, da der her er tale om krænkelser eller overtrædelser, hvor der er et særligt behov for adgang til at kunne få adgang til registrerede og opbevarede oplysninger. Der henvises til pkt. 3.7.1.2.2. Det er Justitsministeriets opfattelse, at en sådan regel opfylder kravene i EU-Domstolens dom i La Quadrature du Net-sagen.

Justitsministeriet har herved også lagt vægt på, at registrering og opbevaring i medfør af den foreslåede ordning kun vil kunne ske på baggrund af vurderinger af den aktuelle trussel mod den nationale sikkerhed, mod personer, der konkret er dømt for grov kriminalitet eller har været genstand for visse tvangsindgreb, mod områder, hvor det konkret er vurderet, at der er en forhøjet risiko for, at det begås eller planlægges grov kriminalitet, eller at der er tale om et særligt sikringskritisk område, eller på baggrund af konkrete vurderinger af behovet for registrering rettet mod en bestemt person eller et bestemt område med forbindelse til grov kriminalitet (konkret begrundede pålæg). Ordningen vil derfor, alt andet lige, være mindre indgribende, end det er tilfældet i dag.

Herudover bemærkes det, at der lægges op til, at politiet og anklagemyndigheden vil have adgang til registrerings- og opbevaringspligtige oplysninger, der er registreret og opbevaret efter den foreslåede forpligtelse til generel og udifferentieret registrering og opbevaring med henblik på at beskytte den

ationale sikkerhed, i de tilfælde, hvor politiet og anklagemyndigheden bekæmper grov kriminalitet. Dette vurderes at medføre en væsentlig procesrisiko i lyset af præmis 166 i La Quadrature du Net-dommen, jf. pkt. 3.7.2. Det bemærkes, at denne procesrisiko ikke vurderes at være til stede, hvor myndighederne gives adgang til data, der er registreret og opbevaret som følge af den foreslåede forpligtelse til målrettet registrering og opbevaring af trafikdata med henblik på at bekæmpe grov kriminalitet.

Det bemærkes desuden, at det er Justitsministeriets opfattelse, at La Quadrature du Net-dommen – udover for så vidt angår hastesikring (præmis 160 ff.) – alene regulerer data, der gøres registrerings- og opbevaringspligtige i medfør af regler, der udformes på baggrund af artikel 15, stk. 1, i direktiv nr. 2002/58. På den baggrund foreslås det, at lovforslaget ikke vil regulere adgang til ikke-registrerings- og opbevaringspligtige oplysninger som f.eks. allerede registreret lokaliseringsdata, jf. pkt. 3.1.3.4 og 3.2.3.3, hvorfor de gældende regler om adgang vil finde anvendelse for sådanne oplysninger. Det vil bl.a. indebære, at adgang til sådanne oplysninger ikke vil være betinget af, at der er tale om efterforskning m.v. af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed. Det forudsættes i den forbindelse, at udbydere af elektroniske kommunikationsnet eller -tjenester i forbindelse med anmodninger fra politiet om udlevering af ikke-registrerings- og opbevaringspligtige oplysninger, der ikke er omfattet af kriminalitetskravet, alene udleverer sådanne oplysninger.

3.7.3.2. Indgreb i meddelelshemmeligheden

Retsplejelovens regler om teleoplysning og udvidet teleoplysning kan bruges til at give adgang til trafikdata, sådan som dette er defineret i e-databeskyttelsesdirektivets artikel 2, stk. 2, litra b, dvs. data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf. Der henvises til pkt. 3.7.1.2. Det følger af EU-Domstolens afgørelse i La Quadrature du Net-dommen, som beskrevet i pkt. 3.7.2, at der kun må gives adgang til registrerings- og opbevaringspligtige oplysninger, når udlevering er begrundet i efterforskning af grov kriminalitet, herunder den nationale sikkerhed.

Justitsministeriet har overvejet, om La Quadrature du Net-dommen giver anledning til at ændre reglerne om teleoplysning og udvidet teleoplysning, for så vidt angår adgang til oplysninger, som teleselskaberne er pålagt at registrere.

Ved indgreb i meddelelshemmeligheden gælder der allerede i dag som udgangspunkt et strengt kriminalitetskrav. Efterforskningen skal således angå en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, eller en overtrædelse af straffelovens kapitel 12 eller 13. Et strafferammekrav på 6 års fængsel eller derover må efter Justitsministeriets klare opfattelse med sikkerhed antages at opfylde betingelsen om, at indgrebet alene anvendes i relation til efterforskningen af »grov kriminalitet«.

Justitsministeriet finder på baggrund af det under pkt. 3.7.3.1 anførte, at det for så vidt angår teleoplysning og udvidet teleoplysning findes hensigtsmæssigt og proportionalt at sænke kriminalitetskravet til 3 år for så vidt angår oplysninger, der er registrerings- og opbevaringspligtige.

Dertil kommer, at indgreb i meddelelshemmeligheden kan ske, hvis efterforskningen angår en række specifikke straffelovsbestemmelser og en række lovovertrædelser oplistet i udlændingeloven. Justitsministeriet vurderer også for disse bestemmelser, at grovhedskriteriet er opfyldt. Der er bl.a. tale om grove trusler, udbredelse og besiddelse af børneporno og afpresning.

Det er endvidere Justitsministeriets opfattelse, at en lovovertrædelse, der er omfattet af straffelovens kapitel 12 eller 13, er at anse som en lovovertrædelser, der angår den nationale sikkerhed.

For så vidt angår de lovovertrædelser, der er særskilt oplistet i retsplejelovens § 781, stk. 1-3, skal Justitsministeriet bemærke, at der er tale om lovovertrædelser, der kan være vanskelige at efterforske, hvis ikke der er adgang til at foretage indgreb i meddelelshemmeligheden, eller at indgreb i meddelelshemmeligheden er et relevant eller hensigtsmæssigt efterforskningsmiddel. Der henvises til pkt. 3.7.1.2.

For så vidt angår overtrædelser af straffelovens § 293, bemærkes endvidere, at indgreb i meddelelshemmeligheden er begrænset til teleoplysning, og at indgrebet kun kan foretages, hvis mistanken angår lovovertrædelser, der er begået ved anvendelse af en telekommunikationstjeneste, jf. retsplejelovens § 781, stk. 3, nr. 2. Der henvises i øvrigt til pkt. 3.7.1.2.

Særligt for reglerne i retsplejelovens § 781, stk. 3, nr. 3-5, skal Justitsministeriet bemærke, at der er tale om regler, der implementerer EU-lovgivning, der forpligter medlemsstaterne til at indføre regler om udlevering af datatrafik. Der henvises til pkt. 3.7.1.2.

For så vidt angår lovovertrædelserne i retsplejelovens § 781, stk. 3, nr. 3 og 5, henviser markedsmisbrugsforordningens artikel 3, nr. 27, til, at »fortegnelser over datatrafik« skal forstås som fortegnelser over trafikdata i e-databeskyttelsesdirektivets artikel 2, stk. 2, litra b, og det fremgår endvidere af betragtning 65 i markedsmisbrugsforordningens præambel, at de oplysninger, der kan kræves udleveret, bl.a. fortegnelser over datatrafik, er yderst vigtigt som bevismateriale i sager om markedsmisbrug.

Uanset at tilsvarende bemærkninger ikke er fremhævet i præamblen til REMIT-forordningen, må de tilsvarende hensyn efter Justitsministeriets opfattelse gøre sig gældende i forhold til de i retsplejelovens § 781, stk. 3, nr. 4, omhandlede overtrædelser af denne forordning, da der er tale om et forbud mod insiderhandel (artikel 3, stk. 1) og et forbud mod markedsmåned (artikel 5), dvs. lovovertrædelser lig dem, der omhandles i retsplejelovens § 781, stk. 3, nr. 3 og 5.

I forhold til retsplejelovens § 781, stk. 3, nr. 3-5, skal Justitsministeriet endvidere bemærke, at det fremgår af betragtning nr. 77 i markedsmisbrugsforordningens præambel samt af betragtning nr. 24 i REMIT-forordningens præambel, at forordningerne respekterer og overholder EU's charter om grundlæggende rettigheder.

Justitsministeriet bemærker endvidere, 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 i pkt. 3.7.1.2 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.

I den forbindelse vil de danske domstole også skulle foretage en afvejning af hensynet til at få udleveret oplysninger til brug for efterforskning af straffesager over for brugernes krav på hemmeligholdelse, sådan som dette er sikret i e-databeskyttelsesdirektivet og i EU's charter om grundlæggende rettigheder.

Særligt i forhold til udvidet teleoplysning skal det fremhæves, at dette indgreb kun kan foretages, når mistanken vedrører en forbrydelse, som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier, jf. retsplejelovens § 781, stk. 5, 1. pkt.

3.7.3.3. Edition

3.7.3.3.1. Generelt

Retsplejelovens regler om edition kan bl.a. anvendes til at få udleveret trafikdata samt oplysninger om brugeridentitet.

Det lægges i EU-Domstolens afgørelse i La Quadrature du Net-dommen, som beskrevet i pkt. 3.7.2, til grund, at registrerings- og opbevaringspligtige oplysninger kun må udleveres, når udlevering er begrundet i efterforskning af grov kriminalitet, herunder den nationale sikkerhed.

Justitsministeriet har overvejet, om La Quadrature du Net-dommen giver anledning til at ændre retsplejelovens regler om edition for så vidt angår adgang til registrerings- og opbevaringspligtig trafikdata eller oplysninger om brugeridentitet.

Efter retsplejelovens § 804 gælder der for pålæg om edition som led i efterforskningen af en lovovertrædelse alene et krav om, at forholdet skal være undergivet offentlig påtale, eller udgøre en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning.

Reglerne om edition kan således anvendes på en bred og ikke på forhånd specificeret kreds af overtrædelser af såvel straffeloven som særlovgivningen.

Henset til den brede kategori af lovovertrædelser, der efter gældende ret kan danne grundlag for edition, er det Justitsministeriets vurdering, at der i lyset af EU-Domstolens dom i La Quadrature du Net-dommen er behov for at begrænse adgangen til at meddele pålæg om edition af registrerings- og opbevaringspligtige oplysninger, således at sådanne pålæg kun kan meddeles

som led i efterforskningen af grov kriminalitet, herunder ud fra hensynet til den nationale sikkerhed.

Dette skal ses i lyset af det ovenfor anførte om, at det er Justitsministeriets opfattelse, at La Quadrature du Net-dommen – udover for så vidt angår hastesikring (præmis 160 ff.) – alene regulerer data, der gøres registrerings- og opbevaringspligtige i medfør af regler, der udformes på baggrund af artikel 15, stk. 1, i direktiv nr. 2002/58.

Justitsministeriet finder, at editionsreglerne for registrerings- og opbevaringspligtige oplysninger bør udformes, så de har samme rækkevide i relation til kriminalitetskravet som den i pkt. 3.7.3.2 skitserede regel vedrørende adgang til registrerings- og opbevaringspligtige oplysninger efter reglerne om indgreb i meddelelseshemmeligheden.

Justitsministeriet finder, at dette bedst kan ske ved indsættelsen af en ny bestemmelse i retsplejelovens kapitel 74, der supplerer de nugældende editionsregler i forhold til registreringspligtige oplysninger.

Politiet vil efter forslaget fortsat kunne få adgang til ikke-registrerings- og opbevaringspligtige oplysninger samt dynamiske IP-adresser mv. efter de gældende regler om edition, dvs. uden at der stilles krav om, at politiet skal anvende oplysningerne til bekæmpelse af grov kriminalitet, herunder beskyttelse af den nationale sikkerhed.

3.7.3.3.2. Telelovens § 13

Det følger af den gældende bestemmelse i telelovens § 13, at udbydere af elektroniske kommunikationsnet eller -tjenester på begæring af politiet skal udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester, jf. pkt. 3.7.1.5.

Bestemmelsen omtaler 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 fremgår netop af forarbejderne til telelovens § 13, at der vil kunne opstå nye typer af oplysninger, der kan betegnes som oplysninger om en slutbrugers adgang til kommunikationsnet eller -tjenester, og som kan tjene til at identificere en bestemt slutbruger.

Det er derfor efter Justitsministeriets opfattelse nødvendigt at ændre bestemmelsen for at tage højde for den varierende praksis hos udbydere af elektroniske kommunikationsnet eller -tjenester med hensyn til, om udlevering af oplysninger knyttet til et IMEI-nummer forudsætter editionskendelse.

Indhentelse af oplysninger om, hvilke mobiltelefoner m.v. 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. Efterforskningsskridtet anvendes bl.a. til helt indledningsvis at fastlægge en mulig sammenhæng mellem fysiske personer og kommunikationsenheder. Hvis dette er tilfældet, iværksættes indgrebet i overensstemmelse med retsplejelovens regler på baggrund af enten forudgående retskendelse eller på øjemedet, efterfulgt af rettens kendelse.

Politiet, der kender et telefonnummer, vil typisk anmode udbyderne af elektroniske kommunikationsnet eller -tjenester om at oplyse nærmere om aktiviteten på knyttet til dette telefonnummer i en given periode.

Det foreslås, at det fastsættes entydigt, at udbyderen af elektroniske kommunikationsnet eller -tjenester i den forbindelse på politiets begæring skal oplyse, hvilke IMEI-numre der f.eks. har været knyttet til et konkret telefonnummer, jf. nærmere herom nedenfor. Disse IMEI-numre vil derefter blive sendt retur til udbyderne af med henblik på at fastslå, om det er tilknyttet andre telefonnumre. Dette er særligt relevant i de tilfælde, hvor skifter mellem flere SIM-kort.

Hvis politiet omvendt kender IMEI-nummeret, vil udbyderne af elektroniske kommunikationsnet eller -tjenester blive anmodet om at oplyse tilknyttede telefonnumre.

Ved at flytte bestemmelsen til retsplejeloven skabes der ensretning og transparens på området for indhentning af oplysninger fra udbyderne af elektroniske kommunikationsnet eller -tjenester til slutbrugere.

Det foreslås på den baggrund, at telelovens § 13 nyaffattes og overflyttes til retsplejeloven i den foreslåede § 804 b, så der skabes en klar hjemmel til, at

udbydere af elektroniske kommunikationsnet eller -tjenester – i overensstemmelse med EU-Domstolens praksis – kan pålægges at udlevere basale oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester til politiet.

Fælles for de oplysninger, der efter lovforslaget tilsigtes omfattet af den foreslåede bestemmelse i retsplejelovens § 804 b, er, at forpligtelsen omfatter udlevering af den fulde oplysning, f.eks. det komplette IMEI-, IMSI- og telefonnummer, uden maskering af et eller flere cifre i det angivne nummer.

Den foreslåede bestemmelse vil fortsat ikke give politiet hjemmel til efter begæring at få oplyst af udbyderne, hvor mange gange og hvornår et IMEI- eller telefonnummer har foretaget aktiviteter på udbydernes net.

Det bemærkes, at den nuværende bestemmelse i telelovens § 13 ikke finder anvendelse på oplysninger, som udbyderne alene ligger inde med som følge af registrerings- og opbevaringspligten i den gældende § 786, stk. 4, i retsplejeloven, idet disse skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven.

Den foreslåede bestemmelse vil videreføre dette udgangspunkt for så vidt angår de nye foreslåede regler om registrering og opbevaring. Derfor vil det være en forudsætning for, at udbyderne skal udlevere en given oplysning efter den foreslåede § 804 b i retsplejeloven, at udbyderne af elektroniske kommunikationsnet eller -tjenester ikke alene ligger inde med oplysningen som følge af registrerings- og opbevaringspligten i de foreslåede §§ 786 a-786 f.

For IP-adresser bemærkes, at bestemmelsen alene omfatter statiske oplysninger, hvis de opfylder betingelserne i bestemmelsen, idet registrering af dynamiske IP-adresser m.v. vil ske i medfør af registreringsforpligtelsen i den foreslåede § 786 f. Udlevering af dynamiske IP-adresser m.v. registeret efter den foreslåede § 786 f vil skulle ske efter retsplejelovens § 804 om edition.

Bestemmelsen foreslås udformet teknologineutralt, således at det eksempelvis også vil kunne omfattes af bestemmelsen, 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 m.v., eller et mobilabonnement.

På teknologiens nuværende stadie vil oplysningerne navnlig omfatte IMEI-nummer, IMSI-nummer og telefonnummer.

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 fremover kun vil kunne anvendes til brug for politiets forebyggelse, efterforskning m.v. af straffelovsovertrædelser, men ikke til politiets øvrige opgavevaretagelse.

Denne indsnævring i anvendelsesområdet er begrundet i behovet for at bringe bestemmelsen i fuld overensstemmelse med EU-Domstolens praksis, herunder dommen af 2. oktober 2018, Ministerio Fiscal, hvor EU-Domstolen fastslog, 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 og retsforfølgning af ”straffelovsovertrædelser” generelt.

På den baggrund foreslås det, at udlevering vil kunne ske med henblik på forebyggelse, efterforskning og retsforfølgning af strafbare forhold. Denne ændring foreslås indført med et krav om, at politiets begæring skal ske som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning.

Det foreslås endeligt, at adgangen til at påklage politiets begæring efter bestemmelsen inden for strafferetsplejen også fremover skal følge den ordning, der er fastsat i retsplejelovens § 101, stk. 2, hvorefter statsadvokaterne behandler klager over afgørelser truffet af politidirektørerne vedrørende strafforfølgning.

I medfør af den gældende telelovs § 81, stk. 1, nr. 1, kan der pålægges bødestraf for overtrædelse af bl.a. telelovens § 13. Det foreslås, at der ligeledes for den foreslåede § 804 b i retsplejeloven skal kunne pålægges udbyderen

en straf. Det foreslås på den baggrund, at en overtrædelse af bestemmelsen kan straffes med bøde.

3.7.3.3.3. Advokatbeskikkelse i sager om edition

Der gælder ikke i dag en almindelig pligt til at underrette den person, hvis oplysninger har været genstand for registrering og opbevaring, hvis politiet begærer edition af oplysningerne. Personen har desuden ingen almindelig adgang til at komme med en udtalelse, før retten træffer afgørelse om spørgsmålet. En sådan pligt vil efter gældende ret kun eksistere, hvis vedkommende er sigtet og repræsenteret af en forsvarer. Der henvises til omtalen af disse regler i pkt. 3.7.1.4.

Dette er forskelligt fra, hvad der gælder vedrørende indgreb i meddelelseshemmeligheden, hvor der vil blive beskikket en advokat for den, som indgrebet angår, jf. retsplejelovens §§ 784-785. Efter indgrebet er afsluttet, vil der skulle ske underretning om indgrebet, jf. retsplejelovens § 788, stk. 1-3, medmindre der er grundlag for at undlade underretningen, jf. bestemmelsens stk. 4.

Det er Justitsministeriets opfattelse, at den person, hvis oplysninger er genstand for en registrerings og opbevaringspligt, bør have samme mulighed for at få varetaget sine interesser, når politiet får adgang til oplysningerne, hvad enten denne adgang sker efter reglerne om indgreb i meddelelseshemmeligheden eller efter reglerne om edition. Justitsministeriet har herved lagt vægt på, at der med den foreslåede ordning vil gælde det samme kriminalitetskrav for pålæg om udlevering af registrerings- og opbevaringspligtige oplysninger, hvad enten pålægget meddeles efter reglerne om indgreb i meddelelseshemmeligheden eller reglerne om edition.

Det foreslås derfor, at der fastsættes regler, der gør retsplejelovens §§ 784 og 785 samt § 788 anvendelige også i den situation, hvor adgangen til registrerings- og opbevaringspligtige oplysninger sker efter reglerne om edition.

3.7.4. Den foreslåede ordning

3.7.4.1. Indgreb i meddelelseshemmeligheden og edition

Det foreslås, at der i retsplejeloven indføres en ny § 804 a, der fastslår, at pålæg om udlevering af registrerings- og opbevaringspligtige oplysninger, jf. de foreslåede bestemmelser i retsplejelovens §§ 786 a – 786 e, kun kan finde sted, hvis efterforskningen angår lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af

straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, tk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, eller krænkelser eller overtrædelser som omfattet af retsplejelovens § 781, stk. 2 eller 3 eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Det foreslås videre, at der indføres en ny § 781 a i retsplejeloven, hvorefter pålæg om udlevering af registreringspligtige oplysninger i form af teleoplysning, jf. § 780, stk. 1, nr. 3, og udvidet teleoplysning, jf. § 780, stk. 1, nr. 4, uanset kriminalitetskravet i § 781, stk. 1, nr. 3, kan meddeles, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a. Den foreslåede § 781 a i retsplejeloven medfører en lempelse af kriminalitetskravet for udlevering af registrerings- og opbevaringspligtige oplysninger.

Den foreslåede § 781 a i retsplejeloven vil sammen med den gældende § 781, stk. 1, nr. 3, medføre, at der vil gælde samme kriminalitetskrav for udlevering af registrerings- og opbevaringspligtige oplysninger, hvad enten pålægget om udlevering sker efter reglerne om edition, jf. den foreslåede § 804 a, eller reglerne om teleoplysning eller udvidet teleoplysning, jf. den foreslåede § 781 a.

De foreslåede bestemmelser i § 781 a og § 804 a i retsplejeloven skal kun anvendes i forhold til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser (registrerings- og opbevaringspligtige oplysninger). Pålæg om udlevering af oplysninger, som udbyderne af elektroniske kommunikationsnet eller -tjenester er i besiddelse af, uden at der består en pligt til at foretage registrering og opbevaring, vil ikke være omfattet af de foreslåede bestemmelser i retsplejelovens § 781 a og § 804 a. Sådanne oplysninger vil kunne kræves udleveret efter de almindelige regler om indgreb i meddelelshemmeligheden, edition eller telelovens § 13, der foreslås videreført i retsplejeloven, jf. pkt. 3.7.4.2 nedenfor, hvis betingelserne herfor i øvrigt er opfyldt.

De foreslåede §§ 781 a og 804 a i retsplejeloven vil i praksis omfatte registrerede trafikdata. Der henvises til pkt. 3.1.3.4, 3.2.3.3 og 3.3.3.

De foreslåede bestemmelser i § 781 a og § 804 a i retsplejeloven indeholder alene et særligt kriminalitetskrav for så vidt angår adgang til registrerings- og opbevaringspligtige oplysninger. De almindelige betingelser, herunder begrænsninger, for at kunne foretage indgreb i meddelelseshemmeligheden og for at meddele pålæg om edition gælder ved siden af de foreslåede bestemmelser. Indikations- og mistankekravene i hhv. retsplejelovens § 781, stk. 1, nr. 1 og 2, samt § 804, stk. 1, skal således stadig være opfyldt ved anvendelse af de foreslåede bestemmelser i § 781 a og § 804 a. For så vidt angår udvidet teleoplysning, vil pålæg om udlevering af oplysninger efter den foreslåede § 781 a tillige forudsætte, at mistanken vedrører en forbrydelse, som har medført eller kan medføre fare for menneskers liv eller velvære eller for betydelige samfundsværdier, jf. § 781, stk. 5, 1. pkt. Der henvises til gennemgangen i pkt. 3.7.1.2-3.7.1.4.

De foreslåede bestemmelser i § 781 a og § 804 a i retsplejeloven vil være undergivet de almindelige regler om proportionalitet, der gælder for indgreb i meddelelseshemmeligheden og for edition, jf. hhv. retsplejelovens § 782 og § 805. Indgrebene vil, som det i dag er tilfældet, efter gældende ret kun kunne foretages efter forudgående retskendelse, medmindre øjemedet ellers ville forspildes, jf. hhv. retsplejelovens § 783 og § 806. Tilsvarende vil retten som efter gældende ret på begæring fra politiet kunne træffe afgørelse om udlevering af oplysninger, hvis der er givet samtykke, jf. retsplejelovens § 786, stk. 2.

Ligesom i dag vil domstolene skulle foretage en afvejning af hensynet til at få udleveret oplysninger til brug for efterforskning af grov kriminalitet over for brugernes krav på hemmeligholdelse, sådan som dette er sikret i e-data-beskyttelsesdirektivet og i EU's charter om grundlæggende rettigheder, over for, jf. Østre Landsrets kendelse af 7. maj 2018 i sag nr. B-2451-17 og B-2458-17, gengivet i *Ugeskrift for Retsvæsen 2019*, s. 2019 ff., jf. pkt. 3.7.1.4.

For indgreb efter den foreslåede § 781 a i retsplejeloven vil gælde, at der også som i dag skal beskikkes en indgrebsadvokat, jf. retsplejelovens § 784, og at der vil skulle gives underretning efter reglerne herom i retsplejelovens § 788. Der henvises til pkt. 3.7.1.2.

For indgreb efter den foreslåede § 804 a i retsplejeloven vil gælde, at den, som pålægget retter sig mod (teleudbyderen), som i dag vil få mulighed for at udtale sig, inden retten træffer afgørelse, hvis ikke der er truffet afgørelse efter § 748, stk. 5 og 6, jf. retsplejelovens § 806, stk. 9. En evt. forsvarer i

sagen vil ligesom i dag skulle indkaldes til retsmødet, hvor der tages stilling til editionsspørgsmål efter den foreslåede § 804 a i retsplejeloven, jf. lovens § 748, stk. 2. Lovens § 804, stk. 1, 2. pkt., og henvisningen til § 189 vil også finde anvendelse på editionspålæg, der er omfattet af den foreslåede § 804 a. Der vil derfor som efter gældende ret kunne meddeles tavshedspligt efter retsplejelovens § 189 også for editionspålæg omfattet af § 804 a. Der henvises til pkt. 3.7.1.3.

Det foreslås endvidere, at der i retsplejelovens § 806 indsættes et nyt stk. 10, der gør lovens §§ 784, 785 og 788 anvendelige i forhold til den, som de registrerede og opbevarede oplysninger, der er genstand for edition, angår.

Formålet med denne ændring er at give den, som oplysningerne angår, samme retsstilling og mulighed for at få varetaget sine interesser, som hvis politiets adgang til de registrerede og opbevarede oplysninger var sket efter retsplejelovens regler om indgreb i meddelelshemmeligheden. Henvisningen til retsplejelovens §§ 784 og 785 vil indebære, at der skal beskikkes en advokat for vedkommende. Henvisningen til § 788 vil medføre, at reglerne om underretning finder anvendelse.

Der henvises til pkt. 3.6.3.2 vedrørende domstolsprøvelse af målrettet registrering og opbevaring af trafikdata på baggrund af konkret begrundede pålæg, hvor reglernes anvendelse i relation til pålæg om registrering og opbevaring af oplysninger er beskrevet.

Når der i medfør af de foreslåede bestemmelser er truffet beslutning om pålæg om udlevering af oplysninger, vil vedkommende teleselskab m.v. således være forpligtet til at udlevere de omhandlede oplysninger. Udlevering af oplysninger til politiet for at efterkomme et sådant pålæg vil efter Justitsministeriets vurdering være i overensstemmelse med databeskyttelsesforordningens behandlingsbetingelser, jf. herved artikel 6, stk. 1, litra c, hvorefter der kan videregives personoplysninger, når det er nødvendigt for at overholde en retlig forpligtelse. Efter Justitsministeriets vurdering vil dette endvidere være i overensstemmelse med de grundlæggende behandlingsprincipper i forordningens artikel 5, herunder principperne om lovlighed og formålsbegrænsning.

Der henvises i øvrigt til de specielle bemærkninger til lovforslagets § 1, nr. 1 og 2 samt nr. 12 og 13.

3.7.4.2. *Telelovens § 13*

Det foreslås, at der i retsplejeloven indføres en ny § 804 b, der fastslår, at politiets begæring om udlevering af oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester, kun kan finde sted, hvis efterforskningen vedrører en lovovertrædelse, der er undergivet offentlig påtale, eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning.

Oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester, omfatter oplysninger, der knytter sig til identifikation af brugeren, eksempelvis navn, telefonnummer, et bestemt IMEI-nummer, et bestemt IMSI-nummer m.v. Sådanne oplysninger vil således kunne udleveres i medfør af bestemmelsen.

Oplysninger om brugeridentitet, hvis disse oplysninger er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, vil politiet kun kunne begære udleveret efter den foreslåede bestemmelse i retsplejelovens § 804 b, hvis udbyderen måtte være i besiddelse af oplysningerne på andet grundlag end de foreslåede pligter til registrering og opbevaring. Oplysninger, som udbyderne alene ligger inde med som følge af en registrerings- eller opbevaringspligt, kan derfor ikke udleveres efter den foreslåede bestemmelse, jf. § 804 b, stk. 2.

Pålæg om edition af oplysninger om brugeridentitet vil fortsat kunne meddeles efter den almindelige regel i retsplejelovens § 804, uanset at disse oplysninger er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser. Det vil sige oplysninger om, hvilken bruger der er indehaver af et bestemt telefonnummer, et bestemt IMEI-nummer, et bestemt IMSI-nummer m.v. Statiske og dynamiske IP-adresser m.v. vil kunne udleveres efter retsplejelovens § 804, men alene statiske IP-adresser er omfattet af den foreslåede § 804 b, hvis de desuden opfylder kravene i bestemmelsen.

Det foreslås, at der i det foreslåede § 804 b i retsplejeloven indsættes en bestemmelse, der fastslår, at en overtrædelse af bestemmelsen kan medføre en bøde. Dermed vil bestemmelsen fortsat være strafbelagt, ligesom telelovens § 13 også er det i dag i medfør af telelovens § 81, stk. 1, nr. 1.

For så vidt angår forholdet til databeskyttelsesforordningen henvises til det ovenfor under pkt. 3.7.4.1 anførte, som finder tilsvarende anvendelse for udlevering efter den foreslåede § 804 b i retsplejeloven.

3.8. Ændring af telelovens § 31, stk. 2, om nummeroplysningsdata

3.8.1. Gældende ret

Telelovens § 31, stk. 2, blev indført ved lov nr. 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester. Loven trådte i kraft den 25. maj 2011 og ophævede lov om konkurrence- og forbrugerforhold på telemarkedet, jf. lovbekendtgørelse nr. 780 af 28. juni 2007.

Telelovens § 31 er en uændret videreførelse af § 34 i lov om konkurrence- og forbrugerforhold på telemarkedet, jf. bemærkningerne til § 31 i Folketingstidende 2010-11, tillæg A, L 59 som fremsat.

Det følger af telelovens § 31, stk. 2, at ved nummeroplysningsdata forstås oplysninger om abonnentnumre, der er tildelt slutbrugere, indeholdende navn, adresse, eventuelle oplysninger om stilling, abonnentnummeret og den kategori af tjeneste, abonnentnummeret anvendes til.

Efter telelovens § 31, stk. 3, kan Energistyrelsen fastsætte nærmere regler om minimumskrav til indsamling og videregivelse af nummeroplysningsdata, afgrænsning af kredsen af berettigede til at modtage data, de pågældende datas fremtrædelsesform, opdatering af oplysninger m.v. og omfanget af de forpligtelser, der kan pålægges udbydere af nummeroplysningsdatabaser og -registre over for slutbrugere.

Telelovens § 31, stk. 3, er udmøntet i bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser. Bekendtgørelsen vedrører blandt andet indsamling, registrering og videregivelse af nummeroplysningsdata.

Efter telelovens § 31, stk. 5, nr. 2, skal nummeroplysningsdata altid videregives til forsyningspligtudbyderens landsdækkende nummeroplysnings-tjeneste ("118-databasen"), jf. telelovens § 14, stk. 2, nr. 4.

Det følger af telelovens § 31, stk. 6, at oplysninger som nævnt i § 31, stk. 5, nr. 2, jf. stk. 4 (dvs. oplysninger om hemmelige og udeladte numre), alene kan videregives af forsyningspligtudbyderens landsdækkende nummerop-

lysningstjeneste til brug for offentlige alarmtjenester, politiet, statsadvokaterne, Styrelsen for Patientsikkerhed, de enkelte retter, kriminalforsorgen eller restanceinddrivelsesmyndigheden.

3.8.2. Justitsministeriets overvejelser og den foreslåede ordning

Justitsministeriet har overvejet, hvordan det sikres, at politiet entydigt kan identificere en slutbruger af et givet kommunikationsmiddel, således at det sikres, at der ikke uforvarende sker registrering og opbevaring for forkerte personers trafikdata, og at det sikres, at der af hensyn til bekæmpelse af grov kriminalitet også kan findes frem til de personer, der efter loven kan iværksættes registrering og opbevaring af trafikdata på.

I den forbindelse er det vigtigt, at 118-databasen, som politiet har adgang til, opnår en datakvalitet, der kan understøtte målrettet registrering og opbevaring af trafikdata, således at politiet herigennem entydigt kan identificere den relevante person at iværksætte målrettet registrering og opbevaring på.

Det er derfor efter Justitsministeriets opfattelse nødvendigt, at der foretages en ændring af § 31, stk. 2, i teleloven, som indeholder definitionen af nummeroplysningsdata, således at nummeroplysningsdata, ud over de i forvejen angivne data, også omfatter unikt ID og eventuelle oplysninger om bruger.

Ændringen af definitionen af nummeroplysningsdata skal ses i sammenhæng med den foreslåede bestemmelse i retsplejelovens § 786 h, hvorefter justitsministeren efter forhandling med og klima-, energi- og forsyningsministeren kan fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters registrering og verificering af nummeroplysningsdata. Der henvises til pkt. 3.4.

Bemyndigelsen, jf. den foreslåede § 786 h, forudsættes udnyttet ved en ændring af den i forvejen eksisterende bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, der er udstedt i medfør af telelovens § 31, stk. 3, og som angår indsamling, registrering og videregivelse af nummeroplysningsdata til nummeroplysningsdatabaser, hvorved oplysningerne om slutbrugeren, herunder det unikke ID, vil kunne videregives til 118-databasen.

Formålet er herigennem at sikre, at de oplysninger, som fremgår af 118-databasen, er korrekte, hvilket vurderes sikret bedst muligt ved registrering af unikt ID på slutbrugeren.

Ved et unikt ID forstås CPR-nummer for personer, der er tildelt et sådant, hvis abonnenten udgør en fysisk person. For personer uden CPR-nummer angives i stedet oplysning om fødselsdato, statsborgerskab ved fødslen og køn. Herudover angives for personer uden CPR-nummer et pasnummer eller nummer fra nationalt identitetskort og udstedelsesland for passet eller det nationale identitetskort. Hvis abonnenten udgør en juridisk person angives CVR-nummer. For juridiske personer uden CVR-nummer angives i stedet selskabsregisteret, hvori den juridiske person er registreret, og registreringsnummeret.

Ved eventuelle oplysninger om bruger forstås oplysninger om den fysiske person, der forventes at anvende teletjenesten. Der kan derfor være et overlap mellem slutbrugeren og brugeren, men i flere tilfælde vil slutbrugeren og brugeren ikke være den samme person. Registrering af oplysninger om brugeren vil alene skulle ske i det omfang, det på tidspunktet for registreringen vides, hvem der er den forventede bruger.

Det bemærkes samtidig, at regler om videregivelse af oplysninger om det unikke ID forudsættes udmøntet i bekendtgørelsen om nummeroplysningsdatabaser således, at oplysninger herom kun vil kunne videregives til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste (118-databasen). Med lovændringen tilsigtes der således ikke en generel videregivelse til nummeroplysningsdatabaser af unikke ID, herunder CPR-numre.

3.9. Opbevaring af registrerings- og opbevaringspligtige oplysninger

3.9.1. Gældende ret

Bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester er udstedt med hjemmel i bl.a. telelovens § 8, stk. 1 og 4, og fastsætter regler for opbevaring og behandling af trafik- og lokaliseringsdata. Bekendtgørelsen trådte i kraft den 21. december 2020.

Det fremgår af bekendtgørelsens § 1, stk. 1, nr. 3, at bekendtgørelsen finder anvendelse på opbevaring og behandling af trafik- og lokaliseringsdata i forbindelse med elektronisk kommunikation.

Det fremgår af bekendtgørelsens § 3, stk. 1, at udbydere af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle

kommunikationstjenester løbende skal træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester. Udbydere skal gennem disse foranstaltninger sikre et sikkerhedsniveau, der, under hensyn til teknologiens aktuelle stadie og omkostningerne i forbindelse med gennemførelsen af foranstaltningerne, står i forhold til risici.

Det fremgår af bekendtgørelsens § 3, stk. 2, nr. 1-3, at de foranstaltninger, der er nævnt i stk. 1, som minimum skal 1) sikre, at kun autoriserede personer får adgang til persondata til lovlige formål, 2) beskytte lagrede eller sendte persondata mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse, og 3) gennemføre en sikkerhedspolitik for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Det fremgår af bekendtgørelsens § 12, stk. 1, at Erhvervsstyrelsen fører tilsyn med de foranstaltninger, som udbydere af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester skal træffe efter bekendtgørelsens § 3. Erhvervsstyrelsen fører ligeledes tilsyn med udbydere af offentlige elektroniske kommunikationstjenesters og nummeruafhængige interpersonelle kommunikationstjenesters efterlevelse af bekendtgørelsens §§ 7-11.

Der er imidlertid ikke efter bekendtgørelsen fastsat regler om den geografiske placering af registrerings- og opbevaringspligtige oplysninger.

3.9.2. EU-Domstolens praksis

EU-Domstolens praksis, herunder Tele2-dommen, er beskrevet under pkt. 2.

For så vidt angår krav om opbevaring af trafikdata på servere i EU er den relevante del af Tele2-dommen præmis 122. Det fremgår heraf navnlig følgende:

”122. Hvad angår reglerne om sikkerheden vedrørende og beskyttelsen af de data, der lagres af udbydere af elektroniske kommunikationstjenester, bemærkes, at artikel 15, stk.

1, i direktiv 2002/58 ikke gør det muligt for medlemsstaterne at fravige direktivets artikel 4, stk. 1 eller stk. 1a. De sidstnævnte bestemmelser opstiller et krav om, at disse udbydere træffer passende tekniske og organisatoriske foranstaltninger, der gør det muligt at sikre en effektiv beskyttelse af de lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til disse data. Henset til mængden af lagrede data, den følsomme karakter af disse data og risikoen for ulovlig adgang til disse skal udbyderne af elektroniske kommunikationstjenester med henblik på at sikre de pågældende datas fulde integritet og fortrolighed sikre et særligt højt niveau for beskyttelse og sikkerhed gennem passende tekniske og organisatoriske foranstaltninger. Særligt skal den nationale lovgivning foreskrive en lagring på EU's område og en irreversibel destruktion af disse data ved udløbet af lagringsperioden (jf. analogt for så vidt angår direktiv 2006/24 Digital Rights-dommen, præmis 66-68).”

3.9.3. Justitsministeriets overvejelser og den foreslåede ordning

Der er ikke efter gældende ret regler om, hvor registrerings- og opbevaringspligtige oplysninger skal opbevares, herunder om de skal opbevares på servere inden for EU.

På baggrund af EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15 (Tele2-dommen), er det Justitsministeriets opfattelse, at det er nødvendigt at indføre national lovgivning, hvorved det er muligt at fastsætte nærmere regler om, hvordan oplysninger registreret som følge af de foreslåede §§ 786 a-786 f i retsplejeloven eller pålæg eller regler udstedt i medfør heraf skal opbevares. Det forudsættes, at der fastsættes regler om, at opbevaring af oplysninger registreret som følge af de foreslåede §§ 786 a-786 f i retsplejelovens eller pålæg eller regler udstedt i medfør heraf skal ske på servere i EU.

Det bemærkes, at nummeroplysningsdata, som defineret i § 31, stk. 2, i teleloven, og som udbydere af elektroniske kommunikationsnet eller -tjenester bl.a. skal indsamle og registrere til brug for nummeroplysningsdatabasen, jf. bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, efter Justitsministeriets opfattelse ikke kan anses som omfattet af Tele2-dommens præmis 122. Det er derfor ikke nødvendigt at indføre en

bestemmelse om at nummeroplysningsdata opbevares på servere inden for EU, og den foreslåede bestemmelse tager ikke sigte herpå.

Bestemmelsen foreslås udformet som en bemyndigelsesbestemmelse, hvorved justitsministeren efter forhandling med erhvervsministeren kan fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af de foreslåede §§ 786 a-786 f i retsplejeloven eller pålæg eller regler udstedt i medfør heraf. Bestemmelsen foreslås udmøntet ved bekendtgørelse, hvor der kan fastsættes krav til, at opbevaringen på servere i EU sletning ved irreversibel destruktion ved udløbet af opbevaringsperioden.

Forslaget skal ses i sammenhæng med bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, som udstedt med hjemmel i bl.a. telelovens § 8, stk. 1 og 4. Det er Justitsministeriets opfattelse, at det foreslåede opbevaringskrav passende vil kunne fastsættes i den nævnte bekendtgørelse.

3.10. Forholdet til tavshedspligt

3.10.1. Gældende ret

Retsplejelovens regler om tvangsindgreb er begrænset således, at de ikke kan bruges til at få adgang til kommunikation, der er undergivet en tavshedspligt, og som er udelukket fra reglerne om vidnepligt, jf. retsplejelovens § 170. Eksempelvis følger det af lovens § 794, stk. 3, og § 795, stk. 2, vedrørende ransagning hos hhv. en mistænkte og en ikke-mistænkt samt af § 804, stk. 4, vedrørende beslaglæggelse og edition, at indgrebene ikke kan bruges vedrørende oplysninger om forhold, som den pågældende ville være udelukket fra at afgive forklaring om som vidne, jf. § 170.

For indgreb i meddelelshemmeligheden følger det af retsplejelovens § 782, stk. 2, at telefonaflytning, anden aflytning, brevåbning og brevstandsning ikke må foretages med hensyn til den mistænktes forbindelse med personer, som efter reglerne i § 170 er udelukket fra at afgive forklaring som vidne.

Det fremgår af retsplejelovens § 170, stk. 1, at der ikke må kræves vidneforklaring fra præster i folkekirken eller andre trossamfund, læger forsvarere, retsmæglere, europæiske patentrådgivere og advokater om det, som er

kommet til deres kundskab ved udøvelsen af deres virksomhed med de pågældendes ønske. Vidneudelukkelsen gælder også for de pågældende personers medhjælpere, jf. § 170, stk. 4.

Det følger af retsplejelovens § 170, stk. 2, 1. pkt., at retten kan pålægge læger, retsmæglere, europæiske patentrådgivere og advokater, bortset fra forsvarere i straffesager, at afgive vidneforklaring, når forklaringen anses for at være af afgørende betydning for sagens udfald, og sagens beskaffenhed og dens betydning for vedkommende part eller samfundet findes at berettigge til, at forklaring afkræves. Vidneudelukkelsen er altså absolut for så vidt angår forsvarsadvokater og præster i folkekirken eller andre trossamfund samt for advokater og europæiske patentagenters arbejde med retssagsbehandling.

Det følger videre af retsplejelovens § 170, stk. 3, at retten kan bestemme, at forklaring ikke skal afgives om forhold, med hensyn til hvilke vidnet i medfør af lovgivningen har tavshedspligt, og hvis hemmeligholdelse har væsentlig betydning. Denne bestemmelse giver retten mulighed for konkret at vidneudelukke personer, der er omfattet af en tavshedspligt, men som ikke er blandt de persongrupper, der nævnes i bestemmelsen. Det er efter bestemmelsens forarbejder en forudsætning for at anvende denne bestemmelse, at vedkommende er underlagt en tavshedspligt, der efter loven er sanktioneret med straf. Det er ikke tilstrækkeligt, at tavshedspligten følger af faglige normer m.v. Der henvises til betænkning nr. 312/1962, s. 103.

Særligt for så vidt angår retsplejelovens § 782, stk. 2, gælder undtagelsen for vidneudelukkede personer ikke indgreb i form af teleoplysning og udvidet teleoplysning, jf. lovens § 780, stk. 1, nr. 3 og 4. Dette beror ifølge bestemmelsens forarbejder dels på praktiske hensyn og dels på, at indgrebet teleoplysning, hvorved kommunikationens indhold ikke røbes, ikke kan siges at anfægte det særlige fortrolighedsforhold, som vidneudelukkelsesreglen i § 170 skal beskytte. Der henvises til betænkning 1023/1984, s. 107.

3.10.2. EU-Domstolens praksis

EU-Domstolen har i forskellige afgørelser udtalt sig om forholdet mellem registrering og opbevaring og tavshedspligt.

I Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15 (Tele2 Sverige m.fl.) udtalte EU-Domstolen, at en ordning med generel og udifferentieret lagring af trafik- og lokaliseringsdata overskrider

det strengt nødvendige og i et demokratisk samfund ikke kan anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58 sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, jf. Tele2-dommens præmis 104-107:

”104. I denne henseende bemærkes for det første, at en sådan lovgivning, henset til sine kendetegn, der er beskrevet i denne doms præmis 97, bevirker, at lagringen af trafikdata og lokaliseringsdata er hovedreglen, mens den ved direktiv 2002/58 indførte ordning opstiller et krav om, at denne lagring af data skal være undtagelsen.

105. For det andet foreskriver en national lovgivning som den i hovedsagen omhandlede, der omfatter alle abonnenter og registrerede brugere generelt, og som er rettet mod alle elektroniske kommunikationsmidler og samtlige trafikdata, ingen 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 finder anvendelse endog på personer, hvis kommunikation i henhold til nationale retsregler er omfattet af tavshedspligt (jf. analogt for så vidt angår direktiv 2006/24 Digital Rights-dommen, præmis 57 og 58).

106. En sådan lovgivning kræver ikke 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 lag-

ring af deres data ville kunne bidrage til bekæmpelse af kriminalitet (jf. analogt for så vidt angår direktiv 2006/24 Digital Rights-dommen, præmis 59).

107. En national lovgivning som den i hovedsagen omhandlede overskrider derfor det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.”

Domstolen anfører dog videre i Tele2-dommen, at artikel 15, stk. 1, i direktiv 2002/58 sammenholdt med Chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke er til hinder for, at en medlemsstat vedtager lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af trafik- og lokaliseringsdata med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen. Der henvises til Tele2-dommens præmis 108 ff. Målrettet registrering og opbevaring af trafikdata med det nævnte formål er omtalt nærmere i pkt. 3.4.

I La Quadrature du Net-dommen gentager EU-Domstolen, at generel og udifferentieret lagring af trafik- og lokaliseringsdata bl.a. kan påvirke personer undergivet nationale regler om tavshedspligt, men at der omvendt ikke er tale om absolutte rettigheder, men rettigheder, der skal ses i sammenhæng med deres funktion i samfundet, jf. dommens præmis 118-121:

”118. For det første bemærkes, at lagring af trafikdata og lokaliseringsdata med henblik på politimæssige formål i sig selv kan medføre et indgreb i retten til respekt for kommunikation, der er sikret ved chartrets artikel 7, og have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved dette charters artikel 11 (jf. i denne retning dom af 8.4.2014, Digital Rights, C-293/12 og C-594/12, EU:C:2014:238, præmis 28, og af 21.12.2016, Tele2, C-203/15 og C-698/15, EU:C:2016:970, præmis 101). Sådanne afskrækkende virkninger kan imidlertid navnlig påvirke de

personer, hvis kommunikation i henhold til nationale bestemmelser er undergivet tavshedspligt, og de whistleblowere, hvis aktiviteter er beskyttet i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (EUT 2019, L 305, s. 17). Disse virkninger er desuden så meget desto mere alvorlige i betragtning af, at der er tale om store mængder af lagrede data af meget forskellig art.

119. For det andet bemærkes, at henset til den store mængde trafikdata og lokaliseringsdata, der løbende kan lagres ved hjælp af en generel og udifferentieret lagringsforanstaltning, og den følsomme karakter af de oplysninger, som disse data kan give adgang til, medfører alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, en risiko for misbrug og ulovlig adgang.

120. Når dette er sagt, afspejler artikel 15, stk. 1, i direktiv 2002/58, for så vidt som den giver medlemsstaterne mulighed for at indføre de undtagelser, der er nævnt i denne doms præmis 110, det forhold, at de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, ikke er absolutte rettigheder, men skal ses i sammenhæng med deres funktion i samfundet (jf. i denne retning dom af 16.7.2020, Facebook Ireland og Schrems, C-311/18, EU:C:2020:559, præmis 172 og den deri nævnte retspraksis).

121. Som det fremgår af chartrets artikel 52, stk. 1, tillader dette charter nemlig begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen og respekterer de nævnte rettigheders væsentligste indhold, og for så vidt som disse begrænsninger under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.”

EU-Domstolen udtaler herefter videre i hvilke tilfælde lagring af oplysninger kan finde sted. Disse tilfælde er omtalt nærmere i pkt. 3.1-3.5.

3.10.3. Justitsministeriets overvejelser

Justitsministeriet har overvejet, om EU-Domstolens praksis medfører, at oplysninger fra vidneudelukkede personer, jf. retsplejelovens § 170, skal undtages fra de foreslåede registrerings- og opbevaringspligter.

Det er Justitsministeriets vurdering, at EU-Domstolens praksis må læses således, at EU-Domstolen ikke stiller krav om, at oplysninger fra vidneudelukkede personer, jf. retsplejelovens § 170, skal undtages fra registrering og opbevaring i de situationer, der omtales i pkt. 3.1-3.5.

Justitsministeriet bemærker, at det i praksis vil blive vanskeligt at undtage oplysninger fra vidneudelukkede personer fra reglerne om registrering og opbevaring. Endvidere bemærker Justitsministeriet, at teleoplysning og udvidet teleoplysning efter gældende ret ikke kan siges at anfægte det særlige fortrolighedsforhold, som vidneudelukkelsesreglerne skal beskytte, og at disse indgreb derfor også omfatter kommunikation med vidneudelukkede personer.

På den baggrund stilles der ikke forslag om, at oplysninger fra vidneudelukkede personer, jf. retsplejelovens § 170, skal undtages fra de foreslåede registrerings- og opbevaringspligter.

Begærer politiet adgang til registrerings- og opbevaringspligtige oplysninger efter reglerne om edition, følger det af retsplejelovens § 804, stk. 4, at et pålæg om edition ikke kan meddeles, såfremt der derved vil fremkomme oplysning om forhold, som den pågældende ville være udelukket fra eller fritaget for at afgive forklaring om som vidne, jf. §§ 169-170. Dette vil også gælde for edition, der sker efter § 804 a, der kun indfører et særligt kriminalitetskrav for så vidt angår registrerings- og opbevaringspligtige oplysninger. De øvrige betingelser for at foretage edition, herunder § 804, stk. 4, vil fortsat gælde. Der henvises til pkt. 3.7.1.4 om reglerne om edition.

4. Konsekvenser for opfyldelsen af FN's verdensmål

Lovforslaget vurderes at bidrage til opfyldelsen af delmål nr. 16.a. Dette delmål vedrører styrkelse af relevante nationale institutioner, bl.a. gennem internationalt samarbejde, for at opbygge kapacitet på alle niveauer, og i særdeleshed i udviklingslande, for at forhindre vold og bekæmpe terrorisme og kriminalitet. Revisionen af reglerne om registrering og opbevaring m.v. har til formål i videst muligt omfang at medvirke til at sikre, at politiet og anklagemyndigheden inden for de givne rammer kan anvende trafikdata

m.v. til bekæmpelse af terrorisme og grov kriminalitet. Den foreslåede revision vil alt andet lige medføre, at politiet ikke får adgang til den samme mængde data som i dag, men med revisionen sikres en så effektiv kriminalitetsbekæmpelse på baggrund af trafikdata m.v. som muligt inden for rammerne af EU-retten.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Den foreslåede revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) forventes at medføre meget betydelige merudgifter for politiet, anklagemyndigheden og domstolene.

Udgifterne er forbundet med meget betydelig usikkerhed, hvilket bl.a. skal ses i lyset af, at udgifterne vil afhænge af, i hvilket omfang målrettet logning vil blive anvendt. Fuldt indfaset skønnes målrettet logning at medføre merudgifter på potentielt over 200 mio. kr. årligt i alt for myndighederne på Justitsministeriets område.

Udgifterne kan henføres til, at opgaveløsningen med målrettet logning vil være kendetegnet ved et omfattende udvidet sagsbehandlingsarbejde.

Det bemærkes, at der herudover vil kunne være udgifter forbundet med brugen af hastesikring.

Udgiftsskønnene vil skulle konsolideres nærmere med henblik på, at udgifterne forventes håndteret i forbindelse med finansloven for 2023. Forslaget om en ordning med målrettet registrering og opbevaring af trafikdata vil have it-mæssige implementeringskonsekvenser for dele af det offentlige. Disse er beskrevet nærmere under pkt. 3.1.3.4.

Forholdet til de databeskyttelsesretlige regler er beskrevet under pkt. 3.7.4.

6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

6.1. Administrative konsekvenser for erhvervslivet

Den foreslåede revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v. forventes på baggrund af den foretagne AMVAB-måling (aktivitetsbaseret måling af virksomhedernes administrative byrder) at medføre omstillingsomkostninger på 206 mio. kr. og løbende administrative byrder på ca. 107 mio. kr. årligt for telebranchen.

Det bemærkes, at den foretagne AMVAB-måling viser, at den foreslåede revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v. forventeligt vil medføre omstillingsomkostninger på ca. 331 mio. kr., hvoraf 125 mio. kr. kan henføres til to virksomheders efterregistrering af unikt ID på eksisterende fastnet- og IP-telefoniabonnenter.

For ikke at pålægge telebranchen unødigt byrdefuld regulering, lægges der med lovforslaget op til, at der ikke skal stilles krav til efterregistrering af unikt ID på eksisterende fastnet- og IP-telefoniabonnenter. Det vil reducere omstillingsomkostningerne fra branchen til de nævnte 206 mio. kr. Det bemærkes i den forbindelse, at kravet herom vurderes at have begrænset efterforskningsmæssig værdi sat over for den estimerede omstillingsomkostning for branchen. Det bemærkes desuden, at der fortsat lægges op til, at der vil være krav om efterregistrering af unikt ID på øvrige abonnenter.

Omstillingsomkostningerne består herefter navnlig i ca. 63,5 mio. kr. til tilpasning af teleudbydernes systemer, så de kan indberette unikt ID på abonnenterne til den såkaldte 118-database, samt 53 mio. kr. til varetagelsen af målrettet logning.

De løbende administrative byrder vedrører særligt udgifter til målrettet logning, byrder i forhold til registrering af brugere af taletidskort samt løbende drift og vedligehold af de tilpassede it-systemer. Navnlig registrering og verificering af unikt ID ved salg af taletidskort udgør en stor omkostning med ca. 69 mio. kr. årligt. Derimod vurderes der ikke at være væsentlige løbende administrative byrder ved registrering af unikt ID ved ny-oprettelse af abonnenter på mobil-, fastnet- eller ip-telefoni.

6.2. Princippet for agil erhvervsrettet regulering

Det er Justitsministeriets vurdering, at lovforslaget opfylder principperne for agil erhvervsrettet regulering.

7. Administrative konsekvenser for borgerne

Lovforslagets § 1, nr. 9, og § 2, nr. 2, forventes at medføre negative administrative konsekvenser for borgerne.

Det skyldes, at der med den foreslåede ændring af definitionen af nummeroplysningsdata i telelovens § 31, stk. 2, og den foreslåede indførelse af mulighed for, at Justitsministeren efter forhandling med klima-, energi- og forsyningsministeren kan fastsætte et registrerings- og verificeringskrav i be-

kendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, lægges op til, at udbyderen af elektroniske kommunikationsnet eller -tjenester, ud over en indsamling og registrering af nummeroplysningsdata, herunder unikt ID på slutbrugeren, skal verificere slutbrugerens unikke ID. Endvidere foreslås det med ordningen, at udbydere af elektroniske kommunikationsnet eller -tjenester skal foretage en dokumentation af verificeringen, ligesom slutbrugeren ikke må opnå adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget.

Der stilles med den foreslåede ordning ikke krav til, hvordan verificeringen skal foretages, men verificeringen vil forventeligt betyde, at borgerne vil blive nødsaget til at verificere sig i nogle tilfælde ved fysisk fremvisning af tiltrækkelig identifikation eller ved online eller telefonisk angivelse af de relevante oplysninger.

8. Klimamæssige konsekvenser

Lovforslaget vurderes ikke at have klimamæssige konsekvenser.

9. Miljø- og naturmæssige konsekvenser

Lovforslaget vurderes ikke at have klimamæssige konsekvenser.

10. Forholdet til EU-retten

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (direktiv 2002/58) indeholder regler om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

Det følger navnlig af artikel 5, stk. 1, at medlemsstaterne skal sikre kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata (princippet om kommunikationshemmelighed).

Det fremgår dog af artikel 15, stk. 1, i direktiv 2002/58, 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 udbydere af elektroniske kommunikationstjenester at lagre trafik- og lokaliseringsdata.

I La Quadrature du Net-dommen anfører EU-Domstolen bl.a., at det fremgår af artikel 15, stk. 1, 3. pkt., i direktiv 2002/58, at medlemsstaterne kun har mulighed for at vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der er omhandlet i dette direktivs artikel 5, 6 og 9, såfremt dette sker i overensstemmelse med EU-retten generelle principper, som bl.a. omfatter proportionalitetsprincippet, og de grundlæggende rettigheder, der er sikret ved EU's charter om grundlæggende rettigheder (Chartret). EU-Domstolen har desuden fastslået, at den pligt, som en medlemsstat i henhold til en national lovgivning har pålagt udbydere af elektroniske kommunikationstjenester til at lagre trafikdata med henblik på i påkommende tilfælde at gøre dem tilgængelige for de kompetente nationale myndigheder, ikke blot rejser spørgsmål vedrørende overholdelsen af Chartrets artikel 7 og 8, der vedrører henholdsvis respekten for privatlivet og beskyttelsen af personoplysninger, men ligeledes vedrørende artikel 11, der omhandler ytringsfriheden, jf. præmis 113 i La Quadrature du Net-dommen, præmis 25 og 70 i EU-Domstolens dom af 8. april 2014 i sagerne C-293/12 og C-594/12, Digital Rights (Digital Rights-dommen) og præmis 91 og 92 i EU-Domstolens dom af 21. december 2016 i sagerne C-203/15 og C-698/15, Tele2 (Tele2-dommen).

Artikel 15, stk. 1, i direktiv 2002/58 skal således fortolkes i lyset af Chartret, herunder navnlig dets artikel 7, 8 og 11.

Af Chartrets artikel 7 følger det, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Den forklarende rapport til Chartret angiver, at de rettigheder, der sikres ved artikel 7, svarer til dem, der er sikret ved Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8. For at tage hensyn til den tekniske udvikling er korrespondance dog ændret til "kommunikation". Det følger endvidere af den forklarende rapport, at retten efter Chartrets artikel 7 har samme betydning og omfang som den tilsvarende ret i EMRK, jf. også Chartrets artikel 52, stk. 3. Heraf følger det samtidig, at de begrænsninger, der lovligt kan foretages i rettighederne efter Chartrets artikel 7, er de samme, som dem, der accepteres inden for rammerne af EMRK artikel 8.

Chartrets artikel 8 indeholder en beskyttelse af personoplysninger. Det følger af artikel 8, stk. 1, at enhver har ret til beskyttelse af personoplysninger,

der vedrører den pågældende. Af artikel 8, stk. 2, følger det, at disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget, ved lov fastsat grundlag, og at enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf. Artikel 8, stk. 3, fastslår, at overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol. I den forklarende rapport til Chartrets artikel 8 anføres det bl.a., at bestemmelsen er baseret på artikel 16 i EUF-Traktaten, artikel 39 i EU-Traktaten og Rådets direktiv 13 95/46/EF (persondatadirektivet) samt på EMRK artikel 8 og Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger.

Efter Chartrets artikel 11, stk. 1, har enhver ret til ytringsfrihed. Retten omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser. Af den forklarende rapport til Chartrets artikel 11 fremgår, at artiklen svarer til artikel 10 i EMRK. Det følger endvidere af den forklarende rapport, at retten efter Charterets artikel 11 har samme betydning og omfang som den tilsvarende ret i EMRK, jf. også Charterets artikel 52, stk. 3. Heraf følger det samtidig, at de begrænsninger, der lovligt kan foretages i rettingerne efter Charterets artikel 11, er de samme, som dem, der accepteres inden for rammerne af EMRK artikel 10.

Med lovforslaget lægges der op til, at indføre en todelt ordning for registrering og opbevaring af trafikdata.

For det første foreslås en ordning med målrettet personbestemt og geografisk registrering og opbevaring af trafikdata, jf. pkt. 3.1.

For det andet foreslås en ordning med generel og udifferentieret registrering og opbevaring, hvorefter justitsministeren bemyndiges til efter forhandling med erhvervsministeren at kunne fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må antages at være reel og aktuel eller forudsigelig, jf. pkt. 3.2.

Det foreslås, at der fastsættes krav om adgang til oplysninger registreret på baggrund af henholdsvis målrettet og generel og udifferentieret registrering

og opbevaring, således at der alene vil kunne gives adgang til oplysningerne til brug for efterforskning og retsforfølgning af grov kriminalitet, herunder trusler mod den nationale sikkerhed, jf. pkt. 3.7.

Herudover foreslås det, at den forpligtelse, der i dag følger af logningsbekendtgørelsens § 5, stk. 1, om registrering af oplysninger om en brugers adgang til internettet ved den tildelte internetprotokol-adresse (IP-adresse) m.v., videreføres i retsplejeloven, jf. pkt. 3.3.

Der foreslås endvidere ændringer i de gældende regler om hastesikring, jf. pkt. 3.5, ligesom der foreslås indført regler om domstolsprøvelse af konkret begrundede pålæg, jf. pkt. 3.6.

Endelig foreslås det, at der skal kunne fastsættes regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af §§ 786 a-786 f eller pålæg eller regler udstedt i medfør heraf, herunder regler med krav om opbevaring på servere i EU for data registreret efter de foreslåede regler.

I lyset af EU-Domstolens seneste praksis som beskrevet ovenfor under pkt. 2, vil de foreslåede ordninger med registrerings- og opbevaringspligt for trafikdata samt adgang hertil efter Justitsministeriets opfattelse udgøre indgreb i rettighederne fastsat i Chartrets artikel 7, 8 og 11. Sådanne indgreb skal kunne retfærdiggøres efter Chartrets artikel 52, stk. 1, hvilket indebærer, at indgrebene skal være fastlagt i lovgivningen og respektere de nævnte rettigheders væsentligste indhold. Desuden skal indgrebene under iagttagelse af proportionalitetsprincippet være nødvendige og faktisk svare til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

Herom anfører EU-Domstolen i La Quadrature du Net-dommen endvidere, at der i forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 i lyset af Chartret også skal tages hensyn til betydningen af de rettigheder, der er sikret ved Chartrets artikel 3, 4, 6 og 7, og til den betydning, som formålene om beskyttelse af den nationale sikkerhed og bekæmpelse af grov kriminalitet har som følge af, at de bidrager til beskyttelsen af andres rettigheder og friheder, jf. præmis 122 i La Quadrature du Net-dommen.

For at opfylde kravet om proportionalitet skal en lovgivning om registrering og opbevaring af trafikdata fastsætte klare og præcise regler, der regulerer

rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug. Denne lovgivning skal være bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser de kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige. Nødvendigheden af at råde over sådanne garantier er så meget desto større, når personoplysningerne er undergivet en automatiseret behandling, navnlig når der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger. Disse betragtninger gør sig især gældende, når der er tale om beskyttelse af den særlige kategori af personoplysninger, som følsomme oplysninger udgør, jf. præmis 132 i *La Quadrature du Net*-dommen og den deri nævnte praksis.

EU-Domstolen har endvidere i præmis 133 i *La Quadrature du Net*-dommen anført, at en lovgivning, der foreskriver lagring af personoplysninger, altid skal opfylde objektive kriterier, som fastlægger et forhold mellem de oplysninger, der skal lagres, og det forfulgte formål.

De foreslåede ordninger med registrerings- og opbevaringspligt for trafikdata samt adgang hertil foreslås indført af hensyn til politiets forebyggelse og efterforskning af grov kriminalitet, hvor politiets adgang til registrerede og opbevarede trafikdata m.v. udgør et helt centralt efterforskningsværktøj. Registreringen og opbevaringen af trafikdata og de efterfølgende muligheder for adgang hertil er således foreslået udformet af hensyn til den nationale sikkerhed og offentlige tryghed, jf. Chartrets artikel 52, stk. 1.

Den foreslåede ordning med registrering og opbevaring af trafikdata m.v. må endvidere – på baggrund af det under pkt. 3.1.3, 3.2.3, 3.3.3, 3.4.3, 3.5.3, 3.6.3, 3.7.3, 3.7.4 og 3.9.3 anførte – efter Justitsministeriets opfattelse anses for nødvendigt for at forfølge de angivne hensyn. Heri ligger, at registreringen og opbevaringen samt adgangen til de registrerede og opbevarede oplysninger skal opfylde proportionalitetsprincippet.

Det bemærkes i den forbindelse, at der med lovforslaget lægges op til, at der alene vil kunne iværksættes generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må antages at være reel og aktuel

eller forudsigelig. Regler om generel og udifferentieret registrering og opbevaring af trafikdata vil endvidere alene kunne fastsættes med en gyldighedsperiode på maksimalt 1 år ad gangen, og en ordning med generel og udifferentieret registrering og opbevaring af trafikdata vil ikke kunne blive det systematiske udgangspunkt. Det følger desuden af den foreslåede ordning, at regler om generel og udifferentieret registrering og opbevaring vil skulle ophæves, hvis grundlaget herfor ikke længere er til stedet. Det vil kunne føre til en gyldighedsperiode på mindre end 1 år.

Når der ikke foreligger en tilstrækkelig alvorlig trussel mod den nationale sikkerhed, vil der efter forslaget kunne iværksættes målrettet registrering og opbevaring af trafikdata. Der vil være tale om automatisk iværksættelse af målrettet registrering og opbevaring på baggrund af klare, objektive kriterier fastsat i loven. Hertil kommer, at der vil være mulighed for ved konkret begrundede pålæg at forpligte udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, til at registrere og opbevare trafikdata vedrørende bestemte personer eller områder, der er grund til at antage har en forbindelse til grov kriminalitet. Sådanne pålæg vil skulle indhentes ved retskendelse. I forbindelse med indhentelsen af retskendelsen, vil pålægget, herunder proportionaliteten, skulle prøves.

Det foreslås desuden, at der – for så vidt angår både ordningen med generel og udifferentieret og ordningen med målrettet registrering og opbevaring – alene skal være adgang til registrerings- og opbevaringspligtige oplysninger ved forudgående indhentelse af retskendelse. Det vil være et krav for adgang til trafikdata, at der anmodes om adgang med henblik på bekæmpelse af grov kriminalitet, mens der for adgang til IP-adresser, indhentet på grundlag af en registrerings- og opbevaringspligt, vil være krav om adgang med henblik på bekæmpelse af kriminalitet.

Endelig vil registrerings- og opbevaringspligtige oplysninger maksimalt skulle opbevares i 1 år, hvilket må anses for ikke at være længere end nødvendigt for at varetage hensynet til den nationale sikkerhed og offentlige tryghed.

De foreslåede ordninger for registrering og opbevaring af trafikdata adskiller sig således væsentligt fra de ordninger, som EU-Domstolen har taget stilling til i La Quadrature du Net-dommen, Tele2-dommen og Digital Rights-dommen m.v.

Ved vurderingen af den foreslåede ordnings proportionalitet er det endvidere tillagt vægt, at der er lagt op til at videreføre de gældende krav til beskyttelse af bl.a. registrerings- og opbevaringspligtige oplysninger, jf. pkt. 3.1.1.3, og at behandling af personoplysninger desuden vil være underlagt henholdsvis Datatilsynets og Tilsynet med Efterretningstjenesternes tilsyn.

Det er således samlet set Justitsministeriets opfattelse, at de foreslåede regler er nødvendige og proportionale samt i overensstemmelse med EU-Domstolens seneste praksis, jf. pkt. 2.

Det bemærkes dog, at der vurderes at være en væsentlig procesrisiko forbundet med, at der i lovforslaget lægges op til, at politiet og anklagemyndigheden vil kunne få adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet, jf. ovenfor under pkt. 3.7.2.

11. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 27. september 2021 til den 25. oktober 2021 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Bitbureauet, Campingrådet, Danske Advokater, Datatilsynet, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Forbrugerrådet TÆNK, Foreningen af Offentlige Anklagere, HK-Landsklubben Danmarks Domstole, HK-Landsklubben for Politiet, Landsforeningen af Forsvarsadvokater, Politiets Efterretningstjeneste, Politiforbundet, Rigsadvokaten, Rigspolitiet, Samtlige byretter, Sø- og Handelsretten, Vestre Landsret, Østre Landsret, Ingeniørforeningen IDA, Institut for Menneskerettigheder Dansk Journalistforbund, Justitia, Rådet for Digital Sikkerhed, Amnesty International, Retspolitisk Forening, DI, Dansk Erhverv, Dansk Metal, Dansk Energi, HORESTA, Brancheforeningen Teleindustrien, Dansk IT, Foreningen af Danske Internet Medier, IT-Branchen, DI Digital, PROSA, SAM-DATA (HK), Business Software Alliance Danmark IT-Politisk Forening, KMD, CSC Danmark A/S, TDC A/S, Telenor A/S, Telia A/S, Hi3G Denmark ApS, SE/Stofa, Lejernes LO, Andelsboligforeningernes Fællesrepræsentation, Dansk Magisterforening, Danmarks Restauranter.

12. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner		Lovforslaget skønnes at medføre be- tydelige merudgifter for politiet, an- klagemyndigheden og domstolene. Udgifterne er forbundet med betyde- lig usikkerhed men kan potentielt overstige 200 mio. kr. årligt. Udgif- terne vil skulle konsolideres nær- mere.
Implemente- ringskonsekven- ser for stat, kom- muner og regio- ner		Forslaget om en ordning med målret- tet registrering og opbevaring af tra- fikdata vil have it-mæssige imple- menteringskonsekvenser for dele af det offentlige, navnlig Rigspolitiet, med henblik på en automatiseret pro- ces. Der henvises til pkt. 3.1.3.4.
Økonomiske konsekvenser for erhvervslivet		Forslaget forventes ikke at medføre væsentlige øvrige erhvervsøkonomi- ske konsekvenser ud over de admini- strative konsekvenser.
Administrative konsekvenser for erhvervslivet		Forslaget forventes at medføre om- stillingsomkostninger på ca. 206 mio. kr. og løbende administrative byrder på ca. 107 mio. kr. årligt for telebranchen.

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)
Administrative konsekvenser for borgerne	Ingen	Lovforslagets § 1, nr. 9, og § 2, nr. 2, forventes at medføre negative administrative konsekvenser for borgerne. Den foreslåede indførelse af mulighed for, at Justitsministeren efter forhandling med klima-, energi- og forsyningsministeren kan fastsætte et registrerings- og verificeringskrav i bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, vil således potentielt kunne betyde, at borgerne vil blive nødsaget til at verificere sig i nogle tilfælde ved fysisk fremvisning af tiltrækkelig identifikation eller ved online eller telefonisk angivelse af de relevante oplysninger, for at opnå adgang til elektroniske kommunikationsnet eller -tjenester.
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU- retten	Det er samlet set Justitsministeriets opfattelse, at de foreslåede regler er nødvendige og proportionale samt i overensstemmelse med EU-Domstolens seneste praksis, jf. pkt. 2. Det bemærkes dog, at der vurderes at være en væsentlig procesrisiko forbundet med, at der i lovforslaget lægges op til, at politiet og anklagemyndigheden vil kunne få adgang til trafikdata, der er registreret og opbevaret med henblik på at beskytte den nationale sikkerhed, til brug for politiets og anklagemyndighedens bekæmpelse af grov kriminalitet, jf. pkt. 3.7.2.	

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, an- før »Ingen«)
Er i strid med de principper for implementering af erhvervsrettet EU-regulering/ Går videre end minimumskrav i EU-regulering (sæt X)	Ja	Nej X

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Til nr. 1

Det fremgår af retsplejelovens § 781, stk. 1, nr. 3, at efterforskningen skal angå en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 233, stk. 1, § 235, § 266, § 281 eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5.

Retsplejelovens § 781 fastsætter således betingelserne for, hvornår der kan foretages indgreb i meddelelseshemmeligheden. Bestemmelsens stk. 1, nr. 1-3, fastlægger de grundlæggende krav til mistankens styrke, indikationen for indgrebet og kravet til alvoren af den kriminalitet, der er under efterforskning. Bestemmelsens stk. 2-5 fastsætter nogle særlige krav for visse typer af indgreb i meddelelseshemmeligheden.

Det foreslås, at ændre retsplejelovens § 781, stk. 1, nr. 3, så der indsættes en henvisning til den foreslåede § 781 a.

Den foreslåede ændring vil medføre, at kriminalitetskravet i retsplejelovens § 781, stk. 1, nr. 3, fraviges for så vidt angår indgreb i meddelelseshemmeligheden, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser. Dette vil også følge direkte af den foreslåede § 781 a, der for sådanne typer indeholder et lempeligere kriminalitetskrav, således at indgreb i meddelelseshemmeligheden i form af teleoplysning og udvidet teleoplysning vil kunne ske for lovovertrædelser, der kan straffes med fængsel i 3 år eller derover.

Ændringen er en konsekvens af den foreslåede ændring i lovforslagets § 1, nr. 2. Der henvises pkt. 3.7.3 og 3.7.4 i de almindelige bemærkninger.

Til nr. 2

Retsplejeloven indeholder ikke i dag en særlig bestemmelse om teleoplysning eller om udvidet teleoplysning, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven. Pålæg om udlevering af sådanne oplysninger, der har karakter af indgreb i meddelelseshemmeligheden, gives i dag efter de almindelige regler om teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4.

Det følger af den gældende § 781, stk. 1, nr. 3, i retsplejeloven at det bl.a. er 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 kapitel 12 eller 13 eller en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 233, stk. 1, § 235, § 266, § 281 eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5. Der gælder i § 781, stk. 2, og 3, forskellige undtagelser til dette kriminalitetskrav for visse typer af indgreb i meddelelseshemmeligheden. Der henvises til pkt. 3.7.1.2 i lovforslagets almindelige bemærkninger.

Retsplejelovens § 781, stk. 2, omfatter overtrædelser af straffelovens § 263, stk. 1, om hacking. Lovens § 781, stk. 3, nr. 1, omhandler krænkelse som nævnt i § 2, stk. 2, nr. 1, i lov om tilhold, opholdsforbud og bortvisning. Bestemmelsen i tilholdslovens § 2, stk. 2, nr. 1, omfatter bl.a. krænkelse af en andens fred ved at forfølge eller genere den anden ved kontakt m.v., 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. Retsplejelovens § 781, stk. 3, nr. 2, omfatter overtrædelser af straffelovens § 279 a (databedrageri) og § 293, stk. 1 (brugstyveri), begået ved anvendelse af en telekommunikationstjeneste. Endelig omfatter retsplejelovens § 781, stk. 3, nr. 3-5, forskellige overtrædelser af EU-regler, der har karakter af misbrug af intern viden eller markedsmanipulation. Der henvises til pkt. 3.7.1.2 i de almindelige bemærkninger.

Det foreslås, at der i retsplejeloven indsættes en ny § 781 a om teleoplysning og udvidet teleoplysning, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Efter den foreslåede § 781 a kan teleoplysning, jf. § 780, stk. 1, nr. 3, og udvidet teleoplysning, jf. § 780, stk. 1, nr. 4, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, uanset § 781, stk. 1, nr. 3, tillige foretages, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Den foreslåede § 781 a i retsplejeloven vil medføre et lempeligere kriminalitetskrav for teleoplysning og udvidet teleoplysning, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, end det, der følger af hovedreglen i retsplejelovens § 781, stk. 1, nr. 3. Teleoplysning som led i efterforskning af krænkelser eller lovovertrædelser, der ikke kan straffes med fængsel i 3 år eller derover, vil stadig kunne foretages, hvis der er tale om efterforskning af en af de krænkelser eller overtrædelser, der er særskilt nævnt i § 781, stk. 1, nr. 3, eller er omfattet af § 781, stk. 2 eller 3. Eksempelvis vil der uanset den foreslåede § 781 a stadig kunne foretages teleoplysning som led i efterforskning af krænkelser som nævnt i § 2, stk. 1, nr. 1, i lov om bortvisning og tilhold, jf. § 781, stk. 3, nr. 1, samt de i § 781, stk. 3, nr. 3-5, omhandlede overtrædelser af forskellige EU-regler vedrørende misbrug af intern viden og markedsmanipulation.

Den foreslåede § 781 a i retsplejeloven vil sammen med den gældende § 781, stk. 1, nr. 3, medføre, at der vil gælde samme kriminalitetskrav for udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, hvad enten pålægget om udlevering sker efter reglerne om edition, jf. den foreslåede § 804 a, eller reglerne om teleoplysning eller udvidet teleoplysning, jf. den foreslåede § 781 a.

Hvis efterforskningen angår en lovovertrædelse, der kan straffes med fængsel i 6 år eller derover, eller en af de lovovertrædelser, der er særskilt nævnt i § 781, stk. 1, nr. 3, eller i stk. 2 og 3, vil adgangen til oplysningerne kunne meddeles allerede efter denne bestemmelse. Den foreslåede § 781 a vil derfor kun særskilt være relevant, hvis der skal gives pålæg om udlevering af oplysninger til brug for efterforskningen af en lovovertrædelse, der ikke er omfattet af § 781, stk. 1, nr. 3, eller af stk. 2 eller stk. 3.

Den foreslåede § 781 a vil bl.a. medføre, at overtrædelser af straffelovens § 136 (offentlig tilskyndelse til en forbrydelse), § 244 (simpel vold), § 243 (psykisk vold), § 261 (frihedsberøvelse), § 264, d, stk. 2 (uberettiget videregivelse af oplysninger om private forhold m.v. under skærpende omstændigheder) og § 293 a (brugstyveri af motorkøretøj) vil kunne danne grundlag for teleoplysning og udvidet teleoplysning, der består i pålæg om udlevering af registrerings- og opbevaringspligtige oplysninger. Disse lovovertrædelser kan straffes med fængsel i indtil 3 år, men er ikke omfattet af den gældende § 781, stk. 1, nr. 3.

Kravet om, at efterforskningen skal angå en lovovertrædelse, der kan straffes med fængsel i 3 år eller derover, vil ikke medføre nogen ændring i forhold til efterforskning af de fleste særlovsovertrædelser. De fleste særlovsovertrædelser, der giver mulighed for fængselsstraf, vil typisk have en strafferamme med et maksimum på fængsel i 2 år, jf. f.eks. § 3 i lov om euforiserende stoffer (overtrædelser af loven og de i medfør af den udfærdigede forskrifter) og færdselslovens § 117, stk. 2 (forskellige kvalificerede overtrædelse af færdselsloven). Efterforskning af sådanne overtrædelser vil derfor heller ikke med den foreslåede ordning kunne begrunde teleoplysning eller udvidet teleoplysning.

Kravet om, at der skal være tale om en lovovertrædelse, der kan straffes med fængsel i 3 år eller derover, vil også medføre, at efterforskning af en række af formueforbrydelserne i straffelovens kapitel 28 ligesom i dag som udgangspunkt ikke vil kunne begrunde teleoplysning eller udvidet teleoplysning af registreringspligtige oplysninger. Det drejer sig f.eks. om tyveri (§ 276), underslæb (§ 278), bedrageri (§ 279), mandatsvig (§ 280) og skyldnersvig (§ 283), da disse lovovertrædelser som hovedregel kun kan straffes med fængsel i indtil 1 år og 6 måneder, jf. § 285, stk. 1. Har overtrædelser af de nævnte forbrydelser været af særlig grov beskaffenhed, f.eks. på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i foreningen, kan straffen imidlertid stige til 6 eller 8 år afhængig af, hvilken forbrydelse der er tale om, jf. straffelovens § 286. Ved efterforskning af sådanne lovovertrædelser vil der som i dag kunne anvendes teleoplysning og udvidet teleoplysning efter retsplejelovens § 781, stk. 1. I forhold til efterforskning af straffelovens formueforbrydelser skal det bemærkes, at der uanset kriminalitetskravet efter den foreslåede § 781 a i retsplejeloven vil kunne meddeles pålæg om edition af registrerings- og opbevaringspligtige oplysninger som led i efterforskning af overtrædelser af straffelovens § 279 a eller § 293,

stk. 1, begået ved anvendelse af en telekommunikationstjenester, jf. § 781, stk. 3.

Henvisningen til lovovertrædelser, som kan medføre strafforhøjelse efter straffelovens § 81 a betyder, at der vil kunne gives adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven, hvis efterforskningen angår en af de overtrædelser, der er nævnt i § 81 a, hvis efterforskningen vel og mærke angår de omstændigheder, der er nævnt i § 81 a. Eksempelvis vil efterforskning af en overtrædelse af straffelovens § 260 (ulovlig tvang) ikke i sig selv kunne begrunde anvendelse af den foreslåede § 781 a, da bestemmelsen ikke kan medføre straf i form af fængsel i 3 år eller derover. Hvis overtrædelsen af § 260 imidlertid er begået under omstændigheder som nævnt i § 81 a, kan den foreslåede § 781 a bringes i anvendelse. Efterforskningen skal således angå en lovovertrædelse, der har baggrund i eller er egnet til at fremkalde en konflikt mellem grupper af personer, hvor der som led i konflikten enten anvendes skydevåben eller anvendes våben eller eksplosivstoffer, som på grund af deres særdeles farlige karakter er egnet til at forvolde betydelig skade, eller begås brandstiftelse omfattet af straffelovens § 180.

Den foreslåede § 781 a i retsplejeloven vil omfatte alle oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede bestemmelser i retsplejelovens §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser. Oplysninger, som udbydere af elektroniske kommunikationsnet og -tjenester er i besiddelse af, som ikke er registrerings- og opbevaringspligtige efter de nævnte bestemmelser, vil kunne kræves udleveret efter de almindelige regler om indgreb i meddelelseshemmeligheden.

Der henvises til pkt. 3.1 og 3.2 i lovforslagets almindelige bemærkninger.

Bestemmelsen vil desuden kun være relevant for pålæg om udlevering af oplysninger hos de udbydere, som registrerings- og opbevaringspligten efter de foreslåede §§ 786 a-786 e består over for. Det vil sige udbydere af elektroniske kommunikationsnet eller -tjenester, jf. pkt. 3.2.3.1 i lovforslagets almindelige bemærkninger, henholdsvis udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, jf. pkt. 3.1.3.1 i lovforslagets almindelige bemærkninger. Anmodning om adgang til registrerings- og opbevaringspligtige oplysninger vil efter den foreslåede bestemmelse skulle rettes til den dataansvarlige udbyder.

Reglerne om teleoplysning omfatter ikke civile identitetsoplysninger (oplysninger om, hvilken bruger der er indehaver af et bestemt telefonnummer, et bestemt IMEI- eller IMSI-nummer etc.). Sådanne oplysninger vil efter forslaget i stedet kunne indhentes efter reglerne om edition eller efter den foreslåede § 804 b i retsplejeloven. Der henvises til pkt. 3.7.1.2.1, 3.7.1.4, 3.7.3.3.3 og 3.7.3.3.4 i de almindelige bemærkninger.

Den foreslåede § 781 a i retsplejeloven vil kun medføre et lempeligere kriminalitetskrav for teleoplysning og udvidet teleoplysning, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser. De øvrige betingelser i retsplejelovens § 781 vil stadig skulle være opfyldt, før der kan foretages teleoplysning og udvidet teleoplysning, der består i pålæg om udlevering af sådanne oplysninger. Eksempelvis kravet til mistankens styrke og kravet til indgrebets indikation, jf. § 781, stk. 1, hhv. nr. 1 og 2. Tilsvarende vil udvidet teleoplysning som efter gældende regler kun kunne foretages, når mistanken vedrører en forbrydelse, som har medført eller kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier, jf. § 781, stk. 5, 1. pkt. Indgreb vil også kun kunne foretages, såfremt det er proportionalt, jf. retsplejelovens § 782. Teleoplysning og udvidet teleoplysning vil som hidtil desuden kun kunne foretages efter forudgående retskendelse, medmindre øjemedet ellers ville forspildes, jf. § 783. Der vil også fortsat skulle beskikkes en indgrebsadvokat, jf. § 784. Tilsvarende vil der som i dag skulle ske underretning af den, som indgrebet angår, jf. reglerne herom i retsplejelovens § 788. Der henvises til pkt. 3.7.1.2 og 3.7.3 i de almindelige bemærkninger.

Der henvises i øvrigt til pkt. 3.7.3 og 3.7.4 i de almindelige bemærkninger.

Til nr. 3

Det fremgår af retsplejelovens § 786, stk. 4, at det påhviler udbydere af tele- eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. For en nærmere beskrivelse af gældende ret henvises til pkt. 3.1.1.1 i de almindelige bemærkninger til lovforslaget.

Det fremgår af retsplejelovens § 786, stk. 6, at overtrædelse af bestemmelsens stk. 4, 1. pkt., straffes med bøde.

Med lovforslagets § 1, nr. 9, foreslås indsat §§ 786 b-786 i efter den gældende § 786 a i retsplejeloven. Bestemmelserne har til formål at indføre en ny ordning for registrering og opbevaring, der skal erstatte den gældende ordning i retsplejelovens § 786, stk. 4 og 6. Som konsekvens heraf, foreslås det, at de gældende bestemmelser i § 786, stk. 4 og 6 ophæves. Stk. 5 bliver herefter stk. 4 og stk. 7 og 8 bliver herefter stk. 5 og 6.

Der henvises til bemærkninger til § 1, nr. 9.

Til nr. 4

Det fremgår af retsplejelovens § 786, stk. 7, at der for overtrædelser af bestemmelser i forskrifter, der er fastsat i medfør af bestemmelsens stk. 4, 2. pkt., og stk. 5 kan fastsættes bestemmelser om bødestraf.

Med lovforslagets § 1, nr. 9, foreslås indsat §§ 786 b-786 i efter den gældende § 786 a i retsplejeloven. Bestemmelserne har til formål at indføre en ny ordning for registrering og opbevaring, der skal erstatte den gældende ordning i retsplejelovens § 786, stk. 4 og 6. På den baggrund foreslås det, at de gældende bestemmelser i § 786, stk. 4 og 6 ophæves.

Det foreslås som konsekvens heraf, at henvisningen i retsplejelovens § 786, stk. 7, der bliver stk. 5, til det gældende stk. 4, 2. pkt., slettes.

Til nr. 5

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

Det foreslås, at bestemmelsen ændres således, at ”trafikdata” ændres til ”trafik- og lokaliseringsdata”. Ændringen har til formål at tydeliggøre bestemmelsens overensstemmelse med EU-Domstolens praksis, således at det fremgår direkte af bestemmelsen, at reglerne om hastesikring gælder alle trafik- og lokaliseringsdata.

Ændringen skal ses i sammenhæng med den foreslåede ændring i lovforslagets § 1, nr. 7. Der henvises til de specielle bemærkninger hertil.

Til nr. 6

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

Med den nuværende bestemmelse i retsplejelovens § 786 a, stk. 2, 3. og 4. pkt., kan sikringsperioden ikke overstige 90 dage, og et pålæg kan ikke forlænges.

Det foreslås, at retsplejelovens § 786 a, stk. 2, 4. pkt., om at et pålæg ikke kan forlænges, udgår, og at det i stedet indsættes, at et pålæg efterfølgende kan opretholdes, men højst med 90 dage ad gangen.

Forslaget skal ses i lyset af, at det fremgår af La Quadrature du Net-dommen, at sikringsperioden gerne må forlænges, når det er begrundet i omstændighederne og det formål, der forfølges.

Retsplejelovens § 786 a blev oprindeligt indsat på baggrund af 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. Det fremgår af konventionens artikel 16, at et pålæg om hastesikring efterfølgende kan opretholdes.

Det foreslås derfor, at et pålæg både kan forlænges inden for de 90 dage, men også kan opretholdes efter de 90 dage kan opretholdes. Det er det samme pålæg om hastesikring, som hhv. kan forlænges og opretholdes. De øvrige betingelser i bestemmelsen skal også her være opfyldt, herunder at sikringsperioden skal være så kort som mulig.

Til nr. 7

Den nuværende bestemmelse i retsplejelovens § 786 a indeholder ikke et kriminalitetskrav for, i hvilke tilfælde politiet kan meddele udbyderne af telenet eller teletjenester pålæg.

På baggrund af La Quadrature du Net-dommen er det nødvendigt at tilpasse den nationale lovgivning, således at der i bestemmelsen fastsættes et kriminalitetskrav for visse oplysninger, således at hastesikring af trafik- og lokaliseringsdata kun må foretages, hvis efterforskningen angår grov kriminalitet, dvs. hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitler 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Det foreslås derfor, at der i § 786 a, efter stk. 2, indsættes et nyt stykke, hvorved der for så vidt angår hastesikring indføres et kriminalitetskrav for trafik- og lokaliseringsdata.

Det vil betyde, at hastesikring af trafik- og lokaliseringsoplysninger kun kan ske med henblik på bekæmpelse af grov kriminalitet, jf. definitionen ovenfor.

Retsplejelovens § 786 a omfatter også øvrige elektroniske data ud over trafik- og lokaliseringsdata. For øvrige oplysninger, som ikke anses for at være trafik- og lokaliseringsdata, vil der således ikke gælde et kriminalitetskrav.

Som konsekvens af forslaget bliver de nuværende stk. 3 og 4 herefter stk. 4 og 5.

Til nr. 8

Den nuværende retsplejelovs § 786 a, stk. 4, indeholder henvisning til den nuværende stk. 3 i bestemmelsen.

Med lovforslagets § 1, nr. 7, foreslås det, at der indsættes et nyt stk. 2 i retsplejelovens § 786 a. Herefter vil § 786 a, stk. 3, blive til § 786 a, stk. 4.

Det foreslås på den baggrund at ændre henvisningen til stk. 3 i den nuværende § 786 a, stk. 4, så henvisningen fremover vil være til bestemmelsens stk. 4.

Den foreslåede ændring er således en konsekvens af lovforslagets § 1, nr. 7. Der henvises til de specielle bemærkninger hertil.

Til nr. 9

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller telenetjenester 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 logningsbekendtgørelsens § 1, at udbydere af elektroniske kommunikationsnet eller -tjenester 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.

Efter logningsbekendtgørelsens § 5, stk. 1, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, skal en udbyder af elektroniske kommunikationsnet eller -tjenester registrere oplysninger om en brugers adgang til internettet, herunder den tildelte brugeridentitet (nr. 1), den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet (nr. 2), navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet (nr. 3) og tidspunktet for kommunikationens start og afslutning (nr. 4).

For nærmere om gældende ret henvises til pkt. 3.1.1 og 3.3.1 i de almindelige bemærkninger til lovforslaget.

Det foreslås, at der efter retsplejelovens § 786 a indsættes §§ 786 b-786 i. Bestemmelserne har til formål at indføre en ny ordning for registrering og opbevaring, der skal erstatte den gældende ordning i retsplejelovens § 786, stk. 4. For nærmere om baggrunden herfor henvises til pkt. 2 i lovforslagets almindelige bemærkninger.

Til § 786 b

Det foreslås, at der indsættes en ny § 786 b, hvorefter det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet

eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata efter stk. 2-5, jf. *stk. 1*.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.1.3.1 i lovforslagets almindelige bemærkninger.

Registrerings- og opbevaringspligten vil efter forslaget skulle gælde fra det tidspunkt, hvor udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, har modtaget tilstrækkelige oplysninger om de omfattede personer fra myndighederne til at iværksætte registrering og opbevaring målrettet de pågældende personer. Der henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det foreslås, at pligten til at foretage personbestemt målrettet registrering og opbevaring vil skulle omfatte de data, der er registrerings- og opbevaringspligtige i dag. Det vil sige de data, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som "teletrafik" (trafikdata). Visse lokaliseringsdata, som udgør trafikdata i forbindelse med telefoni- og sms/mms-kommunikation, er også i dag registrerings- og opbevaringspligtige, idet de anses for omfattet af forpligtelsen i retsplejelovens § 786, stk. 4, eller regler fastsat i medfør heraf. Det gælder oplysninger om den eller de celler, en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen. Disse data vil efter lovforslaget også fremadrettet være registrerings- og opbevaringspligtige.

Det foreslås således, at der vil kunne iværksættes målrettet registrering og opbevaring for alle typer trafikdata.

Begrebet trafikdata skal forstås i overensstemmelse med e-databeskyttelsesdirektivets artikel 2, litra b og c. Ved trafikdata forstås data, som behandles med henblik på overførsel af kommunikation i et elektronisk kommunikationsnet eller debitering heraf.

Der henvises til pkt. 3.1.3.4 og 3.2.3.3 i lovforslagets almindelige bemærkninger for en nærmere omtale af, hvad der forstås ved trafikdata.

Det foreslås, at pligten til at foretage personbestemt målrettet registrering og opbevaring af trafikdata skal baseres på objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafikdata kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, og på den måde 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.

Ved ”grov kriminalitet” forstås samme kriminalitetskrav, som også foreslås for udlevering af registrerings- og opbevaringspligtige oplysninger, jf. de foreslåede § 781 a og § 804 a i retsplejeloven. Herefter vil grov kriminalitet blive anset som lovovertrædelser, der efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller lovovertrædelser der har medført strafforhøjelse efter straffelovens § 81 a. Der henvises til pkt. 3.7.3 i lovforslagets almindelige bemærkninger.

Det foreslås på den baggrund i *stk. 2*, at trafikdata omfattet af forpligtelsen i det foreslåede *stk. 1* skal registreres i

- 1) 3 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som har medført straf efter straffelovens § 81 a,
- 2) 5 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover,
- 3) 10 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i 8 år eller derover.

Er den pågældende dømt for flere lovovertrædelser ved samme dom, vil der skulle tages udgangspunkt i den højeste strafferamme. Er personen dømt for en lovovertrædelse i straffelovens kapitel 12 og 13, der har en strafferamme på 6 år eller derover, vil der efter lovforslaget skulle registreres trafikdata

for vedkommende i 5 år. Er personen dømt for en lovovertrædelse i straffelovens kapitel 12 og 13, der har en strafferamme på 8 år eller derover, vil der efter lovforslaget skulle registreres trafikdata for vedkommende i 10 år.

Det vil således påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at registrere og opbevare trafikdata for personer dømt for grov kriminalitet. Personer, der er dømt for grov kriminalitet vil være i risiko for at recidivere til ny kriminalitet, herunder grov kriminalitet. Derudover må det antages, at disse personer til en vis grad har deres omgangskreds i kriminelle miljøer og dermed ofte vil have kontakt med andre kriminelle personer. Måltrettet personbestemt registrering og opbevaring af trafikdata vedrørende personer dømt for grov kriminalitet vil derfor give politiet mulighed for at efterforske eventuelle kriminelle forbindelser til grov kriminalitet, som tidligere dømte for grov kriminalitet måtte have. En forpligtelse for udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, til at foretage personbestemt måltrettet registrering og opbevaring for sådanne personer må derfor antages at kunne medvirke til at opklare og retsforfølge grov kriminalitet.

Det forudsættes, at registrering og opbevaring af trafikdata for personer dømt for grov kriminalitet kobles til den pågældende person, f.eks. via cpr-nummer (unikt ID). Det vil indebære, at der vil skulle ske registrering og opbevaring af trafikdata hidrørende fra alle kommunikationsmidler, som den pågældende person er registreret som slutbruger eller forventet bruger af. Der henvises til pkt. 3.4.2 i lovforslagets almindelige bemærkninger.

Det bemærkes, at det ikke i dag er muligt entydigt at identificere alle delikter ud fra en gerningskode i de relevante systemer. Det vil således ikke systemisk være muligt at adskille visse delikter, der indeholder flere strafferammer, fra hinanden. Det gælder eksempelvis straffelovens § 249 (uagtsom legemsbeskadigelse) og berigelsesforbrydelserne i §§ 285-287. I det omfang, det ikke er muligt entydigt at identificere et delikt ved en gerningskode, foreslås det, at der ikke vil kunne iværksættes registrering og opbevaring af trafikdata for så vidt angår de berørte delikter. Det vil bl.a. have den betydning, at der ikke vil kunne iværksættes registrering og opbevaring af trafikdata vedrørende personer dømt for tyveri og bedrageri. Det bemærkes

i denne forbindelse, at muligheden for fremadrettet systemisk at kunne understøtte en entydig identifikation af alle delikter i relevante systemer vil blive undersøgt i forbindelse med Rigspolitiets foranalyse, jf. pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det foreslås med *stk. 3*, at er den pågældende idømt en ubetinget frihedsstraf, regnes registreringsperioden, jf. det foreslåede *stk. 2*, nr. 1-3, fra tidspunktet for endelig løsladelse fra afsoning. Prøveløslades den pågældende, regnes perioden fra tidspunktet for prøveløsladelse. Er den pågældende idømt en betinget frihedsstraf, regnes perioden fra endelig dom. Er den pågældende idømt anden strafferetlig retsfølge efter straffelovens §§ 68-70, regnes perioden fra endelig ophævelse af denne retsfølge, dog regnes perioden fra endelig dom, hvis den pågældende er dømt til ambulant behandling, der ikke medfører eller kan medføre indlæggelse i institution.

Hvornår registreringsperioden vil skulle regnes fra, vil således afhænge af de omstændigheder, der gælder for den pågældende person.

Det vil som udgangspunkt ikke være muligt at registrere og opbevare trafikdata fra personer, der er under afsoning, medmindre politiet vurderer, at vedkommende efter en konkret vurdering har en forbindelse til grov kriminalitet, jf. de specielle bemærkninger til den foreslåede § 786 d i retsplejeloven.

Hvis den pågældende inden for registreringsperioden på ny dømmes for grov kriminalitet, der vil medføre, at der vil skulle registreres og opbevares oplysninger om den pågældende, vil der løbe en selvstændig registreringsperiode for denne registrering fra prøveløsladelse m.v., mens den igangværende registrering og opbevaring fortsætter, indtil den fastsatte frist. I disse tilfælde vil registrerings- og opbevaringsperioden muligvis løbe under en afsoning. Der vil ikke efter forslaget være mulighed for at slå registreringsperioder sammen.

Det foreslås desuden med *stk. 4*, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata fra

- 1) kommunikationsapparater, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1 eller 3,

- 2) personer, der, jf. § 783, stk. 2, har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1, eller 3,
- 3) personer, der er indehavere af et kommunikationsapparat, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1, eller 3, og
- 4) kommunikationsapparater, der har været genstand for indgreb i medfør af § 786, stk. 2.

Efter den foreslåede stk. 4, *nr. 1*, skal der ske registrering og opbevaring af trafikdata fra kommunikationsapparater, der, jf. retsplejelovens § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af retsplejelovens § 780, stk. 1, nr. 1 eller 3.

Den foreslåede bestemmelse vil medføre, at hvis retten afsiger en kendelse om eksempelvis aflytning af et bestemt telefonnummer eller IMEI-nummer, jf. retsplejelovens § 783, stk. 1, 2. pkt., vil der automatisk skulle ske registrering og opbevaring af trafikdata fra den pågældende telefon.

Efter den foreslåede stk. 4, *nr. 2*, skal der ske registrering og opbevaring af trafikdata fra personer, der, jf. retsplejelovens § 783, stk. 2, har været genstand for indgreb i medfør af retsplejelovens § 780, stk. 1, nr. 1 eller 3.

Den foreslåede bestemmelse vil medføre, at når retten afsiger en kendelse om aflytning af en bestemt person, jf. retsplejelovens § 783, stk. 2, vil der automatisk skulle ske registrering og opbevaring af trafikdata fra alle kommunikationsmidler, som den pågældende person benytter. Det samme gør sig gældende for personer, der har været genstand for et indgreb i meddelelseshemmeligheden i form af teleoplysning.

Det følger af den foreslåede stk. 4, *nr. 3*, at der skal ske registrering og opbevaring af trafikdata fra personer, der er indehavere af kommunikationsapparater, der, jf. retsplejelovens § 783, stk. 1, 2. pkt., har været genstand for et indgreb i medfør af retsplejelovens § 780, stk. 1, nr. 1 eller 3.

Den foreslåede bestemmelse vil gøre det muligt at registrere og opbevare trafikdata fra alle kommunikationsapparater, som en person er indehaver af, hvis blot et af apparaterne har været genstand for telefonaflytning eller teleobservation, jf. retsplejelovens § 780, stk. 1, nr. 1 eller 3. Den foreslåede bestemmelse vil eksempelvis få betydning, hvis en person skifter telefonnummer ofte eller er indehaver af flere kommunikationsapparater.

»Indehaver« skal forstås på samme måde som i retsplejelovens § 788, stk. 2, nr. 1, som indehaveren af nummeret, dvs. abonnementet eller apparatet afhængig af, hvad der har dannet grundlag for indgrebet.

Det forudsættes også i den forbindelse, at registrering og opbevaring af trafikdata for personer, der har været genstand for et af de omfattede indgreb, kobles til den pågældende persons unikke ID (f.eks. cpr-nummer). Det vil indebære, at der vil skulle ske registrering og opbevaring af trafikdata hidrørende fra alle kommunikationsmidler, som den pågældende er registreret som slutbruger eller, hvis denne kendes, bruger af. Der henvises til pkt. 3.4.2 i lovforslagets almindelige bemærkninger.

De nærmere regler for at foretage indgreb i meddelelshemmeligheden er beskrevet i pkt. 3.7.1.1-3.7.1.3 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede stk. 4, *nr. 4*, i retsplejelovens § 786 b, at der skal ske registrering af trafikdata fra kommunikationsapparater, der har været genstand for indgreb i medfør af retsplejelovens § 786, stk. 2. Efter § 786, stk. 2, kan der foretages indgreb i meddelelshemmeligheden i form af teleoplysning rettet mod en bestemt telefon eller andet kommunikationsapparat, uden at de almindelige betingelser i retsplejelovens § 781 er opfyldt, hvis indehaveren af apparatet har givet samtykke.

Den foreslåede bestemmelse vil medføre, at ligesom indehaveren af et kommunikationsapparat kan give samtykke til teleoplysning, kan indehaveren også give samtykke til registrering og opbevaring af trafikdata fra apparatet.

Det forudsættes således, at der i forbindelse med indhentelse af samtykke til teleoplysning også vil kunne indhentes samtykke til den efterfølgende tidsbegrænsede registrering og opbevaring af trafikdata. Det vil i den forbindelse være et krav, at samtykket er klart og utvetydigt og kommer fra den person, oplysningerne vedrører. Samtykket vil til enhver tid kunne trækkes tilbage.

Det foreslåede *stk. 5* indebærer følge, at trafikdata registreret og opbevaret i medfør af det foreslåede stk. 4 skal registreres i 1 år fra det tidspunkt, hvor indgrebet afsluttes.

Indgreb i medfør af retsplejelovens § 780, stk. 1, nr. 1, betragtes som afsluttet, når politiet har anmodet udbyderen om at tage aflytningen ned. For så vidt angår indhentelse af fremadrettet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3, betragtes indgrebet som afsluttet, når politiet inden udløbet af fristen for indgrebet anmoder udbyderen om at nedtage indgrebet, eller når fristen for indgrebet udløber, mens det for indhentelse af historiske teleoplysninger vil anses for afsluttet på tidspunktet for indhentelse af kendelsen herom.

Endelig foreslås det i *stk. 6*, at trafikdata registreret efter de foreslåede stk. 2-5 skal opbevares i 1 år.

Uanset registreringsperiodens længde, vil trafikdata registreret efter de foreslåede stk. 2-5 således skulle opbevares i 1 år.

Trafikdata, der opbevares med henblik på debitering, vil uanset om de pågældende data omfattes af en af de foreslåede registrerings- og opbevaringspligter som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktiv 2002/58 og § 10, stk. 2, i bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Måltrettet personbestemt registrering og opbevaring vil kunne prøves, jf. grundlovens § 63. Vedrørende domstolsprøvelse henvises i øvrigt til pkt. 3.6 i lovforslagets almindelige bemærkninger.

Til § 786 c

Det foreslås, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk måltrettet registrering og opbevaring på grundlag af objektive og ikke-diskriminerende forhold, der tilsiger, at der i et givet område er en forhøjet risiko for, at planlægges eller begås grov kriminalitet.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.1.3.1 i lovforslagets almindelige bemærkninger.

Registrerings- og opbevaringspligten vil efter forslaget skulle gælde fra det tidspunkt, hvor udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, har modtaget tilstrækkelige oplysninger om de omfattede områder fra myndighederne til at iværksætte registrering og opbevaring målrettet de pågældende områder. Der henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det foreslås, at der indsættes en ny § 786 c, hvor det i *stk. 1* fastsættes, at det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på områder på 3 km gange 3 km, hvor

- 1) antallet af anmeldelser om lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelse eller overtrædelser som omfattet af § 781, stk. 2 eller 3, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, eller
- 2) antallet af beboere dømt for lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelse eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Det bemærkes, at det ikke i dag er muligt entydigt at identificere alle delikter ud fra en gerningskode i de relevante systemer. Det vil således ikke systemisk være muligt at adskille visse delikter, der indeholder flere strafferammer, fra hinanden. Det gælder eksempelvis straffelovens § 249 (uagtsom legemsbeskadigelse) og berigelsesforbrydelserne i §§ 285 og 287. I det omfang, det ikke er muligt entydigt at identificere et delikt ved en gerningskode, foreslås det, at der ikke vil kunne iværksættes registrering og opbevaring af trafikdata for så vidt angår de berørte delikter. Det vil eksempelvis have den betydning, at der ikke vil kunne iværksættes registrering og opbevaring af trafikdata vedrørende personer dømt for tyveri og bedrageri. Det

bemærkes i denne forbindelse, at muligheden for fremadrettet systemisk at kunne understøtte en entydig identifikation af alle delikter ud fra en gerningskode i relevante systemer vil blive undersøgt i forbindelse med Rigspolitiets foranalyse, jf. pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det bemærkes desuden, at master tilhørende udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, er placeret forskelligt. Områder, der geografisk er placeret i nærheden af et område på 3 gange 3 km, hvor der vil skulle foretages målrettet geografisk registrering og opbevaring, vil derfor også, pga. disse tekniske forhold, i et større eller mindre omfang kunne blive omfattet af den registrering og opbevaring, udbyderne iværksætter – afhængig af antallet af masterne og deres placering. Det forudsættes i den forbindelse, at udbyderne iværksætter registreringen og opbevaringen af trafikdata, så registreringen alene omfatter det område, der er strengt nødvendigt. Det påhviler i den forbindelse udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at udpege de fornødne master, således at det angivne område dækkes fuldstændigt. Det forudsættes i den forbindelse, at udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, ved udpegningen af de fornødne master tager højde for bygningsmassen og andre forhold, der typisk vil kunne forårsage såkaldte mastespring. Det vil bl.a. indebære, at det typisk vil være nødvendigt at medtage master uden for området på 3 km gange 3 km, da telefoner vil være mere tilbøjelige til at springe på master, der er placeret længere væk, såfremt disse er mindre belastede af trafikdata end de master, der befinder sig tættest ved telefonen. Er dette tilfældet, vil de oplysninger, der registreres og opbevares, være omfattet af den målrettede geografiske registrering og opbevaring. Det betyder, at politiet og anklagemyndigheden vil kunne få adgang til disse trafikdata, og at disse oplysninger på samme vis som øvrige oplysninger, der registreres og opbevares som følge af en af de foreslåede registrerings- og opbevaringspligter, kan anvendes i efterforskninger og som bevis i straffesager. Det skal ses i lyset af, at det ikke er muligt at frasortere data inden for de enkelte cellers rækkevidde, som stammer fra telefoner, der reelt har befundet sig uden for de udpegede områder.

Det er desuden vurderingen, at der er områder, hvor der er særlige beskyttelseshensyn, der kan begrunde, at området anses for at være særligt sikringskritisk, og at der på den baggrund kan være behov på at foretage registrering og opbevaring af trafikdata vedrørende sådanne områder. Eksempelvis på baggrund af en vurdering af, at der er tale om et trafikknudepunkt, som en stor mængde personer jævnligt passerer igennem, at der i området kan befinde sig særligt sikringskritiske personer, eller at der er tale om et område, der på grundlag af sin funktion i sig selv er særligt sikringskritisk.

Det foreslås derfor med den foreslåede bestemmelses *stk. 2*, at det skal påhvile udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata vedrørende særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.

Det vil kun være muligt at iværksætte målrettet geografisk registrering og opbevaring af særligt sikringskritiske områder, hvis der i forhold til det konkrete område vurderes at være særlige beskyttelseshensyn, der kan begrunde, at området anses for at være særligt sikringskritisk.

Politiets ejendomme vil f.eks. kunne være Politigården, Rigspolitiets øvrige lokationer, politistationer, Politiskolens uddannelsescentre m.v.

Broforbindelser vil f.eks. kunne være Øresundsbroen, Storebæltsbroen, begge Lillebæltsbroer, Storstrømsbroen, Sallingsundbroen, Vejlefjordbroen, Svendborgsundbroen, Limfjordsbroen og Langebro, Knippelsbro, Kalvebodbroen og Sjællandsbroen.

Tunnelforbindelser vil f.eks. kunne være Nordhavnsvejtunnelen, Frederikssundsvejtunnelen, Silkeborgtunnelen, Tårnbytunnelen, Limfjordstunnelen, Øresundstunnelen og Guldborgsundtunnelen.

Færgeforbindelser vil f.eks. kunne være nationale færgeruter såsom færgeruterne mellem Aarhus og Sjællands Odde, Aalborg og Egholm, Esbjerg og

Fanø, Frederikshavn og Læsø, Grenå og Anholt, Svendborg og Ærøskøbing, samt internationale færgeruter såsom færgeruterne mellem København og Oslo, Gedser og Rostock, Helsingør og Helsingborg, København og Swinoujscie, Rødby og Puttgarden, Rømø og Sylt, København og Hven, Rønne og Ystad og Hirsthals og Kristiansand.

Ved trafikknudepunkter forstås områder, hvor flere færdselslinjer og -typer løber sammen eller skærer hinanden. Det vil f.eks. kunne være områderne omkring Nørreport, Vesterport, Østerport og Hovedbanegården i København, Nørreport og Hovedbanegården i Aarhus, trafikerede motorvejskryds, såsom Motorvejskryds Aarhus Nord, Motorvejskryds Skærup-Frøslev, Motorvejskryds Kgs. Lyngby-Virum, Motorvejskryds Køge Vest, trafikerede motorvejsstrækninger, såsom Køge Bugt Motorvejen, Helsingørmotorvejen, Motorring 3, Holbækmotorvejen, Østjyske Motorvej, Sønderjyske Motorvej, Hillerødmotorvejen og Taulovmotorvejen samt trafikerede ringveje rundt om de større byer i Danmark, f.eks. Nordre Ringvej i Silkeborg, Gjesing Ringvej i Esbjerg, Ring 2 i Hillerød, Ring 2, 3 og 4 i København, Ring 1 og 2 i Roskilde og Ringvejen i Køge.

Ved større indfaldsveje forstås indfaldsveje til de større byer i Danmark, f.eks. Lyngbyvej, Nørre Allé, Åboulevarden, Roskildevej, Folehaven og Ellebjergvej i København; Skanderborgvej, Åhavevej, Marselis Boulevard, Silkeborg Vej, Edwin Rahrs Vej og Grenåvej i Aarhus; Otterupvej, Ørbækvej, Munkebjergvej og Assensvej i Odense; samt Storegade og Jernevej i Esbjerg.

Ved grænseovergange forstås både grænseovergange på land, havne og lufthavne, f.eks. grænseovergangene på land ved Padborg, Kruså, Vilmkær, Sæd og Siltoft, havne som Aarhus Havn, Frederikshavn Havn, Ærøskøbing Havn og lufthavne som Lolland-Falster Airport, Grønholm Flyveplads og Lemvig Flyveplads.

Ved busterminaler forstås holdepladser for et større antal buslinjer, f.eks. Aarhus Rutebilstation, Esbjerg Rutebilstation, Aalborg Busterminal og København Busterminal.

Ved fjernbanestationer forstås stationer på fjerntogsruter, eksempelvis togstationerne i Roskilde, Odense, Aarhus, Esbjerg og Aalborg.

Ved stationer på bybaner forstås stationer på metro, letbaner og S-baner, som udfører transport i byer og forstæder. Det kan eksempelvis være metrostationer i København, stationer på letbanen i Aarhus og stationer på S-togsforbindelser i København.

Ved militære områder forstås alle militære anlæg og områder, herunder militære flyvestationer, dvs. flyvepladser som anvendes af forsvaret.

Ved kolonne 3-virksomheder forstås virksomheder, som har oplag af brand- og eksplosionsfarlige stoffer, giftige stoffer eller miljøfarlige stoffer.

Ved offentligt godkendte flyvepladser forstås offentlige flyvepladser, som er certificeret på baggrund af Kommissionens forordning (EU) nr. 139/2014 af 12. februar 2014 om fastsættelse af krav og administrative procedurer for flyvepladser i henhold til Europa Parlamentets og Rådets forordning (EF) nr. 216/2008 eller certificeret i henhold til BL 3-1, Bestemmelser om etablering af offentlige VMC-flyvepladser eller BL 3-2, Bestemmelser om etablering af offentlige IMC-flyvepladser. En oversigt over danske offentligt godkendte flyvepladser fremgår af AIP Danmark (aim.naviair.dk). Offentligt godkendte flyvepladser er f.eks. lufthavnene i København Kastrup, Roskilde, Karup, Billund, Aalborg, Rønne, Esbjerg, Sindal, Sønderborg og Odense.

Der er med ovennævnte eksempler på forskellige særligt sikringskritiske områder ikke er tale om en udtømmende liste.

Det foreslås, at pligten til at foretage geografisk målrettet registrering og opbevaring i de foreslåede stk. 1 og 2 vil skulle omfatte de data, der er registrerings- og opbevaringspligtige i dag.

Der henvises til pkt. 3.1.3.4 og 3.2.3.3 i lovforslagets almindelige bemærkninger for en nærmere omtale af, hvad der forstås ved trafikdata.

Det vil kunne variere over tid, hvor i landet der er en forhøjet risiko for, at der planlægges eller begås grov kriminalitet m.v. og hvilke områder der vurderes at være særligt sikringskritiske. Den nærmere registrering og opbevaring af trafikdata for områder, hvor der er en sådan forhøjet risiko, vil således skulle tilpasses løbende ud fra en vurdering af det aktuelle kriminalitetsbillede.

Det foreslås på den baggrund, at myndighederne årligt skal udarbejde en oversigt over områder omfattet af de foreslåede § 786 c, stk. 1 (områder med et større antal anmeldelser om grov kriminalitet og områder med et større antal beboere dømt for grov kriminalitet) og 2 (særligt sikringskritiske områder). Af oversigten vil skulle fremgå tilstrækkelige oplysninger til så præcist som muligt at udpege de oplistede omfattede geografiske områder, eksempelvis ved angivelse af præcise koordinater. Oversigten vil skulle videreformidles til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, med henblik på iværksættelse af målrettet registrering og opbevaring på de oplistede områder. Det forudsættes, at oplysninger om de omfattede geografiske områder og personer samt oplysningerne om de konkrete pålæg vedrørende personer og områder alene videreformidles til ansatte hos udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, der er sikkerhedsgodkendt til at håndtere følsomme oplysninger om indgreb i meddelelshemmeligheden fra politiet. Der henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Det foreslås i bestemmelsens *stk.* 3, at trafikdata registreret efter stk. 1 og 2 skal opbevares i 1 år.

Trafikdata, der opbevares med henblik på debitering, vil uanset om de pågældende data omfattes af en af de foreslåede registrerings- og opbevaringspligter som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktiv 2002/58 og § 10, stk. 2, i bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Det foreslås desuden, at det i bestemmelsens *stk.* 4 fastsættes, at Justitsministeren efter forhandling med erhvervsministeren kan fastsætte nærmere regler om målrettet geografisk registrering og opbevaring af trafikdata som nævnt i de foreslåede stk. 1.

Der vil i den forbindelse eksempelvis kunne fastsættes nærmere regler om registrering og opbevaring af trafikdata i områder på 3 km gange 3 km, hvor antallet af anmeldelser af grov kriminalitet begået i området udgør mindst

1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, ligesom der vil kunne fastsættes nærmere regler om registrering og opbevaring af trafikdata i områder på 3 km gange 3 km, hvor antallet af beboere dømt for grov kriminalitet udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år. Der vil f.eks. kunne fastsættes regler om en nærmere inddeling af Danmark i kvadrater på 3 km gange 3 km ud fra objektive og ikke-diskriminerende forhold.

Måltrettet geografisk registrering og opbevaring vil kunne prøves, jf. grundlovens § 63. Vedrørende domstolsprøvelse henvises i øvrigt til pkt. 3.6 i lovforslagets almindelige bemærkninger.

Til § 786 d

Det foreslås, at der indsættes en ny § 786 d i retsplejeloven, hvor det i *stk. 1*, fastsættes, at der kan meddeles udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, pålæg om at foretage måltrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, hvis der er grund til at antage, at de har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller overtrædelser der kan medføre strafforhøjelse efter straffelovens § 81 a.

Den foreslåede § 786 d i retsplejeloven er ny og giver mulighed for at pålægge udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage måltrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, der er grund til at antage har forbindelse til grov kriminalitet.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.1.3.1 i lovforslagets almindelige bemærkninger.

Med den foreslåede bestemmelse vil der kunne meddeles pålæg om registrering og opbevaring af trafikdata fra kommunikationsapparater eller per-

soner, som politiet har grund til at antage har en forbindelse til grov kriminalitet, uden at der har været tilstrækkeligt grundlag for at domfælde eller at iværksætte indgreb i meddelelshemmeligheden mod de pågældende, jf. den foreslåede bestemmelse i § 786 b.

Tilsvarende vil der med den foreslåede bestemmelse kunne meddeles pålæg om registrering og opbevaring af trafikdata for et område, uden at dette er omfattet af den foreslåede § 786 c. Der vil således kunne meddeles pålæg om registrering og opbevaring af trafikdata fra bestemte områder, hvor politiet har grund til at antage, at der planlægges eller begås grov kriminalitet.

Det foreslåede krav om, at der skal være grund til at antage, at kommunikationsapparater, personer eller bestemte områder har en forbindelse til grov kriminalitet vil medføre, at kravet for at foretage målrettet registrering og opbevaring af trafikdata efter den foreslåede § 786 d i retsplejeloven vil være lavere, end det krav, der gælder for at foretage indgreb i meddelelshemmeligheden efter den gældende § 781, stk. 1, nr. 1. Dette skal ses i lyset af, at der på tidspunktet for iværksættelse af registrering og opbevaring af trafikdata ikke nødvendigvis vil være nogen særlig konkret mistanke om, at en bestemt person har begået eller vil begå en lovovertrædelse, eller at der er eller vil blive begået lovovertrædelser på et bestemt område. Der vil derfor også kunne meddeles pålæg om registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, når politiet har grund til at antage, at der er en forbindelse til planlægning af grov kriminalitet.

Det vil bero på en konkret vurdering, om kravet er opfyldt.

Politiet vil efter en konkret vurdering f.eks. kunne anmode retten om at træffe afgørelse om meddelelse af pålæg om registrering og opbevaring af trafikdata fra:

- kommunikationsapparater, som politiet har grund til at antage benyttes eller har været benyttet i forbindelse med kriminelle aktiviteter, uanset at brugeren af apparatet ikke konkret kan identificeres,
- mistænkte personer, der er, eller har været, genstand for tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet, og som ikke er omfattet af muligheden for at registrere og opbevare trafikdata fra personer, der har været genstand for indgreb efter retsplejelovens § 780, stk. 1, nr. 1 eller 3,

- personer, der er undergivet systematisk, politimæssig monitoring, eksempelvis inden for rocker- og bandeområdet, randpersoner fra rocker-/bandemiljøet,
- personer, der har været i kontakt med personer, der er eller har været genstand for et tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet,
- afsonere,
- forurettede og
- personer med nære relationer til personer, der har forbindelse til grov kriminalitet, som f.eks. ægtefæller eller samlevende.

Politiet vil desuden efter en konkret vurdering kunne anmode retten om at træffe afgørelse om meddelelse af pålæg om registrering og opbevaring af trafikdata vedrørende eksempelvis bestemte områder, hvor der midlertidigt er grund til at antage, at der er en forhøjet risiko for, at grov kriminalitet begås eller planlægges, f.eks. i forbindelse med større forsamlinger, områder for statsbesøg, festivaler, konkrete efterforskninger for grov kriminalitet, herunder for mistanke om overtrædelse af straffelovens kapitel 12 og 13 m.v.

For så vidt angår målrettet geografisk registrering og opbevaring på baggrund af konkret begrundede pålæg bemærkes det, at størrelsen af det bestemte område vil afhænge af den konkrete forbindelse til grov kriminalitet. Hvis der eksempelvis er mistanke om et forestående bandedrab eller mistanke om et forestående terrorangreb, vil området omfattet af det konkret begrundede pålæg kunne udstrækkes til at omfatte hele det nødvendige område, f.eks. til en hel bydel eller en landsdel. Det forudsættes, at domstolene som led i proportionalitetsvurderingen vil tage højde for, at registrering og opbevaring af trafikdata afgrænses til det strengt nødvendige under hensyntagen til kriminalitetens art, og hvad der er teknisk muligt, jf. nedenfor om proportionalitetskravet.

Kommunikationsapparater, personer eller bestemte områder, der hidtil har været registreret og opbevaret trafikdata for efter en af de andre foreslåede hjemler relateret til målrettet personbestemt eller geografisk registrering og opbevaring, vil også kunne blive genstand for et konkret begrundet pålæg om registrering og opbevaring af trafikdata. I så fald vil det på lige fod med øvrige konkret begrundede pålæg være en betingelse, at politiet har grund til at antage, at kommunikationsapparatet, personen eller området har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3

år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelse eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

En forbindelse til grov kriminalitet vil i sagens natur navnlig foreligge, hvis personen pga. mistanke om grov kriminalitet har været genstand for tvangsindgreb efter retsplejelovens kapitel 70-75, uden at der derved er grundlag for at anvende bestemmelsen i den foreslåede § 786 b. Eksempelvis ved foretagelse af ransagning hos denne person. Tilsvarende vil bestemmelsen kunne anvendes på personer, der afsoner en dom for begået grov kriminalitet.

Politiet vil også efter en konkret vurdering f.eks. kunne anmode om meddelelse af pålæg om registrering og opbevaring af trafikdata for kommunikationsapparater, personer og områder, som Politiets Efterretningstjeneste behandler oplysninger om, og for områder, der er undergivet systematisk, politimæssig monitoring, eksempelvis rocker- og bandemiljøer.

En forbindelse til grov kriminalitet kan eksempelvis også være, hvis der i en persons omgangskreds eller lignende er personer, der begår eller har begået grov kriminalitet, f.eks. rocker-/bandemedlemmer eller lignende, og der ved at foretage målrettet registrering og opbevaring af trafikdata for personen kan fremskaffes oplysninger om disse personer selv, uanset om vedkommende selv er bandemedlem eller mistænkes for at være involveret i lovovertrædelser. Dette kan f.eks. være personer med nære relationer til personer, der har forbindelse til grov kriminalitet, som f.eks. ægtefæller eller samlevende, hvis der eksempelvis er en risiko for, at personen med forbindelse til grov kriminalitet vil anvende f.eks. en mobiltelefon fra en sådan person eller tage kontakt til en sådan person. Tilsvarende vil bestemmelsen kunne anvendes på randpersoner fra rocker-/bandemiljøet, personer med kontakt til menneskesmuglere eller andre organiserede kriminelle eller på personer, der i øvrigt har været i kontakt med personer, der er eller har været genstand for et tvangsindgreb i retsplejelovens kapitel 70-75 på baggrund af grov kriminalitet.

En forbindelse til grov kriminalitet kan eksempelvis også være, hvis der er grund til at antage, at personer, der begår eller har begået grov kriminalitet, opholder sig et bestemt sted. F.eks. hvis der er grund til at antage, at rocker-

/bandemedlemmer ofte opholder sig på et bestemt sted, f.eks. en rockerborg, et særligt stamværtshus, en bestemt park boligområde eller lignende, hvor der ikke er grundlag for at anvende den foreslåede § 786 c til at foretage registrering og opbevaring af trafikdata.

De ovenstående eksempler er ikke udtømmende. Det må bero på en konkret vurdering, om der kan meddeles pålæg efter bestemmelsen.

Endelig behøver en forbindelse til grov kriminalitet ikke være knyttet til en identificeret person. Forbindelsen kan også være et »kommunikationsapparat«, der er grund til at antage har en forbindelse til grov kriminalitet. Eksempelvis fordi en bestemt telefon bliver eller tidligere er blevet anvendt i forbindelse med kriminelle aktiviteter, uanset at de eller de konkrete brugere ikke er kendte.

Det bemærkes desuden, at en forbindelse til en af de omfattede lovovertrædelser m.v. også omfatter planlægning af sådanne lovovertrædelser m.v.

Registrerings- og opbevaringspligten vil efter forslaget skulle gælde fra det tidspunkt, hvor myndighederne har videreformidlet en indhentet retskendelse til udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden. Der henvises til pkt. 3.1.3.4 i lovforslagets almindelige bemærkninger.

Med den foreslåede § 786 d i retsplejeloven vil der kunne iværksættes målrettet registrering og opbevaring for alle typer trafikdata. Der henvises til pkt. 3.1.3.4 og 3.2.3.3 i lovforslagets almindelige bemærkninger for en nærmere omtale af, hvad der forstås ved trafikdata.

Den foreslåede *stk. 2* i § 786 d, vedrører domstolskontrollen med registrering og opbevaring af trafikdata efter bestemmelsen.

Det fremgår af den foreslåede bestemmelse i *stk. 2, 1. pkt.*, at afgørelse om pålæg om registrering og opbevaring efter den foreslåede § 786 d, *stk. 1*, træffes af retten ved kendelse. Dette svarer til, hvad der gælder for så vidt angår indgreb i meddelelshemmeligheden, jf. § 783, *stk. 1, 1. pkt.* Politiet vil kunne foretage indgreb på øjemedet, jf. nærmere nedenfor om den foreslåede henvisning til § 783, *stk. 4*, i § 786 d, *stk. 4*.

Det fremgår af den foreslåede bestemmelse i stk. 2, 2. pkt., i retsplejeloven, at kendelsen skal fastsætte det tidsrum, inden for hvilket indgrebet kan foretages. Videre fremgår det af den foreslåede bestemmelse i stk. 2, 3. pkt., at dette tidsrum skal være så kort som muligt og ikke må overstige 6 måneder. I forlængelse heraf fremgår det af den foreslåede bestemmelse i stk. 2, 4. pkt., at tidsrummet kan forlænges, men højst med 6 måneder ad gangen. Forlængelsen skal efter det foreslåede stk. 2, 5. pkt., ske ved kendelse. Endelig fremgår det af det foreslåede stk. 2, 6. pkt., at kendelsen skal angive den person, det kommunikationsapparat eller det område, som indgrebet angår.

Det foreslåede bestemmelse i stk. 2, 6. pkt. vil medføre, at der for registrering og opbevaring af trafikdata efter bestemmelsen kommer til at gælde regler svarende til, hvad der efter gældende ret findes for indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 783, stk. 1, 2. pkt., og stk. 2, hvorefter der i en kendelse om indgreb i meddelelseshemmeligheden skal anføres hhv. de telefonnumre, lokaliteter, adressater, forsendelser eller den, person som indgrebet angår.

En kendelse om registrering og opbevaring af trafikdata efter bestemmelsen vil ikke nødvendigvis skulle identificere en person ved dennes navn. Anden form for identifikation tænkes at kunne ske ved angivelse af et telefonnummer, IMEI-nummer eller lignende, som kan identificere den pågældende.

Måltrettet personbestemt registrering og opbevaring af trafikdata kobles til den pågældende persons unikke ID (f.eks. cpr-nummer). Det vil indebære, at udbydere skal registrere og opbevare trafikdata hidrørende fra alle kommunikationsmidler, som den pågældende person er eller i kendelsesperioden bliver registreret som abonnent for eller bruger af. Der henvises til pkt. 3.4.2 i lovforslagets almindelige bemærkninger. Herudover vil politiet i kendelsesperioden kunne give meddelelse til udbydere om registrering og opbevaring af trafikdata fra telefonnumre, som der er grunde til at antage, at den pågældende ved afsigelsen af kendelsen eller i kendelsesperioden benytter uden at være registreret som abonnement eller bruger af, jf. herom nedenfor om det foreslåede § 786 d, stk. 2, 7. og 8. pkt.

Det fremgår af det foreslåede § 786 d, stk. 2, 7. pkt., i retsplejeloven, at reglerne i § 783, stk. 2, 2., 3. og 5.-7. pkt., finder tilsvarende anvendelse ved pålæg om registrering og opbevaring af trafikdata for personer. Dette er en

følge af, at politiet løbende i kendelsesperioden kan meddele teleselskaberne, at registrering og opbevaring af trafikdata skal udvides til konkrete telefonnumre, som der er grund til at antage, at den person, som indgrebet retter sig mod, benytter uden at være registreret som abonnent for eller bruger af.

Den foreslåede henvisning til retsplejelovens § 783, stk. 2, 2. pkt., vil medføre, at politiet snarest muligt efter udløbet af det tidsrum, inden for hvilket indgrebet kan foretages, underretter retten om de telefonnumre, som indgrebet har været rettet imod, og som pågældende ikke har været registreret som abonnent for eller bruger af. Den foreslåede henvisning til § 783, stk. 2, 3. pkt., vil medføre, at hvis særlige forhold taler for det, skal underretning ske senest 24 timer efter indgrebets iværksættelse.

Med udtrykket »særlige forhold« sigtes til tilfælde, hvor der kan være anledning til at give den beskikkede advokat, jf. henvisningen til §§ 784 og 785 i det foreslåede § 786 d, stk. 4, 1. pkt., mulighed for hurtig efterprøvelse fra rettens side. Der kan navnlig være tale om tilfælde, hvor særlige principielle hensyn kan siges at gøre sig gældende, f.eks. hvor der måtte opstå spørgsmål om registrering og opbevaring af trafikdata fra kommunikationsapparater, der anvendes af advokater, læger eller journalister.

De foreslåede henvisninger til retsplejelovens § 783, stk. 2, 5.-7. pkt., vil medføre, at retten underretter den beskikkede advokat, jf. henvisningen til § 784, stk. 1, i den foreslåede § 786 d, stk. 4, 1. pkt., der herefter kan indbringe spørgsmålet om lovligheden af indgrebet for retten, samt at retten træffer afgørelse ved kendelse. Burde indgrebet efter rettens opfattelse ikke være foretaget, skal retten give meddelelse herom til Justitsministeriet.

Formålet med henvisningerne er at sikre en adgang til kontrol ved domstolene med hensyn til de konkrete telefonnumre, for hvilke politiet i kendelsesperioden har pålagt teleselskaberne at foretage registrering og opbevaring af trafikdata. Hvis sagen indbringes for retten af den beskikkede advokat, afgør retten ved kendelse, om indgrebet er sket inden for rammerne af den forudgående retskendelse på personen. Hvis sagen indbringes for retten af den beskikkede advokat, afgør retten ved kendelse, om indgrebet er sket inden for rammerne af den forudgående retskendelse på personen.

Det foreslås ikke at henvise til retsplejelovens § 783, stk. 2, 4. pkt., hvorefter underretningen skal indeholde en angivelse af de bestemte grunde, der er til

at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte, hvilket svarer til kravet for at foretage indgreb i meddelelseshemmeligheden, jf. § 781, stk. 1, nr. 1. Som forklaret ovenfor foreslås der et lavere krav til målrettet registrering og opbevaring af trafikdata i § 786 d, stk. 1, end det, der gælder i § 781, stk. 1, nr. 1. I stedet foreslås det med § 786 d, stk. 2, 8. *pkt.*, at underretningen skal indeholde en angivelse af de grunde, der er til at antage, at den person, som indgrebet angår, benytter sig af de pågældende numre.

Det foreslåede § 786 d, stk. 2, 6.-8. *pkt.*, indebærer således sammen med det foreslåede stk. 1, at hvis der er grund til at antage, at en person har en forbindelse til grov kriminalitet, så kan der ske registrering og opbevaring af trafikdata dels fra alle de apparater, som vedkommende er eller bliver registreret som abonnent for eller bruger af, dels fra alle de apparater, som der er grund til at antage, at vedkommende i øvrigt benytter.

Det foreslåede stk. 2 vil indføre en ordning med forudgående retskendelse for registrering og opbevaring af trafikdata efter den foreslåede § 786 d, stk. 1, i retsplejeloven, som kendes fra retsplejelovens regler om indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 783, dog med den forskel, at tidsrummet for pålægget efter forslaget skal være så kort som muligt og ikke må overstige 6 måneder, hvor indgreb i meddelelseshemmeligheden højst kan foretages for 4 uger ad gangen, jf. retsplejelovens § 783, stk. 3, 2. *pkt.*

Dette skal ses i lyset af, at det indgreb, som består i registrering og opbevaring af trafikdata, alt andet lige må anses for mindre indgribende end f.eks. et indgreb i meddelelseshemmeligheden som aflytning, hvor indgrebet også omfatter al indholdet af en elektronisk kommunikation. Der er således ikke på samme måde som ved eksempelvis aflytning af en person tale om en krænkelse af det væsentligste indhold af de grundlæggende rettigheder fastslået i Chartrets artikel 7 og 8, jf. Tele2-dommens præmis 101.

Registrering og opbevaring af trafikdata kan imidlertid have en indvirkning på brugen af de elektroniske kommunikationsmidler og følgelig på brugerne af disse midlers udøvelse af deres ytringsfrihed, som er sikret ved Chartrets artikel 11, jf. Tele2-dommens præmis 101. Der vil derfor være behov for, at tidsrummet for de konkret begrundede pålæg ikke går videre, end hvad der er strengt nødvendigt, jf. Tele2-dommens præmis 108.

Der vil være mange forskellige situationer, der vil kunne resultere i et konkret begrundet pålæg om registrering og opbevaring af trafikdata for bestemte personer eller områder med forbindelse til grov kriminalitet. Der kan både være tale om personer og områder med en relativt stærk forbindelse til grov kriminalitet, og der kan være tale om personer og områder med en mere indirekte forbindelse til grov kriminalitet. Der bør derfor efter Justitsministeriets opfattelse være mulighed for at fastsætte, at et konkret begrundet pålæg skal gælde i op til 6 måneder. Ved vurderingen af, hvor længe tidsrummet for pålægget skal være, vil der kunne lægges vægt på de konkrete omstændigheder i sagen. Er der eksempelvis tale om, at der i forbindelse med et tidsbegrænset arrangement (eksempelvis en fodboldkamp, en festival el. lign.) anmodes om registrering og opbevaring af trafikdata i et nærmere bestemt område, vil tidsrummet skulle fastsættes, så det indsnævres til det strengt nødvendige i relation til det pågældende arrangement. Er der tale om et konkret begrundet pålæg vedrørende en person, som ønskes registreret og opbevaret trafikdata for, fordi der er grund til at antage, at vedkommende har en forbindelse til et større netværk, der forsøges optrevlet, kan der imidlertid foreligge omstændigheder, der kan tilsige, at tidsrummet fastsættes til 6 måneder. Tilsvarende kan gøre sig gældende, hvis der er tale om et konkret begrundet pålæg vedrørende et område, hvor politiet med henblik på bekæmpelse af grov kriminalitet har interesse i at følge området i en længere periode, fordi der er grund til at antage, at det område har en forbindelse til grov kriminalitet.

Det foreslås, at det i bestemmelsens *stk. 3* fastsættes, at oplysninger registreret i medfør af pålæg meddelt efter den foreslåede § 786 d, *stk. 1*, vil skulle opbevares i 1 år.

Trafikdata, der opbevares med henblik på debitering, vil uanset om de pågældende data omfattes af en af de foreslåede registrerings- og opbevaringspligter som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, *stk. 2*, i direktiv 2002/58 og § 10, *stk. 2*, i bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Det fremgår af den foreslåede § 786 d, *stk. 4*, i retsplejeloven, at lovens § 782, *stk. 1*, § 783, *stk. 1*, 3. og 4. pkt., samt *stk. 4*, og §§ 784 og 785 finder tilsvarende anvendelse.

Henvisningen til retsplejelovens § 782, stk. 1, indebærer, at reglen om proportionalitet finder anvendelse. Bestemmelsen i § 782, stk. 1, udtrykker det almindelige proportionalitetsprincip, der gælder for straffeprocessuelle tvangsindgreb. Dette foreslås overført til registrering og opbevaring af trafikdata efter § 786 d.

Forslaget vil have den virkning, at pålæg om målrettet registrering og opbevaring efter den foreslåede § 786 d, stk. 1, ikke må meddeles, 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, vil være et uforholdsmæssigt indgreb. Dette kan eksempelvis være tilfældet, hvis der ved et pålæg om registrering og opbevaring af trafikdata for et bestemt område ikke er proportionalitet mellem størrelsen af det relevante område, og den begåede grove kriminalitet i området. Det vil også være tilfældet, hvis registrering og opbevaring af trafikdata efter bestemmelsen ikke er proportionalt i forhold til den kriminalitet, der danner grundlag for indgrebet. Eksempelvis vil målrettet registrering og opbevaring alene på grundlag af en formodning om en overtrædelse af straffelovens § 110 e om offentlig forhånelse af en fremmed nations flag formentlig kun sjældent være proportionalt, uanset at denne bestemmelse er placeret i straffelovens kapitel 12, der er omfattet af den foreslåede § 786 d, stk. 1.

Henvisningen til retsplejelovens § 783, stk. 1, 3. pkt., i den foreslåede § 786 d, stk. 4, i retsplejeloven vil medføre, at der i kendelsen om registrering og opbevaring af trafikdata efter bestemmelsen skal anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for registrering og opbevaring er opfyldt. Henvisningen til retsplejelovens § 783, stk. 1, 4. pkt., vil medføre, at kendelsen om registrering og opbevaring af trafikdata til enhver tid kan omgøres. Dette kan eksempelvis være tilfældet, hvis betingelserne for at foretage registrering og opbevaring af trafikdata ikke længere er opfyldt, eller at det ville være uproportionalt at fortsætte registreringen og opbevaringen, uanset at det tidsrum, hvori indgrebet må foretages, jf. retsplejelovens § 783, stk. 4, endnu ikke er udløbet.

Den foreslåede henvisning til retsplejelovens § 783, stk. 4, vil medføre, at registrering og opbevaring af trafikdata efter bestemmelsen kan ske uden forudgående retskendelse, hvis øjemedet ellers ville forspildes, jf. § 783, stk.

4, 1. pkt. I sådanne tilfælde vil politiet skulle indbringe spørgsmålet for retten snarest muligt og senest inden 24 timer fra indgrebs iværksættelse, jf. § 783, stk. 4, 2. pkt.

Henvisningen til retsplejelovens §§ 784 og 785 i den foreslåede § 786 d, stk. 4, indebærer, at reglerne om advokatbeskikkelse finder anvendelse på pålæg om registrering og opbevaring af trafikdata efter den foreslåede § 786 d, stk. 1.

Den foreslåede henvisning vil have den virkning, at der i forbindelse med pålæg om registrering og opbevaring af trafikdata efter den foreslåede § 786 d, stk. 1, vil skulle ske beskikkelse af en advokat, der varetager interesserne for den eller de personer, hvis oplysninger er genstand for målrettet registrering og opbevaring. Dette svarer til, hvad der i dag gælder for personer, der er genstand for indgreb i meddelelshemmeligheden.

Der henvises til pkt. 3.6.3.2 og 3.7.1.2 i lovforslagets almindelige bemærkninger.

Til § 786 e

Det foreslås, at der indsættes en ny § 786 e i retsplejeloven, hvor det i *stk. 1, 1. pkt.*, fastsættes, at justitsministeren efter forhandling med erhvervsministeren kan fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.2.3.1 i lovforslagets almindelige bemærkninger.

Det forudsættes, at justitsministeren vil skulle foretage vurderingen af, om der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, på baggrund af en gennemgang af aktuelle straffesager omhandlende overtrædelser af bestemmelserne i straffelovens kapitel 12 og 13, herunder både verserende sager og sager, hvori der er sket domfældelse, samt på baggrund af Center for Terroranalysens ”Vurderingen af Terrortruslen

mod Danmark” og øvrige relevante analyseprodukter. Der henvises til pkt. 3.2.3 i de almindelige bemærkninger til lovforslaget.

Hvis det vurderes, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, kan der fastsættes regler om, at der i hele landet skal registreres og opbevares trafikdata generelt og udifferentieret.

Det foreslås, at registrering og opbevaring vil kunne iværksættes for de data, der er registrerings- og opbevaringspligtige i dag. Det vil sige de data, der efter retsplejelovens § 786, stk. 4, og regler udstedt i medfør heraf registreres og opbevares som ”teletrafik” (trafikdata).

Der henvises til pkt. 3.1.3.4 og 3.2.3.3 i lovforslagets almindelige bemærkninger for en nærmere omtale af, hvad der forstås ved trafikdata.

Det foreslås desuden, at det i bestemmelsens *stk. 2* fastsættes, at regler om registreringspligt fastsat i medfør af det foreslåede *stk. 1* kan fastsættes for en periode på højst 1 år ad gangen.

Udbydere af elektroniske kommunikationsnet eller -tjenesters registreringspligt vil efter forslaget således højst kunne fastsættes for en periode på 1 år ad gangen. Den tidsmæssige udstrækning skal begrænses til det strengt nødvendige, og udstrækningen kan derfor fastsættes til mindre end 1 år, såfremt det skønnes nødvendigt. Det forudsættes, at fastsatte regler ophæves, hvis der opstår grundlag for at antage, at de ikke længere kan opretholdes. Det forudsættes også, at udbyderne af elektroniske kommunikationsnet eller -tjenester med kort varsel kan understøtte en overgang fra generel og udifferentieret registrering og opbevaring til målrettet personbestemt og geografisk registrering og opbevaring.

Det foreslås i forlængelse heraf, at oplysninger, der er registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, vil skulle opbevares i 1 år fra registreringstidspunktet, også efter overgangen til målrettet registrering og opbevaring. Det skal ses i lyset af, at oplysninger, der er registreret og opbevaret som følge af en gældende pligt til generel og udifferentieret registrering og opbevaring, vil være registreret på lovligt grundlag, og at sådanne oplysninger derfor vil kunne opbevares i 1 år efter selve registreringen med henblik på efterforskning og retsforfølgning af grov kriminalitet. Det bemærkes, at det vil være et krav for, at politiet

og anklagemyndigheden kan få adgang til sådanne oplysninger, at det sker med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed. Oplysninger registreret og opbevaret som følge af en pligt til generel og udifferentieret registrering og opbevaring, der er indhentet af politiet og anklagemyndigheden inden opbevaringsperioden for de pågældende oplysninger er udløbet, vil også efter udløbet af opbevaringsperioden kunne anvendes i efterforskningen og som bevis i straffesager.

Gyldigheden af regler udstedt i medfør af bemyndigelsen kan prøves, jf. grundlovens § 63. Det forudsættes, at grundlaget for vurderingen af, at der foreligger en alvorlig trussel mod Danmarks nationale sikkerhed, der nødvendiggør fastsættelse af regler om generel og udifferentieret registrering og opbevaring af trafikdata, offentliggøres ved udstedelsen af reglerne.

Vedrørende domstolsprøvelsen henvises i øvrigt til pkt. 3.6 i lovforslagets almindelige bemærkninger.

Til § 786 f

Retsplejelovens § 786, stk. 4, som logningsbekendtgørelsens § 5, stk. 1, er udstedt i medfør af, foreslås ophævet, jf. lovforslagets § 1, nr. 3. Det vil derfor være nødvendigt at indføre en hjemmel i retsplejeloven for fortsat at kunne registrere og opbevare oplysninger om en slutbrugers adgang til internettet.

På den baggrund foreslås det, at der indsættes en ny § 786 f i retsplejeloven, hvor det i *stk. 1* fastsættes, at det påhviler udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.2.3.1 i lovforslagets almindelige bemærkninger.

Det foreslås, at det i bestemmelsens *stk. 2* fastsættes, at oplysninger registreret i medfør af stk. 1 skal opbevares i 1 år.

Tilsvarende de gældende regler foreslås det således, at oplysninger, der registreres i medfør af den foreslåede § 786 f, stk. 1, skal opbevares i 1 år. Oplysninger, der opbevares med henblik på debitering, vil uanset om de på-

gældende data omfattes af den lovbestemte registrerings- og opbevaringspligt som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktiv 2002/58 og § 10, stk. 2, i bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester.

Der gives i *stk. 3* hjemmel til, at justitsministeren kan fastsætte nærmere regler om pligten til registrering og opbevaring af oplysninger om slutbrugers adgang til internettet.

Den foreslåede regulering er en delvis videreførelse § 5, stk. 1, i logningsbekendtgørelsen, da der med den foreslåede bestemmelse også tilsigtes en præcisering af de oplysninger, der skal registreres og opbevares.

For så vidt angår oplysninger om en slutbrugers adgang til internettet vil det omfatte oplysninger, som politiet skal bruge for at entydigt identificere, hvilke slutbrugere der benytter internettet på givne tidspunkter. Det kan eksempelvis være IP-adresse, portnummer, evt. andre identificerende oplysninger, som udbydere af elektroniske kommunikationsnet eller -tjenester tildeler slutbrugeren ved adgang til internettet samt tidspunktet, hvor en slutbruger bliver tildelt en given IP-adresse, portnummer eller andre identificerende oplysninger. Det bør derfor også tilstræbes, at reglerne sikrer, at korrekt dansk realtid registreres.

Bestemmelsen sigter på at være teknologineutral, hvilket bør overvejes i forbindelse med den nærmere regelfastsættelse. Særligt for IP-adresser bemærkes, at bestemmelsen derfor ikke sonder mellem forskellige typer IP-adresser, hverken om de er statiske, dynamiske, IPv4 eller IPv6. Bestemmelsen omfatter alle de nuværende og fremadrettede typer af slutbrugeridentifikationer. Det forudsættes i denne sammenhæng også, at de nærmere regler fastsættes efter dialog med udbydere af elektroniske kommunikationsnet eller -tjenester. Dette er ikke mindst afgørende for at sikre en hensigtsmæssig teknologisk udformning af reglerne.

Der vil ikke kunne fastsættes regler om, at udbydere af elektroniske kommunikationsnet eller -tjenester løbende skal foretage registrering af, hvilke hjemmesider, chatrooms m.v. kunderne besøger. Hensigten med forslaget

er alene at kunne føre elektroniske spor, der findes på internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

Der henvises i øvrigt til pkt. 3.3.3 i de almindelige bemærkninger til lovforslaget.

Til § 786 g

Efter gældende ret findes der regler omkring opbevaring af trafikdata. Dette er eksempelvis tilfældet med retsplejelovens § 786, stk. 4, og de regler, der er udstedt i medfør heraf. Det fremgår af 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 ”de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold”. Det fremgår endvidere, at der vil kunne opstilles regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger. Endvidere fremgår det, at det bør tilstræbes, at reglerne sikrer, at korrekt dansk realtid registreres.

Desuden findes der i telelovens § 8, stk. 1 og stk. 3, nr. 2, regler om, at Erhvervs- og vækstministeren (i dag erhvervsministeren) kan fastsætte regler for udbydere af offentlige elektroniske kommunikationsnet eller -tjenester om minimumskrav til behandling af persondata i elektroniske kommunikationsnet og -tjenester, herunder om opbevaring og behandling af trafikdata og lokaliseringsdata i forbindelse med elektronisk kommunikation.

Der findes imidlertid efter gældende ret ikke regler om, hvor trafikdata skal opbevares, herunder om de skal opbevares på servere inden for EU.

Den foreslåede § 786 g er ny og indebærer, at der kan fastsættes regler for opbevaringen af oplysninger registreret og opbevaret i medfør af de foreslåede §§ 786 a-786 f i retsplejeloven eller pålæg eller regler udstedt i medfør heraf.

Bestemmelsen foreslås indført som en bemyndigelsesbestemmelse, hvorved justitsministeren efter forhandling med erhvervsministeren kan fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af de foreslåede

§§ 786 a- 786 f i retsplejeloven eller pålæg eller regler udstedt i medfør heraf. Det forudsættes, at der fastsættes nærmere regler om, at sådanne data, jf. reglerne i de foreslåede §§ 786 a-786 f, skal opbevares på servere i EU, og at der skal ske en irreversibel destruktion af de pågældende data ved lagringsperiodens udløb. Der vil desuden kunne fastsættes regler om opbevaringsformat (læsbarhed), foranstaltninger til beskyttelse mod uautoriseret adgang til og manipulation af loggen samt opbevaring af kontooplysninger.

Det bemærkes, at nummeroplysningsdata som defineret i § 31, stk. 2, i teleloven, og som udbydere af elektroniske kommunikationsnet eller -tjenester bl.a. skal indsamle og registrere til brug for nummeroplysningsdatabasen, jf. bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser, ikke vil være omfattet af bestemmelsen.

For nærmere om afgrænsningen af de omfattede udbydere henvises til afsnit 3.2.3.1 i lovforslagets almindelige bemærkninger.

Der henvises i øvrigt til pkt. 3.9 i lovforslagets almindelige bemærkninger.

Til § 786 h

I den nuværende bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser findes der ikke krav om verificering af nummeroplysningsdata.

Med indførelsen af muligheden for målrettet personbestemt registrering og opbevaring af trafikdata vil det efter Justitsministeriets opfattelse være afgørende, at der i videst muligt omfang kan ske en entydig identifikation af brugeren af et givet kommunikationsmiddel. Dels for at det bedst muligt undgås, at der ikke sker uforvarende registrering og opbevaring af forkerte personers trafikdata, dels for at det bedste muligt sikres, at der af hensyn til bekæmpelse af grov kriminalitet også kan findes frem til de personer, der efter loven kan iværksættes registrering og opbevaring på.

Den foreslåede § 786 h i retsplejeloven er ny og indebærer, justitsministeren efter forhandling med klima-, energi- og forsyningsministeren, kan udstede regler om, at udbydere af elektroniske kommunikationsnet eller -tjenester skal verificere nummeroplysningsdata.

Det foreslås, der fastsættes en bemyndigelse for justitsministeren til, efter forhandling med klima-, energi- og forsyningsministeren, at kunne udstede regler om registrering og verificering, hvorved udbydere af elektroniske kommunikationsnet eller -tjenester vil kunne blive pålagt at verificere nummeroplysningsdata, som registreres og opbevares til brug for nummeroplysningsdatabasen, særligt med det formål, at 118-databasen, som politiet har adgang til, opnår en datakvalitet, der kan understøtte målrettet registrering og opbevaring af trafikdata.

For nærmere om afgrænsningen af de forpligtede udbydere henvises til afsnit 3.2.3.1 i lovforslagets almindelige bemærkninger.

Formålet med den foreslåede bemyndigelse vil være, at der i bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser fastsættes regler med nærmere krav til verificering af visse nummeroplysningsdata og dokumentation af, at udbyderen har verificeret disse, ligesom slutbrugeren ikke skal kunne opnå adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget.

Forslaget skal ses i sammenhæng med den foreslåede ændring af definitionen af nummeroplysningsdata i telelovens § 31, stk. 2, jf. lovforslagets § 2, nr. 2, hvor det foreslås, at der foretages en ændring af § 31, stk. 2, i teleloven, som indeholder definitionen af nummeroplysningsdata, således at nummeroplysningsdata, ud over de i forvejen angivne data, også omfatter unikt ID og eventuelle oplysninger om bruger.

Med den foreslåede ændring af definitionen af nummeroplysningsdata og den foreslåede indførelse af mulighed for, at justitsministeren efter forhandling med klima-, energi- og forsyningsministeren kan fastsætte et registrerings- og verificeringskrav, lægges der op til, at udbydere af elektroniske kommunikationsnet eller -tjenester, ud over en indsamling og registrering af gældende nummeroplysningsdata, skal indsamle og registrere unikt ID og eventuelle oplysninger om bruger og herunder verificere slutbrugerens unikke ID. Endvidere forudsættes, at der med hjemmel i den foreslåede bemyndigelse fastsættes krav om dokumentation af verificeringen, ligesom det forudsættes, at slutbrugeren ikke må opnå adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget. Endeligt foreslås det, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter. Det vil indebære, at

der fra lovens ikrafttræden ikke længere vil kunne købes anonyme taletidskort.

Der stilles ikke krav til, hvordan verificeringen skal foretages. Verificering vil eksempelvis kunne ske gennem en ny systemunderstøttet adgang til opslag i Det Centrale Personregister, hvorved det oplyste CPR-nummer kontrolleres i CPR-systemet for at verificere, at det af slutbrugeren oplyste er korrekt. Hvis slutbrugeren ikke har et CPR-nummer kan verificeringen af de af slutbrugeren oplyste oplysninger i stedet ske ved, at slutbrugeren fremviser billedlegitimation i form af et pas eller nationalt civilt identitetskort. Udbyderen kan herved kontrollere, at passet eller det nationale identitetskort, hvor fødselsdato og hhv. pasnummer eller personnummer vil fremgå, sammen med foto af slutbrugeren, stemmer overens med den person, som slutbrugeren til udbyderen oplyser at være. For personer med et CPR-nummer vil udbydere af elektroniske kommunikationsnet og -tjenester også kunne kombinere et opslag i CPR med forevisning af billede-ID. Det afgørende er, at der foretages en verificering af slutbrugers unikke ID. Erhvervskunder registreres med et CVR-nummer, som kan verificeres ved opslag i CVR-registeret (som er offentligt tilgængeligt). For erhvervskunder uden CVR-nummer kan verificeringen være opslag i det selskabsregister, hvor erhvervskunden er registreret i. Det bemærkes, at den foreslåede ordning med verificering ikke kan udelukke alle tilfælde, hvor en slutbruger forsætligt afgiver oplysninger til udbyderen af elektroniske kommunikationsnet eller -tjenester, der godt kan verificeres, men ikke er korrekte. F.eks. ved identitetstyveri, hvor andres personlige oplysninger bliver misbrugt ved at nogen oplyse dem i forbindelse med indsamling og registrering af nummeroplysningsdata.

Der stilles heller ikke krav til, hvordan udbydere skal foretage dokumentation af verificeringen. Kravet vil eksempelvis kunne opfyldes ved, at udbyderen opbevarer en kopi af billedlegitimationen eller i deres system registrerer, at verificering er foretaget, og hvordan det er foretaget, således at dette fremgår i udbyderens system. Energistyrelsen vil i medfør af telelovens § 32 kunne føre tilsyn med, at udbydere har dokumentation for at have foretaget verificering.

Endvidere forudsættes det, at der fastsættes regler om, at udbydere fremadrettet ikke må give slutbrugeren adgang til elektroniske kommunikationsnet eller -tjenester, før verificeringen er foretaget. Dette for at sikre, at veri-

ficeringsen foretages straks med indsamlingen og registreringen, da verificeringen af afgørende for, at de oplysninger, som videregives til forsyningspligtudbydernes landsdækkende nummeroplysningsdatabase (118-databasen), er korrekte og for at sikre, at det er muligt for politiet hurtigt at kunne iværksætte registrering og opbevaring af trafikdata for en person, som måtte være omfattet af personbestemt målrettet registrering og opbevaring, der eksempelvis opretter et nyt abonnement.

Det forudsættes desuden, at der skal registreres og verificeres de samme nummeroplysningsdata for uregistrerede taletidskort som for andre abonnenter omfattet af bekendtgørelse nr. 435 af 9. maj 2011 om nummeroplysningsdatabaser. Ordningen vil medføre, at det fra tidspunktet for lovens ikrafttræden ikke længere vil være muligt at købe nye uregistrerede taletidskort.

Det foreslås også, at der fastsættes overgangsbestemmelser, således at udbyderne kan nå at tilvejebringe den nødvendige systemunderstøttelse for verificering af kunder på tidspunktet for forpligtelsens indtrædelse.

Endeligt foreslås det, at udbyderne også skal indsamle og registrere unikt ID for alle eksisterende mobilabonnenter. Derfor forudsættes det, at der fastsættes regler vedrørende en overgangsordning, således at udbyderne inden en nærmere bestemt periode skal have foretaget den fornødne registrering af eksisterende mobilabonnementskunder. Der foreslås, at dette krav om indsamling og registrering af eksisterende kunder ikke gælder for andre kundegrupper som f.eks. taletidskort, fastnet- og IP-telefoni, hvor kravet alene vil være fremadrettet.

Der henvises endvidere til pkt. 3.4.2 i lovforslagets almindelige bemærkninger.

Til § 786 i

Den foreslåede bestemmelse er ny og vedrører strafansvar for udbydere af elektroniske kommunikationsnet eller -tjenesters manglende iagttagelse af reglerne om registrering og opbevaring af trafikdata. Der er i vidt omfang tale om videreførelse af gældende ret, hvor der også er foreskrevet straf for overtrædelse af logningsbekendtgørelsen. Der henvises til pkt. 3.1.1.2 i lovforslagets almindelige bemærkninger. Det vurderes, at der fortsat vil være

behov for strafansvar for ikke at foretage registrering og opbevaring af trafikdata i medfør af de foreslåede bestemmelser eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Den foreslåede straffebestemmelse vil også gælde for juridiske personer, jf. retsplejelovens § 1022, såfremt betingelser i straffelovens kapitel 5 er opfyldt. Simpel uagtsomhed vil være tilstrækkeligt for at kunne straffe efter bestemmelsen, jf. straffelovens § 19, 2. pkt. Retsplejelovens almindelige regel om tvangsbøder, jf. § 997, stk. 3, vil også kunne anvendes på manglende overholdelse af reglerne om registrering og opbevaring af trafikdata, sådan at der i en straffesag om overtrædelse af den foreslåede § 786 i kan nedlægges påstand om tvangsbøder, jf. § 684, stk. 1, nr. 1, med henblik på at gennemtvinge reglernes efterlevelse.

Det følger af den foreslåede *stk. 1*, i § 786 i at overtrædelse af § 786 b, stk. 1, 2 og 4-6, § 786 c, stk. 1-3, og § 786 f, stk. 1 og 2, samt af pålæg udstedt i medfør af § 786 d, stk. 1 og 3, straffes med bøde.

Henvisningen til den foreslåede § 786 b, stk. 1, 2 og 4-6, i retsplejeloven vil medføre, at en udbyder, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, der ikke foretager registrering og opbevaring af trafikdata vedrørende dømte personer, kommunikationsapparater, eller personer der har været genstand for et indgreb efter § 780, stk. 1, nr. 1 eller 3, vil kunne straffes med bøde. Strafansvaret vil også gælde, hvis der ikke foretages opbevaring i den foreskrevne periode. Eksempelvis hvis oplysningerne slettes før tid.

Henvisningen til den foreslåede § 786 c, stk. 1-3, i retsplejeloven vil medføre, at en udbyder, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller –tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, der ikke foretager registrering og opbevaring af trafikdata for de bestemte områder omhandlet af bestemmelserne, vil kunne straffes med bøde. Uagtsomhedskravet vil medføre, at strafansvar normalt vil forudsætte, at viden om, hvilke områder der er omfattet af registrerings- og opbevaringspligten, har været tilgængelig for udbyderen. Strafansvaret vil også gælde, hvis der ikke foretages opbevaring i den foreskrevne periode. Eksempelvis hvis oplysningerne slettes før tid.

Den foreslåede henvisning til den foreslåede § 786 f, stk. 1 og 2, vil medføre, at en udbyder af elektroniske kommunikationsnet eller -tjenester, der ikke foretager registrering og opbevaring af oplysninger om en brugers adgang til internettet ved den tildelte brugeridentitet, herunder IP-adresse, vil kunne straffes med bøde. Strafansvaret vil også gælde, hvis der ikke foretages opbevaring i den foreskrevne periode. Eksempelvis hvis oplysningerne slettes før tid.

Henvisningen til pålæg udstedt i medfør af § 786 d, stk. 1 og 3, vil medføre, at en udbyder, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, der ikke foretager registrering og opbevaring for et kommunikationsapparat, en person eller et bestemt område i overensstemmelse med et pålæg meddelt i medfør af de nævnte bestemmelser, kan straffes med bøde.

Den foreslåede *stk. 2* vedrører strafansvar i bemyndigelsesbestemmelser.

Det følger af bestemmelsen, at for overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af § 786 c, stk. 4, § 786 e, § 786 f, stk. 3, § 786 g og § 786 h, kan der fastsættes bestemmelser om bødestraf.

Den foreslåede henvisning til § 786 c, stk. 3, vil medføre, at der kan fastsættes bestemmelser om strafansvar i de regler, der er udstedt i medfør af denne bestemmelse.

Henvisningen til regler fastsat i medfør af § 786 e vil medføre, at der kan fastsættes bestemmelser om, at en udbyder af elektroniske kommunikationsnet eller -tjenester kan straffes med bøde, hvis udbyderen ikke foretager registrering og opbevaring af trafikdata i overensstemmelse med regler udstedt i medfør af bestemmelsen.

De foreslåede henvisninger til regler fastsat i medfør af § 786 f, stk. 3, og § 786 h vil medføre, at der kan foreskrives strafansvar i de regler der fastsættes om den nærmere registrering og opbevaring af oplysninger om en brugers adgang til internettet ved den tildelte brugeridentitet, herunder IP-adresse, samt verifikation af nummeroplysningsdata.

Med hensyn til strafansvar for reglerne i de foreslåede § 781 a, § 804 a og § 804 b i retsplejeloven henvises til bemærkningerne til disse bestemmelser.

For pålæg om hastesikring, jf. retsplejelovens § 786 a, findes der en straffestemme i § 786 a, stk. 4, der ikke foreslås ændret.

Til nr. 10

Det fremgår af retsplejelovens § 804, stk. 1, 1. pkt., at 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, kan 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 konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

Med lovforslagets § 1, nr. 12, foreslås det, at der i retsplejeloven indsættes en ny § 804 a, hvorefter der vil gælde et særligt kriminalitetskrav for så vidt angår adgang til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 e. Der henvises til de specielle bemærkninger hertil.

Som konsekvens heraf foreslås det, at der i det gældende § 804, stk. 1, 1. pkt., indsættes en henvisning til den foreslåede § 804 a.

Den foreslåede ændring vil medføre, at de almindelige editionsbetingelser i retsplejelovens § 804 for så vidt angår adgang til oplysninger, der er registrerings- og opbevaringspligtige i medfør af de foreslåede §§ 786 a-786 e fraviges. Efter forslaget vil det således være den foreslåede § 804 a, der vil regulere adgang til sådanne oplysninger.

Der henvises i øvrigt til bemærkningerne til pkt. 3.6.3 og 3.6.4 i de almindelige bemærkninger og bemærkningerne til § 1, nr. 9.

Til nr. 11

Til § 804 a

Det foreslås, at der i retsplejeloven indsættes en ny § 804 a om edition af oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede

§§ 786 a-786 e i retsplejeloven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Retsplejeloven indeholder ikke i dag en særlig bestemmelse om edition af registrerings- og opbevaringspligtige oplysninger. Pålæg om udlevering af sådanne oplysninger sker efter de almindelige regler om edition, medmindre oplysningerne er omfattet af lovens regler om indgreb i meddelelseshemmeligheden, jf. herom i pkt. 3.7.1.2 og 3.7.1.4 i de almindelige bemærkninger.

Efter den gældende § 804, stk. 1, 1. pkt., i retsplejeloven 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 konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

Efter den foreslåede § 804 a, 1. pkt., i retsplejeloven kan pålæg om edition, jf. § 804, af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 i eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, kun meddeles, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 (landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed) eller kapitel 13 (forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.), en overtrædelse af straffelovens § 124, stk. 2 (befrielse af en anholdt eller fængslet m.v.), § 125 (hjælp til at unddrage nogen fra forfølgning for en forbrydelse m.v.), § 127, stk. 1 (unddragelse af krigstjeneste m.v.), § 235 (udbredelse og besiddelse af børnepornografisk materiale), § 266 (trusler), § 281 (afpresning), en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5 (forskellige former for forsætlig bistand til en udlænding med ulovlig indrejse, ophold eller lignende), en krænkelse eller overtrædelse som omhandlet af § 781, stk. 2 eller 3, eller en overtrædelse, der kan medføre strafforhøjelse efter straffelovens § 81 a (overtrædelser begået som led i bandekonflikt m.v.).

Retsplejelovens § 781, stk. 2, omfatter overtrædelser af straffelovens § 263, stk. 1, om hacking. Lovens § 781, stk. 3, nr. 1, omhandler krænkelse som nævnt i § 2, stk. 2, nr. 1, i lov om tilhold, opholdsforbud og bortvisning. Bestemmelsen i tilholdslovens § 2, stk. 2, nr. 1, omfatter bl.a. krænkelse af

en andens fred ved at forfølge eller genere den anden ved kontakt m.v., 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. Retsplejelovens § 781, stk. 3, nr. 2, omfatter overtrædelser af straffelovens § 279 a (databedrageri) og § 293, stk. 1 (brugstyveri), begået ved anvendelse af en telekommunikationstjeneste. Endelig omfatter retsplejelovens § 781, stk. 3, nr. 3-5, forskellige overtrædelser af EU-regler, der har karakter af misbrug af intern viden eller markedsmanipulation. Der henvises til pkt. 3.7.1.2 i de almindelige bemærkninger.

Den foreslåede § 804 a, 1. pkt., vil medføre et skærpet kriminalitetskrav ved edition af registrerings- og opbevaringspligtige oplysninger.

Kravet om, at efterforskningen skal angå en lovovertrædelser, der kan straffes med fængsel i 3 år eller derover, vil medføre, at der ikke længere vil kunne foretages edition af registrerings- og opbevaringspligtige oplysninger i de fleste overtrædelser af særlovgivningen, hvor lovovertrædelser typisk ikke kan straffes med mere end fængsel i 2 år, se f.eks. § 3 i lov om euforiserende stoffer og færdselslovens § 117, stk. 2 (forskellige kvalificerede overtrædelse af færdselsloven).

Kravet om efterforskning af en lovovertrædelse, der kan straffes med fængsel i 3 år eller derover, vil også medføre, at efterforskning af en række af formueforbrydelserne i straffelovens kapitel 28 som udgangspunkt ikke vil kunne begrunde edition af registrerings- og opbevaringspligtige oplysninger. Det drejer sig f.eks. om tyveri (§ 276), underslæb (§ 278), bedrageri (§ 279), mandatsvig (§ 280) og skyldnersvig (§ 283), da disse lovovertrædelser som hovedregel kun kan straffes med fængsel i indtil 1 år og 6 måneder, jf. § 285, stk. 1. Har overtrædelser af de nævnte forbrydelser været af særlig grov beskaffenhed, f.eks. på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i foreningen, kan straffen imidlertid stige til fængsel i 6 eller 8 år afhængig af, hvilken forbrydelse, der er tale om, jf. § 286. Ved efterforskning af sådanne lovovertrædelser vil der kunne meddeles pålæg om edition efter den foreslåede § 804 a. I forhold til efterforskning af straffelovens formueforbrydelser skal det bemærkes, at der uanset kriminalitetskravet efter den foreslåede § 804 a vil kunne meddeles pålæg om edition under efterforskning af overtrædelser af straffelovens § 279 a eller § 293, stk. 1, begået ved anvendelse af en telekommunikationstjenester, jf. henvisningen til § 781, stk. 3, i den foreslåede § 804 a.

Efterforskning af de fleste af lovovertrædelserne i straffelovens kapitel 27 om freds- og ærekrænkelser vil som hovedregel heller ikke kunne begrunde edition af registrerings- og opbevaringspligtige oplysninger, da mange af disse forbrydelser ikke kan straffes med fængsel i 3 år. Det bemærkes i den forbindelse, at der alligevel med den foreslåede § 804 a i retsplejeloven vil kunne foretages edition i forbindelse med efterforskning af overtrædelser af straffelovens § 263, stk. 1, om hacking, jf. henvisningen til § 781, stk. 1, i den foreslåede § 804 a, hvor overtrædelser af § 263, stk. 1, er nævnt.

Derimod vil de fleste af straffelovens seksualforbrydelser i straffelovens kapitel 24 være omfattet, f.eks. voldtægt (§ 216). Besiddelse og udbredelse af børnepornografi (§ 235) vil som udgangspunkt ikke være omfattet af kriminalitetskravet på 3 år, men denne lovovertrædelse kan dog alligevel danne grundlag for edition af registrerings- og opbevaringspligtige oplysninger, da den er en af de lovovertrædelser, der er særskilt fremhævet i § 781, stk. 1, nr. 3, der henvises til i den foreslåede § 804 a. Tilsvarende vil de fleste af lovovertrædelserne i straffelovens kapitel 25 (forbrydelser mod liv og legeme) være omfattet, f.eks. manddrab (§ 237), simpel og grov vold (hhv. §§ 244 og 245) og forsætlig fareforvoldelse (§ 252) samt psykisk vold (§ 243).

Henvisningen til lovovertrædelser, som kan medføre strafforhøjelse efter straffelovens § 81 a vil medføre, at der vil kunne gives adgang til registrerings- og opbevaringspligtige oplysninger, hvis efterforskningen angår en af de overtrædelser, der er nævnt i § 81 a, hvis overtrædelsen vel og mærke er begået under de omstændigheder, der er nævnt i § 81 a. Eksempelvis vil efterforskning af en overtrædelse af straffelovens § 260 (ulovlig tvang), ikke i sig selv kunne begrunde anvendelse af den foreslåede § 804 a, da bestemmelsen ikke kan medføre straf af fængsel i 3 år eller derover. Hvis overtrædelsen af § 260 imidlertid er begået under omstændigheder som nævnt i § 81 a, kan den foreslåede § 781 a bringes i anvendelse.

Den foreslåede § 804 a i retsplejeloven vil i praksis omfatte historiske masteplysninger, det vil sige oplysninger om, hvilke sendemaster og masteceller en telefon eller kommunikationsapparat har været registreret på. Oplysninger efter den foreslåede bestemmelse vil også omfatte oplysninger om, hvilke kommunikationsapparater der på et givent tidspunkt har befundet sig i et bestemt område. Bestemmelsen vil dog også omfatte andre oplysninger, som udbyderne af elektroniske kommunikationsnet og -tjenester er forpligtet til at registrerer efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Den foreslåede § 804 a i retsplejeloven vil kun være relevant for edition hos udbydere af elektroniske kommunikationsnet eller -tjenester, som er omfattet af en af de foreslåede registrerings- og opbevaringspligter. Anmodning om adgang til registrerings- og opbevaringspligtige oplysninger vil efter den foreslåede bestemmelse skulle rettes til den dataansvarlige udbyder.

Den foreslåede § 804 a i retsplejeloven vil kun omfatte edition af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser. Oplysninger, som udbyderne af elektroniske kommunikationsnet og -tjenester er i besiddelse af, uden at der består en registreringspligt og opbevaringspligt efter §§ 786 a-786 e, vil således ikke kunne kræves udleveret med henvisning til den foreslåede § 804 a. Sådanne oplysninger vil kunne kræves udleveret efter den almindelige editionsregel i § 804 afhængig af, hvilke oplysninger, der er tale om. Hvis der er tale om oplysninger, der er omfattet af den foreslåede § 804 b, kan politiet også kræve oplysningerne udleveret med hjemmel i denne bestemmelse.

Det bemærkes, at den foreslåede § 804 a i retsplejeloven derfor ikke vil omfatte den foreslåede § 786 f om registrering og opbevaring af oplysninger om en slutbrusers adgang til internettet, der bl.a. omfatter IP-adresser. Sådanne oplysninger vil kunne kræves udleveret efter den almindelige editionsregel i retsplejelovens § 804.

Den foreslåede § 804 a i retsplejeloven vil alene indebære et særligt kriminalitetskrav for pålæg om edition af registrerings- og opbevaringspligtige oplysninger efter §§ 786 a-786 e i forhold til, hvad der gælder i § 804. De øvrige almindelige regler om edition vil således også finde anvendelse ved edition af registrerings- og opbevaringspligtige oplysninger efter §§ 786 a-786 e. Eksempelvis vil der ikke kunne meddeles pålæg om edition af registrerings- og opbevaringspligtige oplysninger, der er omfattet af en vidneudelukkelses- eller fritagelsesgrund, jf. § 804, stk. 3. Tilsvarende vil afgørelser om pålæg om edition af registrerings- og opbevaringspligtige oplysninger skulle træffes af retten, jf. § 806, stk. 1 og 2, medmindre øjemedet ellers ville forspildes, jf. stk. 4. Endvidere skal der være givet teleudbyderen, der har rådighed over de registrerings- og opbevaringspligtige oplysninger, adgang til at udtale sig, inden retten træffer afgørelse, hvis ikke retten bestemmer andet i medfør af § 748, stk. 5 og 6, jf. § 806, stk. 9, 1. og 2. pkt.

Bestemmelsen i § 805 hvorefter 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, vil derfor også gælde for sådanne afgørelser. Der henvises til pkt. 3.7.4 i de almindelige bemærkninger.

Retsplejelovens § 804, stk. 1, 2. pkt., og henvisningen til § 189 vil også finde anvendelse på editionspålæg, der er omfattet af den foreslåede § 804 a. Der vil derfor som efter gældende ret kunne meddeles tavshedspligt efter § 189 også for editionspålæg omfattet af § 804 a.

Ligesom i dag vil domstolene skulle foretage en afvejning af hensynet til at få udleveret oplysninger til brug for efterforskning af straffesager over for brugernes krav på hemmeligholdelse, sådan som dette er sikret i e-databeskyttelsesdirektivet og i EU's charter om grundlæggende rettigheder, jf. her ved Østre Landsrets kendelse af 7. maj 2018 i sag nr. B-2451-17 og B-2458-17, gengivet i *Ugeskrift for Retsvæsen 2019, s. 2019 ff.*, jf. pkt. 3.7.1.4 i de almindelige bemærkninger.

Der henvises i øvrigt til pkt. 3.7.3 og 3.7.4 i de almindelige bemærkninger.

Til § 804 b

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

Den gældende bestemmelse i telelovens § 13 giver politiet adgang, uden kendelse, til oplysninger om en slutbrugers adgang til kommunikationsnet- og tjenester, der ikke er indeholdt i 118-databasen, som udbyderne er i besiddelse af og hvor besiddelsen ikke alene skyldes en logningsforpligtigelse efter retsplejeloven. Bestemmelsen omfatter oplysninger om adresser eller numre, som udbyderen af elektroniske kommunikationsnet eller -tjeneste har tildelt slutbrugeren som led i en konkret tjeneste, og som således kan benyttes til at identificere den pågældende slutbruger, herunder statiske IP-adresser og e-mailadresser.

Bestemmelsen omtaler 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 fremgår af forarbejderne til telelovens § 13, at der vil kunne opstå nye typer af oplysninger, der kan betegnes som oplysninger om en slutbrugers adgang til kommunikationsnet og -tjenester, og som kan tjene til at identificere en bestemt slutbruger.

Det foreslås, at den nuværende bestemmelse i telelovens § 13 ophæves, jf. lovforslagets § 2, nr. 1, og at bestemmelsen i stedet overføres til retsplejeloven som en ny bestemmelse, hvor der skabes en klar hjemmel til, at udbydere af elektroniske kommunikationsnet eller -tjenester – i overensstemmelse med EU-Domstolens praksis – kan pålægges at udlevere basale oplysninger om en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester til politiet.

Det foreslås derfor, at der indsættes en ny § 804 b, hvorefter udbydere af elektroniske kommunikationsnet eller -tjenester på begæring af politiet som led i efterforskningen af en lovovertrædelse, der er er undergivet offentlig påtale, eller krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, vil skulle udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester, jf. *stk. 1*.

Bestemmelsen 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 også omfatte IP-adresser, som telelovens § 13 gør i dag. Bestemmelsen vil alene omfatte statiske oplysninger, hvis de opfylder betingelser i bestemmelsen, idet registrering af dynamiske IP-adresser m.v. vil ske i medfør af registreringsforpligtelsen i den foreslåede § 786 f.

Fælles for de oplysninger, der tilsigtes omfattet af bestemmelsen er, at forpligtelsen omfatter udlevering af den fulde oplysning, f.eks. det komplette IMEI-, IMSI- og telefonnummer, uden maskering af et eller flere cifre i det angivne nummer.

Den foreslåede bestemmelse vil fortsat heller ikke give politiet hjemmel til at begære udbyderne at oplyse, hvor mange gange og hvornår et IMEI- eller telefonnummer har foretaget aktiviteter på udbydernes net.

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 m.v., eller et mobilabonnement, vil disse således også kunne omfattes af bestemmelsen.

På teknologiens nuværende stadie vil oplysningerne navnlig omfatte IMEI-nummer, IMSI-nummer og telefonnummer.

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 fremover kun vil kunne anvendes til brug for politiets forebyggelse, efterforskning m.v. af straffelovsovertrædelser, men ikke til politiets øvrige opgavevaretagelse.

Denne indsnævring i anvendelsesområdet er begrundet i behovet for at bringe bestemmelsen i fuld overensstemmelse med EU-Domstolens praksis, herunder dom af 2. oktober 2018, Ministerio Fiscal, der som nævnt fastslog, 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 og retsforfølgning af ”straffelovsovertrædelser” generelt.

Efter § 804 b vil udlevering således kun kunne ske med henblik på forebyggelse, efterforskning og retsforfølgning af strafbare forhold. Denne ændring foreslås indført med et krav om, at politiets begæring skal ske som led i

efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning.

Det foreslås endelig, at adgangen til at påklage politiets begæring efter bestemmelsen inden for strafferetsplejen, også fremover skal følge den ordning, der er fastsat i retsplejelovens § 101, stk. 2, hvorefter statsadvokaterne behandler klager over afgørelser truffet af politidirektørerne vedrørende strafforfølgning.

Den foreslåede bestemmelse udelukker ikke, at oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester, kan kræves udleveret efter andre bestemmelser, herunder navnlig de gældende regler om edition i strafferetsplejen, jf. retsplejelovens § 804. Politiet er dog ikke forpligtet til at gå frem efter reglerne om edition; og det må bero på politiets skøn, hvorvidt det er mest hensigtsmæssigt at gå frem efter reglerne om edition eller reglerne i den foreslåede § 804 b. En begæring fra politiet efter den foreslåede § 804 b og et pålæg om edition fra domstolene vil begge undergive adressaten en aktiv handlepligt, hvorfor forpligtelsen vil være den samme. Sanktionen for ikke at efterkomme en begæring efter den foreslåede § 804 b eller et pålæg om edition efter § 804 vil i begge tilfælde kunne indebære strafansvar, jf. nedenfor om forslaget til stk. 3.

Det foreslås i *stk. 2*, at oplysninger som opbevares som følge af §§ 786 a-786 f ikke er omfattet af stk. 1.

Bestemmelsen viderefører og præciserer således retstilstanden efter telelovens § 13, da telelovens § 13 ikke finder anvendelse på oplysninger, som udbyderne alene ligger inde med som følge af registrerings- og opbevaringspligten i den gældende § 786, stk. 4, i retsplejeloven, idet disse skal udleveres i medfør af en retskendelse efter reglerne i retsplejeloven.

Det bemærkes, at hvis udbyderne ligger inde med sådanne oplysninger, som udbyderne desuden skal registrere og opbevare efter de foreslåede §§ 786 a-786 f, af andre grunde, skal disse oplysninger udleveres på baggrund af § 804 b, stk. 1, for så vidt angår §§ 786 a-786 e og udleveres på baggrund af § 804 for så vidt angår § 786 f.

Det foreslås i *stk. 3*, at udbydere af elektroniske kommunikationsnet eller -tjenester kan straffes med en bøde, hvis de overtræder stk. 1. Dermed vil

bestemmelsen fortsat være strafbelagt, ligesom telelovens § 13 også er det i dag i medfør af telelovens § 81, stk. 1, nr. 1.

Til nr. 12

Efter retsplejelovens § 806, stk. 9, 1. pkt., skal der inden retten træffer afgørelse om pålæg om edition være givet den, der har rådighed over genstanden adgang til at udtale sig. Lovens § 748, stk. 5 og 6, finder tilsvarende anvendelse, jf. § 806, stk. 9, 2. pkt.

Er genstanden for edition oplysninger, der er registrerings- og opbevaringspligtige, jf. de foreslåede §§ 786 a-786 e, vil det være en teleudbydere, der har rådighed over genstanden, og som skal have adgang til at udtale sig, før der træffes afgørelse. Den, som oplysninger angår (den registrerede), vil ikke have adgang til at udtale sig efter den gældende § 806, stk. 9. Er vedkommende sigtet, vil en eventuel forsvarer dog blive underrettet om retsmødet og have mulighed for at fremsætte bemærkninger, jf. § 748, stk. 2 og 3.

Det foreslås, at der indsættes et nyt *stk. 10* i retsplejelovens § 806.

Det fremgår af det foreslåede stk. 10 i retsplejelovens § 806, at retsplejelovens § 784, § 785 og § 788 finder tilsvarende anvendelse ved pålæg om edition, jf. den foreslåede § 804 a, i forhold til den, som oplysningerne angår.

Den foreslåede bestemmelse vil medføre, at der vedrørende pålæg om edition af registrerings- og opbevaringspligtige oplysninger indføres regler om advokatbeskikkelse og underretning af den, som oplysningerne angår, der svarer til, hvad der i dag gælder i forhold til lovens regler om indgreb i meddelelseshemmeligheden. Baggrunden for bestemmelsen er, at den, hvis oplysninger indgrebet angår, bør have samme muligheder for at varetage sine interesser, hvad enten politiets adgang til loggede oplysninger sker efter reglerne om indgreb i meddelelseshemmeligheden eller reglerne om edition.

Den foreslåede henvisning til lovens §§ 784 og 785 vil have den virkning, at der i forbindelse med pålæg om edition af registrerings- og opbevaringspligtige oplysninger, jf. den foreslåede § 804 a, vil skulle ske beskikkelse af en advokat, der varetager interesserne for den eller de personer, hvis oplysninger er genstand for målrettet registrering og opbevaring. Der henvises til pkt. 3.6.3.2 og 3.7.1.2 i de almindelige bemærkninger.

Til nr. 13

Det fremgår af retsplejelovens § 807 a, 1. pkt., at private har samme beføjelser til at foretage beslaglæggelse som politiet, jf. § 806, stk. 4. Det beslaglagte skal snarest overgives til politiet, jf. 2. pkt. Efter 3. pkt. skal politiet forelægge sagen for retten i overensstemmelse med § 806, st. 4, 2. pkt., medmindre det beslaglagte inden udløbet af 24 timer udleveres til den, mod hvem indgrebet er foretaget, eller denne meddeler skriftligt samtykke til beslaglæggelse i overensstemmelse med § 806, stk. 10.

Det foreslås at ændre henvisningen i retsplejelovens § 807 a, 3. *pkt.*, til § 806, stk. 11. Ændringen er alene en konsekvens af, at § 806, stk. 10, med forslaget til § 1, nr. 12, bliver stk. 11, og vil ikke medføre substantielle ændringer i reglerne om beslaglæggelse.

Til § 2

Til nr. 1

Det fremgår af telelovens § 13, at udbydere af elektroniske kommunikationsnet eller -tjenester på begæring af politiet skal udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester. For en nærmere beskrivelse af gældende ret henvises til pkt. 3.7.1.5 i lovforslagets almindelige bemærkninger.

Det følger af den foreslåede § 804 b i retsplejeloven, jf. lovforslagets § 1, nr. 11, at telelovens § 13 overflyttes til retsplejeloven.

Det foreslås derfor, at telelovens § 13 ophæves.

Til nr. 2

Det fremgår af telelovens § 31, stk. 2, at ved nummeroplysningsdata forstås oplysninger om abonnentnumre, der er tildelt slutbrugere, indeholdende navn, adresse, eventuelle oplysninger om stilling, abonnentnummeret og den kategori af tjeneste, abonnentnummeret anvendes til.

Det foreslås, at bestemmelsen ændres således, at nummeroplysningsdata også omfatter unikt ID og eventuelle oplysninger om bruger.

Ændringen af definitionen af nummeroplysningsdata skal ses i sammenhæng med den foreslåede bestemmelse i retsplejelovens § 786 h, hvorefter justitsministeren efter forhandling med og klima-, energi- og forsyningsministeren fastsætter regler om, at udbydere af elektroniske kommunikationsnet eller -tjenesters registrering og verificering af nummeroplysningsdata. Der henvises også herom til de almindelige bemærkninger i pkt. 3.4.

Formålet med ændringen er at sikre, at de oplysninger som fremgår af 118-databasen, er korrekte, hvilket vurderes sikret bedst muligt ved registrering af unikt ID på slutbrugeren, idet datakvaliteten i 118 dermed vil blive øget, således at der kan ske en entydig identifikation af slutbrugeren, hvilket kan have betydning for politiet, bl.a. ved iværksættelse af målrettet registrering og opbevaring på personer.

Ved et unikt ID forstås CPR-nummer for personer, der er tildelt et sådant, hvis abonnenten udgør en fysisk person. For personer uden CPR-nummer angives i stedet oplysning om fødselsdato, statsborgerskab ved fødslen og køn. Herudover angives for personer uden CPR-nummer et pasnummer eller nummer fra nationalt civilt identitetskort og udstedelsesland for passet eller det nationale identitetskort. Hvis abonnenten udgør en juridisk person angives CVR-nummer. For juridiske personer uden CVR-nummer angives i stedet selskabsregisteret, hvori den juridiske person er registreret, og registreringsnummeret. Oplysning om eventuel bruger vil være oplysning om brugeren, hvis denne person ikke er den samme som abonnenten, og dette er kendt af abonnenten (slutbrugeren).

Ved eventuelle oplysninger om bruger forstås oplysninger om den fysiske person, der forventes at anvende teletjenesten. Der kan derfor være et overlap mellem slutbrugeren og brugeren, men i flere tilfælde vil slutbrugeren og brugeren ikke være den samme person. Det vil være en forudsætning, at brugeren kendes ved registrering.

Der henvises i øvrigt til pkt. 3.8 i lovforslagets almindelige bemærkninger.

Til § 3

Det foreslås i *stk. 1*, at loven træder i kraft 1. januar 2022.

Loven gælder ikke for Færøerne og Grønland, fordi hovedloven ikke gælder for Færøerne og Grønland, og vil således ikke kunne blive sat i kraft for Færøerne og Grønland.

Det foreslås i *stk. 2*, at justitsministeren efter forhandling med erhvervsministeren i en overgangsperiode kan fastsætte nærmere regler om registrering og opbevaring af trafikdata for så vidt angår retsplejelovens § 786 b, § 786 c, stk. 1, nr. 2, og § 786 d, stk. 1, 1. pkt., som affattet ved denne lovs § 1, nr. 9.

Den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata, jf. de foreslåede § 786 b og § 786 d, stk. 1, i retsplejeloven, og en del af ordningen med målrettet geografisk registrering og opbevaring af trafikdata, jf. den foreslåede § 786 c, stk. 1, nr. 2, i retsplejelovens, vil kræve ny it-systemunderstøttelse. Da en sådan it-systemunderstøttelse ikke vil kunne være færdigudviklet på tidspunktet for lovens ikrafttrædelse, foreslås det, at justitsministeren bemyndiges til i en overgangsperiode at kunne fastsætte nærmere regler om registrering og opbevaring af trafikdata for så vidt angår den foreslåede ordning med målrettet personbestemt registrering og opbevaring af trafikdata samt for så vidt angår den nævnte del af ordningen med målrettet geografisk registrering og opbevaring af trafikdata (områder med en overhyppighed af beboere dømt for grov kriminalitet).

Det forudsættes, at bemyndigelsen udnyttes til at fastsætte regler om, hvordan myndighederne og udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, i en periode, indtil den nødvendige it-systemunderstøttelse er på plads – og i overensstemmelse med betingelserne i de foreslåede § 786 b, § 786 c, stk. 1, nr. 2, og § 786 d, stk. 1, i retsplejeloven – kan administrere målrettet personbestemt og geografisk registrering og opbevaring af trafikdata. Dette med henblik på, at der i perioden indtil den nødvendige it-systemunderstøttelse er færdigudviklet, og ud fra de betingelser, der fastsættes i de nævnte foreslåede bestemmelser, kan ske målrettet personbestemt registrering og opbevaring samt målrettet geografisk registrering og opbevaring i relation til områder, hvor der er en overhyppighed af beboere dømt for grov kriminalitet.

Det foreslås i *stk. 3*, at for oplysninger om teletrafik, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, finder retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition anvendelse.

Den foreslåede bestemmelse udgør derfor en undtagelse til de foreslåede bestemmelser i retsplejelovens § 781 a og § 804 a, der ellers kun kan finde anvendelse i forhold til oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 f eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Bestemmelsen vil indebære, at oplysninger om teletrafik, der er registreret efter retsplejelovens § 786, stk. 4, på tidspunktet for lovens ikrafttræden, vil kunne udleveres til politiet efter de foreslåede bestemmelser i retsplejelovens § 781 a og § 804 a, som disse foreslås affattes med nærværende lovforslag, uanset bestemmelsernes afgrænsning til oplysninger, der er registrerings- og opbevaringspligtige efter de foreslåede §§ 786 a-786 f i retsplejelo-ven eller efter pålæg eller regler udstedt i medfør af disse bestemmelser.

Det bemærkes, at oplysninger om teletrafik, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, og udleveret efter retsplejelovens kapitel 71 og 74 om indgreb i meddelelseshemmeligheden og edition, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, også vil kunne anvendes som bevis i forbindelse med retsmøder under efterforskning, tiltalerejsning og hovedforhandling efter tidspunktet for lovens ikrafttræden. Det bemærkes i den forbindelse, at den mistænkte, sigtede eller tiltalte vil være i stand til effektivt at udtale sig om oplysningerne og disses værdi som bevis, og at der derfor vil være adgang til fuld kontradiktion for så vidt angår sådanne oplysninger.

Det foreslås i *stk. 4*, at oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, skal opbevares i 1 år fra registreringstidspunktet.

Bestemmelsen vil indebære, at udbydere af elektroniske kommunikationsnet eller -tjenester vil være forpligtet til at opbevare oplysninger om teletrafik, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, i 1 år fra registreringstidspunktet – også

efter nærværende lovs ikrafttræden. Det skal ses i lyset af, at oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, vil være registreret på lovligt grundlag.

Det bemærkes, at det vil være et krav for, at politiet og anklagemyndigheden kan få adgang til sådanne oplysninger, at det sker med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed, jf. lovforslagets § 3, stk. 3.

Det bemærkes desuden, at oplysninger, der på tidspunktet for lovens ikrafttræden er registreret og opbevaret efter retsplejelovens § 786, stk. 4, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, og som indhentes af politiet og anklagemyndigheden efter nærværende lovs ikrafttræden, men inden opbevaringsperioden for de pågældende oplysninger er udløbet, også efter udløbet af opbevaringsperioden vil kunne anvendes som bevis i forbindelse med retsmøder under efterforskning, tiltalerejsning og hovedforhandling. Det bemærkes i den forbindelse, at den mistænkte, sigtede eller tiltalte vil være i stand til effektivt at udtale sig om oplysningerne og disses værdi som bevis, og at der derfor vil være adgang til fuld kontradiktion for så vidt angår sådanne oplysninger.

Det foreslås i *stk. 5*, at regler fastsat i medfør af retsplejelovens § 786, stk. 5, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 4.

Overgangsreglen skyldes, at forslaget om at ophæve stk. 4 i retsplejelovens § 786 (jf. lovforslagets § 1, nr. 4), har den konsekvens, at det gældende § 786, stk. 5, bliver til § 786, stk. 4.

Det foreslås i *stk. 6*, at regler fastsat i medfør af retsplejelovens § 786, stk. 7, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 5.

Overgangsreglen skyldes, at forslaget om at ophæve stk. 4 og 6 i retsplejelovens § 786 (jf. lovforslagets § 1, nr. 4), har den konsekvens, at det gældende § 786, stk. 7, bliver til § 786, stk. 5.

Det foreslås i *stk. 7*, at regler fastsat i medfør af retsplejelovens § 786, stk. 8, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 786, stk. 6.

Overgangsreglen skyldes, at forslaget om at ophæve stk. 4 og 6 i retsplejelovens § 786 (jf. lovforslagets § 1, nr. 4), har den konsekvens, at det gældende § 786, stk. 8, bliver til § 786, stk. 5.

Der foreslås i *stk. 8*, at retsplejelovens § 786 b, stk. 2 og 4, som affattet ved denne lovs § 1, nr. 9, kun finder anvendelse for domme afsagt og indgreb iværksat efter lovens ikrafttræden.

Det foreslåede § 786 b, stk. 2, vil således ikke finde anvendelse for så vidt angår personer, der er dømt for grov kriminalitet forud for lovens ikrafttræden, hvilket vil have den konsekvens, at der ikke kan iværksættes registrering og opbevaring af trafikdata efter det foreslåede § 786 b, stk. 2, for sådanne personer på baggrund af domme afsagt inden lovens ikrafttræden.

Tilsvarende vil det foreslåede § 786 b, stk. 4, ikke finde anvendelse for så vidt angår indgreb omfattet af det foreslåede § 786 b, stk. 4, der er iværksat forud for lovens ikrafttræden, hvilket vil have den konsekvens, at der ikke kan iværksættes registrering og opbevaring af trafikdata efter det foreslåede § 786 b, stk. 4, for kommunikationsapparater eller personer, der er iværksat et af de omfattede indgreb i meddelelseshemmeligheden på inden lovens ikrafttræden.

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering

Lovforslaget

§ 1

I retsplejeloven, jf. lovbekendtgørelse nr. 1445 af 29. september 2020, som senest ændret ved § 3 i lov nr. 1174 af 8. juni 2021, foretages følgende ændringer:

§ 781. Indgreb i meddelelseshemmeligheden må kun foretages, såfremt

1-2). ---

3) 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, 125, 127, stk. 1, 233, stk. 1, 235, 266, 281 eller en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5

Stk. 2-5. ---

1. I § 781, stk. 1, nr. 3, indsættes efter »udlændingelovens § 59, stk. 8, nr. 1-5«: », jf. dog § 781 a«.

2. Efter § 781 indsættes:

»§ 781 a. Politiet kan, uanset § 781, stk. 1, nr. 3, tillige foretage teleoplysning, jf. § 780, stk. 1, nr. 3, og udvidet teleoplysning, jf. § 780, stk. 1, nr. 4, der består i pålæg om udlevering af oplysninger, der er registrerings- og opbevaringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.«

§ 786. ---

Stk. 2-3. ---

Stk. 4. Det påhviler udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om denne registrering og opbevaring.

Stk. 5. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Stk. 6. Overtrædelse af stk. 4, 1. pkt., straffes med bøde.

Stk. 7. For overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af stk. 4, 2. pkt., og stk. 5 kan der fastsættes bestemmelser om bødestraf.

Stk. 8. Justitsministeren kan fastsætte regler om økonomisk godtgørelse til de i stk. 1 nævnte virksomheder for udgifter i forbindelse med bistand til politiet til gennemførelse af indgreb i meddelelseshemmeligheden

3. § 786, *stk. 4 og 6*, ophæves.

Stk. 5 bliver herefter stk. 4 og stk. 7 og 8 bliver herefter stk. 5 og 6.

4. I § 786, *stk. 7*, der bliver stk. 5, slettes »stk. 4, 2. pkt., og«.

§ 786 a. Som led i en efterforskning, hvor elektronisk bevismateriale kan være af betydning, kan politiet meddele udbydere af telenet eller teletjenester pålæg om at foretage hastesikring af elektroniske data, herunder trafikdata.

Stk. 2. Et pålæg om hastesikring i medfør af stk. 1 kan alene omfatte elektroniske data, som opbevares på det tidspunkt, hvor pålægget meddeles. I pålægget 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.

Stk. 3. Det påhviler udbydere af telenet eller teletjenester som led i sikring efter 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,

5. I § 786 a, *stk. 1*, ændres »trafikdata« til: »trafik- og lokaliseringsdata«

6. § 786 a, *stk. 2, 4. pkt.*, affattes således: »Et pålæg kan dog efterfølgende opretholdes, men højst med 90 dage ad gangen.«

7. I § 786 a indsættes efter stk. 2 som nyt stykke:

»*Stk. 3.* Hastesikring af trafik- og lokaliseringsdata må kun foretages, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.«

Stk. 3 og 4 bliver herefter stk. 4 og 5.

Gældende formulering

Lovforslaget

som kan være af betydning for efterforskningen.

Stk. 4. Overtrædelse af stk. 1 og 3 straffes med bøde.

8. I § 786 a, *stk. 4*, der bliver *stk. 5*, ændres »stk. 1 og 3« til »stk. 1 og 4«.

9. Efter § 786 a indsættes:

»§ 786 b. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata efter stk. 2-5.

Stk. 2. Trafikdata omfattet af forpligtelsen i stk. 1 registreres i

- 1) 3 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 3 år, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a,
- 2) 5 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 6 år,
- 3) 10 år, hvis personen er dømt for en lovovertrædelse, som efter loven kan straffes med fængsel i mindst 8 år.

Stk. 3. Er den pågældende person idømt en ubetinget frihedsstraf, regnes registreringsperioden, jf. stk. 2, nr. 1-3, fra tidspunktet for endelig løsladelse fra afsoning. Prøveløslades den pågældende person, regnes perioden fra tidspunktet for prøveløsladelse. Er den pågældende person idømt en betinget frihedsstraf, regnes perioden fra endelig dom. Er den pågældende person idømt anden strafferetlig retsfølge efter straffelovens §§ 68-70, regnes perioden fra endelig ophævelse af denne retsfølge, dog regnes perioden fra endelig dom,

hvis den pågældende person er dømt til ambulantly behandling, der ikke medfører eller kan medføre indlæggelse i institution.

Stk. 4. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage personbestemt målrettet registrering og opbevaring af trafikdata fra

- 1) kommunikationsapparater, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1 eller 3,
- 2) personer, der, jf. § 783, stk. 2, har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1 eller 3,
- 3) personer, der er indehavere af et kommunikationsapparat, der, jf. § 783, stk. 1, 2. pkt., har været genstand for indgreb i medfør af § 780, stk. 1, nr. 1, eller 3, og
- 4) kommunikationsapparater, der har været genstand for indgreb i medfør af § 786, stk. 2.

Stk. 5. Trafikdata registreret i medfør af stk. 4 skal registreres i 1 år fra det tidspunkt, hvor indgrebet afsluttes.

Stk. 6. Trafikdata registreret efter stk. 2-5 skal opbevares i 1 år.

§ 786 c. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på områder på 3 km gange 3 km, hvor

- 1) antallet af anmeldelser af lovovertrædelser begået i området, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13,

overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år, eller

- 2) antallet af beboere dømt for lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller som er dømt efter straffelovens § 81 a, udgør mindst 1,5 gange landsgennemsnittet opgjort som gennemsnit over de seneste 3 år.

Stk. 2. Det påhviler udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, at foretage geografisk målrettet registrering og opbevaring af trafikdata på særligt sikringskritiske områder, såsom kongehusets residenser, Christiansborg Slot, statsministerboligen Marienborg, ambassader, politiets ejendomme, kriminalforsorgens institutioner, bro-, tunnel- og færgeforbindelser, trafikknudepunkter og større indfaldsveje, grænseovergange, busterminaler, fjernbanestationer, stationer på bybaner, militære områder, kolonne 3-virksomheder og offentligt godkendte flyvepladser.

Stk. 3. Trafikdata registreret efter stk. 1 og 2 skal opbevares i 1 år.

Stk. 4. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere

regler om målrettet geografisk registrering og opbevaring af trafikdata som nævnt i stk. 1.

§ 786 d. Der kan meddeles udbydere, som med et kommercielt formål udbyder elektroniske kommunikationsnet eller -tjenester som sin hovedydelse eller som en ikkeaccessorisk del af virksomheden, pålæg om at foretage målrettet registrering og opbevaring af trafikdata for kommunikationsapparater, personer eller bestemte områder, hvis der er grund til at antage, at de har forbindelse til lovovertrædelser, som efter loven kan straffes med fængsel i 3 år eller derover, forsætlige overtrædelser af straffelovens kapitel 12 eller 13, overtrædelser af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, overtrædelser af udlændingelovens § 59, stk. 8, nr. 1-5, krænkelser eller overtrædelser som omfattet af § 781, stk. 2 eller 3, eller lovovertrædelser, som kan medføre strafforhøjelse efter straffelovens § 81 a.

Stk. 2. Afgørelse om pålæg om registrering og opbevaring efter stk. 1 træffes af retten ved kendelse. I kendelsen fastsættes det tidsrum, inden for hvilket indgrebet kan foretages. Dette tidsrum skal være så kort som muligt og må ikke overstige 6 måneder. Tidsrummet kan forlænges, men højst med 6 måneder ad gangen. Forlængelsen sker ved kendelse. I kendelsen angives den person, det kommunikationsapparat eller det område, som indgrebet angår. Reglerne i § 783, stk. 2, 2., 3. og 5.-7. pkt., finder tilsvarende anvendelse ved pålæg om registrering og opbevaring af trafikdata for personer. Underretningen efter 7. pkt., jf. § 783, stk. 2, 2. og 3. pkt., skal ideholde en angivelse af de grunde, der er til at antage, at den person, som indgrebet angår, benytter sig af de pågældende numre.

Stk. 3. Trafikdata registreret i medfør af pålæg meddelt efter stk. 1 skal opbevares i 1 år.

Stk. 4. Reglerne i § 782, stk. 1, § 783, stk. 1, 3 og 4. pkt., samt stk. 4, og §§ 784 og 785 finder tilsvarende anvendelse for pålæg omfattet af stk. 1.

§ 786 e. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler, der pålægger udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.

Stk. 2. Regler om registreringspligt fastsat i medfør af stk. 1 kan fastsættes for en periode på højst 1 år ad gangen.

§ 786 f. Det påhviler udbydere af elektroniske kommunikationsnet eller -tjenester at foretage generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet.

Stk. 2. Oplysninger registreret efter stk. 1 skal opbevares i 1 år.

Stk. 3. Justitsministeren fastsætter efter forhandling med erhvervsministeren nærmere regler om registrering og opbevaring som nævnt i stk. 1.

§ 786 g. Justitsministeren kan efter forhandling med erhvervsministeren fastsætte regler om udbydere af elektroniske kommunikationsnet eller -tjenesters opbevaring af oplysninger registreret og opbevaret i medfør af §§ 786 a-786 f eller pålæg eller regler udstedt i medfør heraf.

§ 786 h. Justitsministeren kan efter forhandling med og klima-, energi- og forsyningsmi-

nisteren fastsætte regler om udbydere af elektroniske kommunikationsnet eller –tjenesters registrering og verificering af nummeroplysningsdata.

§ 786 i. Overtrædelse af § 786 b, stk. 1, 2 og 4-6, § 786 c, stk. 1-3, og § 786 f, stk. 1 og 2, samt af pålæg udstedt i medfør af § 786 d, stk. 1 og 3, straffes med bøde.

Stk. 2. For overtrædelse af bestemmelser i forskrifter, der er fastsat i medfør af § 786 c, stk. 4, § 786 e, § 786 f, stk. 3, § 786 g og § 786 h, kan der fastsættes bestemmelser om bødestraf.«

§ 804. 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 kan der 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 konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. Når pålæg meddeles en erhvervsvirksomhed, finder § 189 tilsvarende anvendelse for andre, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen.

Stk. 2-5. ---

10. I § 804, stk. 1, 1. pkt., indsættes efter »som kan kræve den tilbage«: », jf. dog § 804 a«.

11. Efter § 804 indsættes:

»§ 804 a. Pålæg om edition, jf. § 804, af oplysninger, der er registreringspligtige efter §§ 786 a-786 e eller efter pålæg eller regler udstedt i medfør af disse bestemmelser, kan kun meddeles, hvis efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 3 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, en overtrædelse af straffelovens § 124, stk. 2, § 125, § 127, stk. 1, § 235, § 266 eller § 281, en overtrædelse af udlændingelovens § 59, stk. 8, nr. 1-5, en krænkelse eller overtrædelse som omfattet af § 781, stk. 2 eller 3, eller en lovovertrædelse, som kan medføre strafforhøjelse efter straffelovens § 81 a.

§ 804 b. Uanset §§ 804 og 804 a skal udbydere af elektroniske kommunikationsnet eller -tjenester på politiets begæring som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, eller en krænkelse som nævnt i § 2, stk. 1, nr. 1, i lov om tilhold, opholdsforbud og bortvisning, udle-

vere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

Stk. 2. Oplysninger, som opbevares som følge af §§ 786 a-786 f, er ikke omfattet af stk. 1.

Stk. 3. Overtrædelse af stk. 1 straffes med bøde.

§ 806. ---

Stk. 2-9. ---

Stk. 10. Afgørelse om beslaglæggelse træffes af politiet, såfremt den, som indgrebet retter sig imod, meddeler skriftligt samtykke til indgrebet

§ 807 a. Samme beføjelser til beslaglæggelse som politiet, jf. § 806, stk. 4, har enhver, der træffer nogen under eller i umiddelbar tilknytning til udøvelsen af et strafbart forhold. Det beslaglagte skal snarest muligt overgives til politiet med oplysning om tidspunktet og grundlaget for beslaglæggelsen. Politiet forelægger sagen for retten i overensstemmelse med § 806, stk. 4, 2. pkt., medmindre det beslaglagte inden udløbet af 24 timer udleveres til den, mod hvem indgrebet er foretaget, eller denne meddeler skriftligt samtykke til beslaglæggelse i overensstemmelse med § 806, stk. 10

12. I § 806 indsættes efter stk. 9 som nyt stykke:

»*Stk. 10.* Ved pålæg om edition, jf. § 804 a, finder §§ 784-785 og § 788 tilsvarende anvendelse i forhold til den, som oplysningerne angår.«

Stk. 10 bliver herefter stk. 11.«

13. I § 807 a, 3. pkt., ændres »§ 806, stk. 10« til: »§ 806, stk. 11«

§ 2

I lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014, som senest ændret ved § 4 i lov nr. 1176 af 8. juni 2021, foretages følgende ændringer:

§ 13. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal på begæring af politiet udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester.

1. § 13 ophæves.

§ 31. ---

Stk. 2. Ved nummeroplysningsdata forstås oplysninger om abonnentnumre, der er tildelt slutbrugere, indeholdende navn, adresse, eventuelle oplysninger om stilling, abonnentnummeret og den kategori af tjeneste, abonnentnummeret anvendes til.

Stk. 3-5. ---

2. I § 31, *stk. 2*, indsættes efter »indeholdende«: »unik ID«, og efter »eventuelle oplysninger om stilling«: »eventuelle oplysninger om bruger«.