JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Dato:
Kontor: Sikkerhed og forebyggelseskontoret
Sagsbeh: Trine Priess Sørensen
Sagsnr.: 2012-187-0020
Dok.: 549331

Redegørelse

om

diverse spørgsmål vedrørende

logningsreglerne

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

1. Indledning

Ved Folketingets Retsudvalgs betænkning af 31. maj 2012 over lovforslag nr. L 53 om ændring af lov 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 (Ændring af revisionsbestemmelse) har Retsudvalget anmodet Justitsministeriet om

- snarest muligt og senest ultimo 2012 at undersøge, hvorvidt logningsdirektivet[1] er overimplementeret i Danmark, jf. nedenfor pkt. 3,
- at undersøge, hvilke andre regler end logningsreglerne der indebærer, at borgernes tele- og internetkommunikation registreres og opbevares, og hvilken betydning disse regler har, samt afklare, i hvilket omfang data opbevaret efter logningsreglerne kan kræves udleveret efter andre hjemler end retsplejeloven, jf. nedenfor pkt. 4,
- at sikre, at der fra politiets side i forbindelse med revisionen af reglerne fremlægges en kvalitativ og kvantitativ opgørelse over den hidtidige brug af logningsdata, som bør foreligge ultimo 2012, jf. nedenfor pkt. 5, og
- at sikre, at der for efterretningstjenesternes vedkommende fremlægges en kvalitativ opgørelse over, hvor effektive de forskellige elementer af logning indtil nu har været i kampen mod terror og kriminalitet, så vidt dette er muligt uden at kompromittere efterretningstjenesternes arbejde, jf. nedenfor pkt. 6.

Nærværende redegørelse følger – efter en oversigt over det retlige grundlag i pkt. 2 – op på Retsudvalgets anmodning.

2. Det retlige grundlag

2.1. Retsplejelovens § 786, stk. 4

Ved lov nr. 378 af 6. juni 2002 om ændring straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven,

[1] Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF.

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), blev der indsat en ny bestemmelse i retsplejelovens § 786, stk. 4, om registrering og opbevaring af oplysninger om teletrafik samt om telenet- og teletjenesteudbyderes praktiske bistand til politiet.

Efter retsplejelovens § 786, stk. 4, påhviler det således 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. Efter bestemmelsen fastsætter justitsministeren efter forhandling med (nu) erhvervs- og vækstministeren nærmere regler om denne registrering og opbevaring.

Det er i forarbejderne til bestemmelsen forudsat, at udbydere alene skal registrere og opbevare oplysninger om, hvem der har haft kontakt, men ikke oplysninger om, hvad indholdet af kommunikationen imellem de pågældende var, f.eks. i form af optagelse af en telefonsamtale.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgning af kriminalitet udgør et indgreb i meddelelseshemmeligheden, og adgangen til at få udleveret oplysninger, som en udbyder har registreret og opbevaret efter bestemmelsen, reguleres derfor af reglerne om indgreb i meddelelseshemmeligheden i retsplejelovens kapitel 71 samt eventuelt også reglerne i kapitel 74 om edition.

2.2. Logningsdirektivet

Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (logningsdirektivet) blev vedtaget den 21. februar 2006.

Det fremgår af præamblen til logningsdirektivet, at baggrunden for direktivet bl.a. er, at medlemsstaterne har praktiske erfaringer for, at trafikdata og lokaliseringsdata har stor betydning i efterforskning, afsløring og retsforfølgning af strafbare handlinger, og at det derfor er nødvendigt på euro-

pæisk plan at sikre, at data, som genereres eller behandles af udbydere af elektronisk kommunikation, lagres i en vis periode.

2.3. 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 retsplejelovens § 786, stk. 4. Bekendtgørelsen er i vid udstrækning udtryk for en gennemførelse af logningsdirektivets bestemmelser om pligt til at registrere og opbevare oplysninger om teletrafik.

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

Efter bekendtgørelsens § 4 skal teleudbydere registrere en række nærmere angivne oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, herunder oplysninger om det opkaldte og det opkaldende nummer og tidspunktet for kommunikationens start og afslutning.

Efter bekendtgørelsens § 5 skal teleudbydere registrere en række nærmere angivne oplysninger om internettrafik. Det gælder bl.a. oplysninger om en brugers adgang til internettet, IP-adresser i forbindelse med brug af internettet samt tidspunktet for kommunikationens start og afslutning.

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

Udbyderne skal derimod ikke registrere og opbevare indholdet af kommunikation, hverken i forbindelse med telefonsamtaler, brug af internettet eller brug af udbyderens e-mail-tjenester.

Efter bekendtgørelsens § 9 skal de registrerede oplysninger opbevares i 1 år.

Logningsbekendtgørelsen regulerer ikke spørgsmålet om, hvem der har adgang til at få udleveret de registrerede oplysninger eller betingelserne herfor. Som anført under pkt. 2.1 er dette nærmere reguleret i retsplejelovens regler om indgreb i meddelelseshemmeligheden og edition.

3. Logningsdirektivets implementering

Retsudvalget har ved sin betænkning af 31. maj 2012 anmodet Justitsministeriet om at undersøge, hvorvidt logningsdirektivet er overimplementeret i Danmark.

Indledningsvis kan det oplyses, at det følger af artikel 288 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF), at et direktiv med hensyn til det tilsigtede mål er bindende for enhver medlemsstat, som det rettes til, men overlader det til de nationale myndigheder at bestemme form og midler for gennemførelsen.

Direktiver kan efter deres indhold overlade varierende grader af råderum for medlemsstaterne til at fastsætte krav, der går videre end direktivets ordlyd.

Logningsdirektivet er et minimumsdirektiv, hvilket indebærer, at direktivet alene fastsætter, hvilken regulering de enkelte medlemsstater som minimum er forpligtede til at gennemføre. Direktivet er således ikke til hinder for, at medlemsstaterne fastsætter regler, som er mere vidtgående end direktivet.

Desuden overlader direktivet det til medlemsstaterne at foretage visse afgrænsninger af logningsreglernes anvendelsesområde. Det drejer sig for det første om, hvilke former for kriminalitet anvendelsen af de registrerede oplysninger skal rette sig imod, og for det andet om, hvor længe de registrerede oplysninger skal opbevares.

Som anført under pkt. 2.3 gennemfører logningsbekendtgørelsen logningsdirektivets bestemmelser om pligt til at registrere og opbevare oplysninger om teletrafik. I det følgende redegøres under pkt. 3.1 for de bestemmelser i logningsbekendtgørelsen, der går videre end direktivets minimumskrav.

Under pkt. 3.2 redegøres for, hvordan Danmark har udfyldt de bestemmelser i direktivet, der overlader det til medlemsstaterne at foretage en nærmere afgrænsning af reglernes anvendelsesområde.

3.1. Hvorvidt logningsbekendtgørelsen går videre end direktivets minimumskrav

3.1.1. Logningsbekendtgørelsen går kun i få tilfælde videre end de forpligtelser, der følger af logningsdirektivet. Der er således stor lighed mellem de forpligtelser, der pålægges teleudbyderne efter henholdsvis logningsbekendtgørelsen og logningsdirektivet for så vidt angår logning af oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation, oplysninger om internettrafik samt oplysninger om brug af udbyderens egne e-mail- og internettelefonitjenester.

For så vidt angår bestemmelserne i logningsbekendtgørelsen om teleudbydernes registrerings- og opbevaringspligt (§§ 4-6), kan det oplyses, at direktivets bestemmelser om logning af oplysninger om *e-mail- og internet-telefoni-kommunikation* er implementeret ved bekendtgørelsens § 6, og at man ved implementeringen ikke er gået videre end direktivets minimumskrav.

3.1.2. Direktivets bestemmelser om logning af *fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation* er implementeret ved bekendtgørelsens § 4, og her er man på et enkelt punkt, der vedrører mobiltelefoni, gået videre end krævet i direktivet.

Efter bekendtgørelsens § 4, stk. 1, nr. 6, skal der således logges oplysninger om den første og sidste mast, som en mobiltelefon er forbundet til som led i en kommunikation, uanset at logningsdirektivet kun stiller krav om, at der logges oplysninger om den første mast, jf. artikel 5, stk. 1, litra f, nr. 1.

3.1.3. Både logningsbekendtgørelsen og logningsdirektivet omhandler følgende typer af *internetkommunikation*: internetadgang, internet e-mail og internettelefoni. Herudover stiller bekendtgørelsen krav om logning af selve internetsessionen, jf. § 5, stk. 1 og stk. 4.

I det følgende foretages der en sammenligning af bestemmelsen om registrering af internetoplysninger i logningsbekendtgørelsen med reglerne herom i logningsdirektivet med fokus på, i hvilket omfang Danmark ved implementeringen er gået videre end direktivets minimumskrav.

Logningsbekendtgørelsen sammenholdt med logningsdirektivet:

LOGNINGSBEKENDTGØRELSEN	LOGNINGSSDIREKTIVET
§ 5	**Artikel 5**
§ 5, stk. 1 Pligt til registrering af følgende oplysninger om en **internetsessions** initierende og afsluttende pakke: • afsendende internetprotokol-adresse • modtagende internetprotokol-adresse • transportprotokol • afsendende portnummer • modtagende portnummer • tidspunkt for kommunikationens start og afslutning Denne bestemmelse om sessionslogning går videre end logningskravene i direktivet. Bekendtgørelsens § 5, stk. 4 og 5, lemper i et vist omfang pligten efter stk. 1.	
§ 5, stk. 2 Pligt til **endvidere** at registrere følgende oplysninger om en brugers adgang til internettet: • tildelt brugeridentitet • den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet. • navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet. • tidspunktet for kommunikationens start og afslutning. De her nævnte oplysninger skal logges i tillæg til de i § 5, stk. 1, nævnte oplysninger, jf. formuleringen 'endvidere'. Der skal således også i relation til § 5, stk. 2, foretages logning af transportprotokol og portnumre. Denne bestemmelse har samme formål og indhold som direktivets artikel 5, stk. 1, litra a, nr. 2, og litra c, nr. 2: at skaffe data, der er nødvendige for at	**Artikel 5, stk. 1** Kategorier af data, der skal lagres: • **Litra a, nr. 2:** Data, der er nødvendige for at **spore** og **identificere kilden** til en internetkommunikation: • tildelt brugeridentitet • den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt telefonnet. • navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse (IP-adresse), en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet. • **Litra c, nr. 2:** Der skal endvidere lagres data, der er nødvendige for at fastslå internetkommunikationens dato, klokkeslæt og varighed.

spore og identificere kilden til en internetkommunikation.	
§ 5, stk. 3 Udbydere, der tilbyder trådløs adgang til internet, skal logge netværkets præcise geografiske placering. Der henvises hermed til de udbydere, der tilbyder trådløse WiFi Hot Spots, dvs. trådløse netværk, der udbydes i caféer, på restauranter eller i det offentlige rum, som f.eks. S-tog. Bestemmelsen er indsat for at logge datatrafik, der udgår fra trådløse Hot Spots. Logningsdata skal foruden trafik og brugerinformation også indeholde geografisk information om hvor det trådløse hot spot er lokaliseret/placeret. Denne bestemmelse om logning af datatrafik fra hot spots går videre end logningskravene i direktivet.	

Den ovennævnte forpligtelse i logningsbekendtgørelsens § 5, stk. 1, til at logge selve internetsessionen, dvs. kilden og endepunktet for en internetkommunikation (sessionslogning) er begrundet i operative og efterforskningsmæssige hensyn. Baggrunden for bestemmelsen er således et ønske om at kunne kortlægge en brugers samlede kommunikation, uanset om denne har karakter af traditionel telefoni eller internetaktivitet. I forbindelse med implementeringen af direktivet var det vurderingen, at denne udvidelse af logningsforpligtelsen var nødvendig for at opnå den optimale operative værdi, bl.a. henset til udbredelsen af højhastighedstinternet.

Logningsbekendtgørelsens § 5, stk. 4 og 5, indebærer dog som nævnt en lempelse af denne forpligtelse.

Logningsbekendtgørelsens § 5, stk. 4, er udtryk for et kompromis med internetudbyderbranchen. I forbindelse med udarbejdelsen af logningsbekendtgørelsen argumenterede branchen for, at datamængderne ville blive enorme, og at det i visse tilfælde ikke ville være muligt for udbyderne at logge al internettrafik. Dette medførte indsættelsen af undtagelsesbestemmelsen i stk. 4, hvorefter forpligtelsen til registrering efter stk. 1 ikke gælder, hvis denne form for registrering ikke er teknisk mulig i internetudbyderens system. I sådanne tilfælde skal udbyderen i stedet registrere hver

500. pakke, der indgår i en brugers internetkommunikation, samt tidspunktet for denne registrering. Med udtrykket 'hver 500. pakke' refereres til de datapakker, enhver internetkommunikation består af, hvilket kan være flere hundredetusinde. Det følger af vejledningen til logningsbekendtgørelsen, at man ved denne form for logning, der kaldes 'sampling', fortsat er forpligtet til at registrere oplysninger om afsendende og modtagende IP-adresse, portnumre samt transportprotokol.

Bekendtgørelsens § 5, stk. 5, om logning af data "på kanten" til andre net, er ligeledes udtryk for et kompromis med internetudbyderbranchen. I forhold til at sikre politiet en effektiv adgang til relevante oplysninger i en efterforskning ville en optimal implementering af logningsforpligtelsen bestå i en opsamling af data så tæt på brugerne som muligt, men da dette samtidig ville forudsætte en større investering hos udbyderne, specielt TDC, Telia og Telenor, blev kompromisset efter forhandlinger med disse udbydere, at logningen af trafikken skulle ske "på kanten" til andre net for at holde udbydernes udgifter til logningsudstyr på et for dem acceptabelt niveau.

3.2. Råderum for afgrænsning af logningsreglernes anvendelsesområde

I det følgende redegøres der for de bestemmelser i logningsdirektivet, der overlader det til medlemsstaterne at foretage en nærmere afgrænsning af reglernes anvendelsesområde.

3.2.1. Definition af 'grov kriminalitet'

Efter artikel 1, stk. 1, har direktivet (bl.a.) til formål at sikre, at der er adgang til de loggede oplysninger i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning.

Direktivet overlader det således til medlemsstaterne at fastlægge, hvilke typer af kriminalitet, der i hver enkelt medlemsstat skal anses for at udgøre 'grov kriminalitet' med den virkning, at oplysninger, der omfattes af logningsreglerne, efter omstændighederne kan kræves udleveret til de kompetente myndigheder.

Det følger af § 1 i logningsbekendtgørelsen, at udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i

udbydernes net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

De nærmere betingelser for, hvornår oplysningerne kan udleveres, herunder hvilke former for kriminalitet, der skal være tale om, fremgår af retsplejelovens bestemmelser om indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71, og om edition, jf. retsplejelovens kapitel 74.

Indhentelse af oplysninger om teletrafik i forbindelse med efterforskning og retsforfølgning af kriminalitet udgør efter dansk ret et indgreb i meddelelseshemmeligheden.

Det er alene politiet, der efter retsplejelovens § 780 kan foretage indgreb i meddelelseshemmeligheden, herunder få udleveret registrerede oplysninger om teletrafik. De oplysninger, som teleselskaberne er forpligtede til at registrere, vil kun kunne kræves udleveret, hvis retsplejelovens betingelser for at foretage indgreb i meddelelseshemmeligheden er opfyldt.

De nærmere betingelser for at foretage indgreb i meddelelseshemmeligheden fremgår navnlig af retsplejelovens §§ 781-783.

Retsplejelovens § 781 opstiller således særlige krav til mistankegrundlaget (mistankekravet), behovet for at foretage indgrebet (indikationskravet) samt til grovheden af den kriminalitet, som mistanken angår (kriminalitetskravet). Således kræves det, at der foreligger bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt, ligesom indgrebet må antages at være af afgørende betydning for efterforskningen. Det er endvidere et krav, at efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af f.eks. straffelovens kapitel 12 og 13, eller en række særligt oplistede bestemmelser i straffeloven, herunder § 235 om børnepornografi og § 281 om afpresning samt overtrædelse af udlændingelovens § 59, stk. 7, nr. 1-5, om menneskesmugling.

Efter retsplejelovens § 782 må indgrebet ikke være uforholdsmæssigt i forhold til indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer.

Endelig foreskriver retsplejelovens § 783, at indgreb i meddelelseshemmeligheden alene kan ske efter indhentelse af en retskendelse, medmindre indgrebets øjemed ville forspildes, hvis retskendelse skulle afventes. I så fald skal indgrebet forelægges for retten senest 24 timer fra indgrebets iværksættelse.

For så vidt angår reglerne om edition fremgår det af retsplejelovens § 804, at retten kan meddele en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande, 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. Det fremgår af retspraksis, at lagrede teleoplysninger kan kræves udleveret efter reglerne om edition, dog forudsat at de ovennævnte materielle betingelser i retsplejelovens § 781 er opfyldt, herunder kriminalitetskravet.

3.2.1. Opbevaringsperiode

Efter artikel 6 skal medlemsstaterne sørge for, at de registrerede oplysninger opbevares i mindst seks måneder og højst to år fra datoen for kommunikationen. Direktivet overlader det dermed til medlemsstaterne – inden for de nævnte grænser – at fastsætte, hvor længe de registrerede oplysninger skal opbevares.

Efter retsplejelovens § 786, stk. 4, påhviler det 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.

I overensstemmelse hermed bestemmes det i logningsbekendtgørelsens § 9, at de registrerede oplysninger skal opbevares i 1 år.

Der kan i øvrigt henvises til EU-Kommissionens evalueringsrapport af 18. april 2011 om logningsdirektivet[2], hvoraf det under pkt. 4.5 bl.a. fremgår, at én medlemsstat stiller krav om opbevaring af teledata i 2 år, én medlemsstat i 1½ år, ti medlemsstater i 1 år og tre medlemsstater i ½ år. Herudover har fem medlemsstater fastsat forskellige opbevaringsperioder for de enkelte datakategorier.

[2] Beretning fra Kommissionen til Rådet og Europa-Parlementet – Evalueringsrapport af 18. april 2011 om datalagringsdirektivet (direktiv 2006/24/EF).

3.3. Sammenfatning

Logningsdirektivet overlader efter sit indhold medlemsstaterne adgang til at foretage nogle valg, som bl.a. vil afhænge af, hvordan den enkelte medlemsstats øvrige lovgivning er indrettet, og hvordan de berørte virksomheder i den enkelte medlemsstat har indrettet sig.

Som anført under pkt. 3.1 går logningsbekendtgørelsen i få tilfælde videre end de forpligtelser, der følger af logningsdirektivet. For så vidt angår internetoplysninger betyder de udvidede forpligtelser, at selve internetsessionen skal logges, dvs. kilden og endepunktet for en internetkommunikation. Der skal tillige logges oplysninger om trådløs adgang til internettet ("hot spots"), herunder oplysninger om det lokale netværks geografiske placering samt identiteten på det benyttede kommunikationsudstyr. For så vidt angår mobil-oplysninger, skal der logges oplysninger om både den første og sidste mast, en mobiltelefon er forbundet til som led i en kommunikation.

Fra dansk side har man valgt at udvide logningsforpligtelsen for så vidt angår de ovennævnte oplysninger, idet disse set i efterforskningsmæssig sammenhæng er meget væsentlige.

4. Anden lovgivning om registrering, opbevaring og udlevering af borgernes tele- og internetkommunikation

Retsudvalget har ved sin betænkning af 31. maj 2012 anmodet Justitsministeriet om at undersøge, hvilke andre regler end logningsreglerne der indebærer, at borgernes tele- og internetkommunikation registreres og opbevares, og hvilken betydning disse regler har, jf. pkt. 4.1. Retsudvalget har endvidere anmodet Justitsministeriet om at afklare, i hvilket omfang data opbevaret efter logningsreglerne kan kræves udleveret efter andre hjemler en retsplejeloven, jf. 4.2.

Justitsministeriet har anmodet øvrige ministerier (bortset fra Statsministeriet) om bidrag herom.

Finansministeriet, Økonomi- og Indenrigsministeriet, Ministeriet for Fødevarer, Landbrug og Fiskeri, Ministeriet for Børn og Undervisning, Ligestillings- og Kirkeministeriet samt Social- og Integrationsministeriet har oplyst, at der ikke findes lovgivning inden for deres respektive ressortområder, som indebærer, at oplysninger om tele- og internetkommunikation

registreres og opbevares. Disse ministerier har endvidere oplyst, at der ikke inden for deres respektive ressortområder findes regler, der hjemler mulighed for at indhente oplysninger, der registreres og opbevares efter logningsreglerne på Justitsministeriets område.

Klima, Energi- og Bygningsministeriet, Miljøministeriet, Ministeriet for By, Bolig og Landdistrikter, Transportministeriet samt Udenrigsministeriet har endnu ikke besvaret Justitsministeriets anmodning. Når bidragene fra disse ministerier modtages, vil de blive sendt til Folketingets Retsudvalg.

Det skal bemærkes, at nogle ministerier (Ministeriet for Forskning, Innovation og Videregående Uddannelser, Beskæftigelsesministeriet, Ministeriet for Sundhed og Forebyggelse samt Kulturministeriet) har oplyst, at der inden for deres ressortområder findes lovgivning, der indeholder bestemmelser, som efter deres ordlyd umiddelbart synes at omfatte de i logningsbekendtgørelsen anførte oplysninger, men hvor der hverken er tale om egentlig registrering og opbevaring svarende til, hvad der følger af logningsreglerne, eller hjemmel til at indhente oplysninger, der registreres og opbevares efter logningsreglerne på Justitsministeriets område.

Det drejer sig bl.a. om regler om elektronisk indberetning og registrering af forskellige oplysninger. Som eksempel kan nævnes, at ansøgning om optagelse på universiteterne kan ske digitalt via en optagelsesportal, og at der sker en logning for hver enkelt ansøger. Som yderligere eksempel kan a-kassernes udbetaling af ydelser nævnes, hvor udbetalinger sker på baggrund af oplysninger, som medlemmerne har givet digitalt eller indtastet telefonisk, og som a-kasserne registrerer og opbevarer. Indhentelse, registrering eller lignende af sådanne oplysninger anses ikke for at være relevant i denne sammenhæng og er derfor ikke medtaget i redegørelsen nedenfor.

4.1. Registrering og opbevaring af borgernes tele- og internetkommunikation efter anden lovgivning end logningsreglerne

4.1.1. Forsvarsministeriet

Forsvarsministeriet har bl.a. oplyst følgende:

> ”Projektenhed for Cybersikkerhed i Forsvarsministeriet oplyser, at der på Forsvarsministeriets område findes lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler mv. (GovCERT-loven).

Loven bemyndiger statens varslingstjeneste for internettrusler (GovCERT) til uden retskendelse at behandle, herunder indsamle, registrere, analysere og opbevare tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Pakkedata er indholdet af internetbaseret kommunikation, og trafikdata er data, som behandles med henblik på overførsel af pakkedata. Loven indeholder bl.a. også regler om sletning og videregivelse af de nævnte data.

Formålet med loven er, at GovCERT kan udøve sin virksomhed som varslingstjeneste for internettrusler, og derved medvirke til, at der i staten er overblik over trusler og sårbarheder i tjenester, net og systemer relateret til internettet. Dette skal ses på baggrund af, at internettet og informationssystemer er blevet en afgørende faktor for den økonomiske og samfundsmæssige udvikling, hvorfor sikkerhed i den forbindelse får en stadig større betydning."

4.1.2. Erhvervs- og Vækstministeriet

Erhvervs- og Vækstministeriet har bl.a. oplyst følgende:

"Ifølge bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet og -tjenester (udbudsbekendtgørelsen), § 19, skal teleudbydere, hvis deres opkrævning er afhængig af forbruget, tilbyde kunden specificeret regning. Til brug for dette registrerer og opbevarer teleudbyderen oplysninger, sådan at kunden kan identificere forbruget af tjenesten. De oplysninger, teleudbyderen skal registrere, er blandt andet tidspunkt, varighed og opkaldt nummer.

Formålet med bestemmelsen er at give kunderne mulighed for at kontrollere, at teleudbyderens opkrævning for forbrug af teletjenesten er korrekt."

4.1.3. Justitsministeriet (Kriminalforsorgen)

Direktoratet for Kriminalforsorgen, har bl.a. oplyst følgende:

"*Telekommunikation*
Efter straffuldbyrdelseslovens § 57, stk. 3, optages, aflyttes eller påhøres de indsattes telefonsamtaler i lukkede institutioner uden retskendelse, medmindre dette ikke findes nødvendigt af ordens- eller sikkerhedsmæssige hensyn eller af hensyn til den forurettede ved lovovertrædelsen. Såfremt samtalen optages, påhøres eller aflyttes, skal samtalepartneren forinden gøres bekendt hermed. Optagelse af telefonsamtaler slettes, senest 6 måneder efter at de er foretaget. Telefonsamtaler med bl.a. den indsattes forsvarer og myndigheder, som den indsatte kan brevveksle ukontrolleret med, optages, påhøres eller aflyttes ikke, jf. straffuldbyrdelseslovens § 57, stk. 3.

Der er i bekendtgørelse nr. 290 af 26. marts 2012 (telefonbekendtgørelsen) fastsat nærmere regler bl.a. om optagelse af telefonsamtaler og om kontrol af samtalerne.

Det fremgår af bekendtgørelsens § 12, at de telefonsamtaler, der optages, er samtaler, som foretages af indsatte, der har fået en generel tilladelse til at telefonere til op til 10 telefonindehavere, der på forhånd er godkendt af institutionen. En sådan ordning findes på de almindelige afsoningsafdelinger i lukkede fængsler. De indsatte ringer til de godkendte numre uden personalets mellemkomst fra særligt indrettede telefoner, der er tilsluttet et system, der optager samtalerne. Optagelse af samtalen sker med henblik på senere kontrol. Kontrollen foretages ved at personalet, enten ved hyppig stikprøvevis kontrol eller med konkret begrundelse i de hensyn, der er nævnt ovenfor, lytter til den optagne telefonsamtale.

Det fremgår af en log, hvilke numre hver enkelt indsat har ringet op til. Logfortegnelsen over numrene slettes samtidig med optagelserne af samtalerne.

I arresthusene sker de indsattes telefonopkald med personalets mellemkomst. Samtalen påhøres eller aflyttes i overensstemmelse med straffuldbyrdelseslovens § 57, men optages ikke. Der foretages hyppigt, men ikke systematisk, notat i den indsattes journal, når der er givet tilladelse til at ringe.

Telefonopkald (og sms-kommunikation) foretages fra de åbne fængsler typisk fra mobiltelefoner uden internetadgang, som de indsatte lejer af fængslet til brug på egen stue. De indsatte anvender eget simkort eller betalingskort, og samtalerne påhøres, aflyttes eller optages ikke.

Internetkommunikation
I lukkede fængsler og arresthuse kan der gives indsatte med tilknytning til fængslets skole mulighed for at anvende kriminalforsorgens sikrede pc-netværk. Netværket understøtter ikke e-mail eller andre former for elektronisk kommunikation.

Netværket giver bl.a. adgang til udvalgte hjemmesider og programmer med relevans for undervisning m.v. og til en undervisningsportal med mulighed for at udveksle filer m.v. mellem elev og lærer.

Al færden på systemet logges, inklusiv anvendelse af programmer og internet.

Godkendt personale i institutionerne og i Direktoratet for Kriminalforsorgen har adgang til at gennemse logfilerne. Logfilerne slettes automatisk efter 6 måneder.

Kriminalforsorgens adgang til at registrere de indsattes anvendelse af det sikrede pc-netværk ligger i forudsætningerne for de indsattes anvendelse af netværket, idet det er en betingelse for at få adgang til det sikrede pc-netværk, at den indsatte bl.a. har accepteret, at anvendelsen registreres og gemmes i logfiler i Direktoratet, og at alle filer og konti slettes automatisk efter 6 måneder.

Efter § 2, stk. 1, nr. 15, i bekendtgørelse nr. 1046 af 4. november 2009 (genstandsbekendtgørelsen) må de indsatte ikke besidde egen computer, telefax og modem. I de åbne fængsler kan det tillades, at der udleveres en computer til opstilling i eget opholdsrum, hvis uddannelses- eller arbejdsmæssige hensyn i det enkelte tilfælde taler derfor. Der kan kun tillades udlevering af modem til internetadgang, når særlige grunde taler derfor, og det er foreneligt med ordens- og sikkerhedsmæssige hensyn.

Det er en betingelse for tilladelsen til udlevering, at den indsatte giver samtykke til, at personalet til hver en tid kan gøre sig bekendt med, hvilke programmer mv. der er på computeren. Dette anvendes bl.a. til, at personalet kan gøre sig bekendt med, at der ikke foregår e-mailkorrespondance i strid med tilladelsen. Betingelsen stilles således med henblik på, at personalet kan konstatere, om computeren anvendes uretmæssigt."

4.2. Anden hjemmel end retsplejeloven til udlevering af oplysninger, der registreres og opbevares efter logningsreglerne

4.2.1. For så vidt angår Justitsministeriets område kan det oplyses, at Datatilsynet efter persondatalovens § 62, stk. 1, kan kræve enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under persondatalovens bestemmelser.

Baggrunden for bestemmelsen, der udspringer af persondatadirektivets[3] artikel 28, stk. 3, er, at Datatilsynet som tilsynsmyndighed skal have mulighed for at kræve oplysninger udleveret af både den offentlige forvaltning og private dataansvarlige.

Bestemmelsen omfatter – jf. udtrykket "enhver oplysning" – i princippet også oplysninger registreret efter logningsbekendtgørelsen, men det må antages, at det kun i helt særlige tilfælde vil være relevant for Datatilsynet at indhente sådanne oplysninger.

[3] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

4.2.2. Efter § 73 i teleloven, som hører under Erhvervs- og Vækstministeriet, kan IT- og Telestyrelsen kræve alle oplysninger og alt materiale, som IT- og Telestyrelsen skønner relevant i forbindelse med tilsyn med overholdelse af lovens regler eller regler fastsat i medfør heraf og i forbindelse med administration, undersøgelser og konkrete afgørelser, der gennemføres og træffes efter lovens bestemmelser herom, af blandt andre udbydere af elektroniske kommunikationsnet eller -tjenester og udbydere af teleterminaludstyr, der anvendes til mobilkommunikationstjenester.

Erhvervs- og Vækstministeriet har oplyst, at bestemmelsen efter sin ordlyd principielt kunne omfatte de i logningsbekendtgørelsen anførte oplysninger, men at indhentelse mv. af sådanne oplysninger ville forudsætte, at dette kunne betragtes som relevant i forhold til de pågældende bestemmelsers formål, hvilket er usandsynligt.

4.2.3. Efter skattekontrollovens § 8 D, som hører under Skatteministeriet, skal blandt andre bestyrelser eller lignende øverste ledelser for private juridiske personer efter anmodning meddele told- og skatteforvaltningen oplysninger, der af myndighederne skønnes at være af væsentlig betydning for skatteligningen.

Skatteministeriet har oplyst, at SKAT med hjemmel i den nævnte bestemmelse i forbindelse med ligning af en skattepligtig kan anmode teleselskaberne om at oplyse den skattepligtiges brug af telefon, typisk ved fremsendelse af specificeret faktura. Skatteministeriet har endvidere oplyst, at der i praksis er tale om oplysninger, der registreres i henhold til udbudsbekendtgørelsen, jf. pkt. 4.1.2, og at det er usandsynligt, at SKAT skulle få behov for at indhente oplysninger registreret i henhold til logningsbekendtgørelsen. Efter det oplyste har Skatteministeriet ikke taget stilling til, om sådanne oplysninger i givet fald ville kunne indhentes med hjemmel i skattekontrollovens § 8 D.

5. Politiets erfaringer med logningsreglerne

Retsudvalget har ved sin betænkning af 31. maj 2012 anmodet Justitsministeriet om at sikre, at der fra politiets side fremlægges en kvalitativ og kvantitativ opgørelse over den hidtidige brug af logningsdata.

Justitsministeriet har i den forbindelse indhentet en udtalelse fra Rigspolitiet, som danner grundlag for pkt. 5.1-5.6 nedenfor.

5.1 Betydningen af den teknologiske udvikling

De senere års øgede digitalisering af samfundet har medført, at brugen af internet er en vigtig del af danskernes hverdag. Dette har en direkte indvirkning på politiets virksomhed og stiller derfor yderligere krav til politiets efterforskningsmæssige muligheder. Kriminalitetsudviklingen har samtidig vist en fortsat stigning i den organiserede kriminalitet samt en øget professionalisering og globalisering i de kriminelle strukturer.

Den øgede digitalisering af samfundet og kriminalitetsmønstrene medfører komplicerede tekniske og grænseoverskridende problemstillinger, der i takt med en drastisk stigning i internetbaserede forbrydelser medvirker til at sætte politiets efterforskningsmæssige indsats under pres. Den teknologiske udvikling vil endvidere i de kommende år medføre, at de nuværende teknologier, der anvendes til telefoni, i hastigt stigende omfang vil blive afløst af internetbaseret (IP-baseret) trafik. Denne sammensmeltning af telefoni og datatrafik vil udgøre en yderligere teknologisk udfordring for dansk politi både efterforsknings- og efterretningsmæssigt.

Beslutningen om i Danmark at udvide logningsforpligtelsen i forhold til direktivets regler skal bl.a. ses i lyset af, at Danmark allerede under tilblivelsen af logningsbekendtgørelsen i 2006 var ét af de europæiske lande med den største udbredelse af højhastighedsinternetforbindelser, hvilket medfører en ”always on” tilstand, som udvider politiets muligheder for tilgang til loggede data.

Europol fastslår i sine seneste OCTA-rapporter (Organised Crime Threat Assessments), at internetteknologi er en nøglefaktor i forhold til de kriminelle netværk, der er involveret i organiseret kriminalitet. I tilføjelse til traditionel IT-kriminalitet som hacking, kreditkortsvindel og distribution af børnepornografi spiller internetteknologi nu også en afgørende rolle i forbindelse med anden organiseret kriminalitet, såsom menneskehandel og pengefalskneri. Endvidere anvendes internetteknologi også som en sikker kommunikationsmåde og som et værktøj til hvidvaskning af penge.

Enhver kommunikation på internettet foregår ved hjælp af internetprotokol-adresser (IP-adresser), der identificerer afsender og modtager af en internetkommunikation. En IP-adresse kan populært sagt sidestilles med et telefonnummer ved telekommunikation, og alle efterlader derfor et tydeligt

aftryk, når de er på internettet[4]. I de seneste år er omfanget af disse aftryk steget drastisk i takt med, at en større del af befolkningen anvender internettet mere aktivt. Den politi- og efterforskningsmæssige indsats udfordres derfor af de øgede datamængder, som den enkelte bruger genererer ved hjælp af en lang række forskellige opkoblingsmuligheder til internettet, der alle skal afdækkes i forbindelse med indhentningen af dataoplysninger i en efterforskning.

Da logningsbekendtgørelsen blev udformet i 2006, var internetteknologien anderledes, end den er i dag. De senere års udvikling har således medført, at internetsider i dag er mere komplicerede og samtidig opbygget dynamisk, således at en internetsession nu indeholder adskillige andre sessioner, hvilket udvider og forøger den datamængde, der skal registreres (logges).

5.2. Generelt om politiets brug af loggede tele- og internetoplysninger

Tele- og internetoplysninger, der logges i medfør af logningsbekendtgørelsen, anvendes af politiet til understøttelse af den efterforsknings- og efterretningsmæssige opgave. Disse data kan grundlæggende anvendes på to forskellige måder; som bevis i en straffesag og som efterforskningsmæssigt styringsredskab.

Dansk politi har igennem de seneste 15 år anvendt loggede teleoplysninger som en bevismæssig nøglesten i forbindelse med langt de fleste større straffesager, hvorimod loggede internetoplysninger på grund af forskellige teknologiske udfordringer kun i ringe grad har været inddraget i efterforskningen.

Anvendelse af loggede data som efterforskningsmæssigt styringsredskab kan bidrage til i en indledende fase at målrette indhentningen af data, der skal bruges bevismæssigt. Denne fase indeholder en analyse og profilering af den pågældende brugers (mistænktes) kommunikation – såkaldt 'intelligence-led policing' – og er afgørende for et effektivt og ressourcebesparende politiarbejde. En sådan evidensbaseret tilgang til indhentelse af data vil give et overblik over den pågældende brugers kommunikationsmønstre, således at den efterfølgende efterforsknings- eller efterretningsmæssige indsats kan målrettes herefter. På denne måde undgår man f.eks. at binde

[4] IP-baseret trafik baserer sig grundlæggende på den såkaldte OSI-model. Dette medfører, at trafikken skal følge nogle regler og skal være opbygget på en bestemt måde, så den danner aftryk og spor, når der kommunikeres via internettet.

unødige ressourcer til en traditionel telefonaflytning, hvis den indledende analysefase har vist, at vedkommende primært kommunikerer på anden vis, ligesom der hurtigere kan iværksættes relevante indgreb, som kan tilføre sagen de afgørende beviser.

5.3. Eksempler på brug af loggede teleoplysninger

Som eksempler på konkrete sager, hvor loggede teleoplysninger har været af væsentlig betydning for efterforskningen, kan nævnes følgende:

5.3.1. Organiseret narkohandel

En udenlandsk statsborger (kuréren) blev ved grænsen til Danmark anholdt med 7,5 kg amfetamin. Kureren oplyste navn og telefonnummer på leverandøren, og politiet iværksatte en aflytning af både kurérens og bagmandens telefon. Politiet indhentede endvidere ved rettens kendelse godkendelse til at benytte sig af agentvirksomhed med henblik på opklaring af sagen.

Amfetaminen blev ved hjælp af agenten afleveret til en bestemt adresse i Danmark, hvor modtageren af amfetaminen blev anholdt.

På de aflyttede telefoner indgik der opkald fra en teleboks et nærmere angivet sted på Sjælland samt et nærmere angivet sted i Jylland. Ved hjælp af videoovervågning fra det pågældende sted i Jylland udfandt politiet yderligere to mistænkte i sagen. Politiet indhentede loggede historiske kaldsdata på de to mistænkte, og blandt andet på baggrund heraf kunne politiet sigte de pågældende.

Der blev endvidere indhentet loggede historiske kaldsdata på kurérens, modtagerens og bagmandens telefoner. På baggrund af de indhentede kaldsdata kunne politiet påvise en sammenhæng mellem de implicerede personer.

Kuréren, modtageren og yderligere to personer blev tiltalt og dømt i sagen. Bagmanden er fortsat eftersøgt internationalt.

Af rettens præmisser fremgår det, at retten ved skyldsspørgsmålet blandt andet lagde afgørende vægt på de indhentede loggede teleoplysninger.

5.3.2. Skudattentat

I forbindelse med et skudattentat ved en restaurant i Danmark indfandt tre personer sig ved restauranten og affyrede i alt 15 skud. Efter skudattentatet kørte de tre personer fra stedet.

Ud fra vidneafhøringer og en gennemgang af videoovervågning fra stedet rettede politiet mistanke mod tre medlemmer af en rockergruppe. De tre personer blev sigtet og anholdt.

På baggrund af indhentede loggede teledata kunne det bevises, at de tre personer alle forinden og efterfølgende havde været ved den pågældende rockerklubs klubhus, hvorfor det måtte antages, at attentatet var udført efter forudgående aftale og i forening. Endvidere kunne politiet på baggrund af de indhentede kaldsdata til dels fastlægge flugtruten. Der blev efterfølgende langs den formodede flugtrute udfundet overvågningsmateriale, der underbyggede politiets teori. De loggede kaldsdata viste ligeledes, at der havde været en tæt kontakt mellem de tre op til attentatet.

De blev alle tre dømt for forholdet.

5.3.3. Drab

En ældre kvinde blev fundet dræbt på sin bopæl. Kort efter det formodede gerningstidspunkt blev der hævet 6000 kr. på den dræbtes dankort. Efterfølgende blev der hævet og forsøgt hævet yderligere 12 gange.

Politiet indhentede optagelser fra de videokameraer, der dækkede de hæveautomater samt forretninger, hvor den dræbtes dankort var blevet brugt. Af disse optagelser fremgik det, at hævningerne blev foretaget af to mænd. Politiet frigav optagelserne til pressen med henblik på identifikation af de pågældende. Dette gav imidlertid ikke noget resultat.

Samtidig hermed fik politiet ved rettens kendelse tilladelse til at indhente loggede oplysninger om, hvilke mobiltelefoner der havde været i området ved gerningsstedet i det formodede gerningstidsrum, og hvilke mobiltelefoner der havde været i områderne ved hæveautomaterne og forretningerne på tidspunkterne for hævningerne.

Dette gav i første omgang anledning til mistanke mod en ung mand, men da politiet indhentede loggede kaldsdata på den unge mands mobiltelefon,

kunne det afvises, at han havde været i de områder, hvor hævekortet var blevet brugt.

Ved yderligere analyse af de nævnte historiske kaldsdata blev det konstateret, at to brødre havde været i området ved gerningsstedet og efterfølgende i området, hvor den første hævning på den dræbtes dankort var foretaget.

Gennem indhentede loggede data på disse personers mobiltelefoner kunne politiet fastlægge, at de begge havde været i området ved gerningsstedet og efterfølgende var især den enes mobiltelefon interessant, idet denne dels blev registreret på master og celler, der dækkede hver eneste hævekortautomat og forretning, og dels var det på tidspunkter i nær tilknytning til de tidspunkter, hvor hævningerne var blevet foretaget.

De to personer blev anholdt og er for tiden varetægtsfængslet blandt andet på baggrund af oplysningerne fra de indhentede loggede data. De er nu begge yderligere tilknyttet til drabet gennem DNA spor. Begge var ukendte i DNA-registeret før deres anholdelse. Sagen er nu berammet til hovedforhandling i 1. instans.

5.3.4. Drab

En 33-årig mand (A) blev af sin samlever (B) under angivelse af, at de skulle ud og fiske, lokket ud til et åløb beliggende i et landområde nogle kilometer fra deres fælles bopæl.

Ved ankomsten satte de sig et sted ved bredden, hvor de flere gange tidligere havde været for at fiske. På et tidspunkt gik B væk fra stedet under påskud af at skulle forrette sin nødtørft.

Forudgående havde B imidlertid overtalt sin tidligere kæreste (C) til at slå A ihjel. C lå som planlagt skjult i noget bevoksning ca. 8 meter bag det sted, hvor A og B sad og fiskede. Da B gik væk fra stedet, affyrede C et skud mod A med et jagtgevær. Kuglen ramte A i hovedet, og A afgik ved døden.

Efter drabet forsvandt C diskret fra stedet, mens B løb hen til en ejendom cirka 300 m fra gerningsstedet. Herfra tilkaldte hun en ambulance, idet hun angav, at der var sket en ulykke med hendes samlever A.

Efterforskningen gav straks anledning til, at politiet mistænkte B for at være involveret i drabet. B blev anholdt og fremstillet i grundlovsforhør. B nægtede ethvert kendskab til drabet og blev løsladt af retten, da retten ikke fandt, at der var tilstrækkeligt mistankegrundlag.

Ved den efterfølgende efterforskning blev mistankegrundlaget mod B bestyrket i en sådan grad, at retten tillod politiet at foretage en telefonaflytning af B samt indhente loggede historiske teleoplysninger.

På baggrund af de indhentede teleoplysninger på B, blev C interessant for efterforskningen, idet historikken viste, at B i de sidste dage op til drabet og helt frem til ca. en time før gerningstidspunktet havde kommunikeret flere gange med C pr. SMS og tale.

Der blev efterfølgende ved rettens kendelse tillige indhentet loggede historiske teleoplysninger på mobiltelefonen benyttet af C.

På baggrund af de indhentede teleoplysninger blev B og C anholdt og sigtet for drabet. Begge blev varetægtsfængslet.

Af de historiske teleoplysninger på mobiltelefonen tilhørende C fremgik det, at mobiltelefonen omkring gerningstidspunktet loggede på mobilceller, der dækkede det område, hvor drabet var sket. C´s forklaring om, at han på gerningstidspunktet havde opholdt sig på sin bopæl omkring 25 km fra gerningsstedet, og at han havde sin mobiltelefon på sig, kunne dermed tilbagevises.

C tilstod efterfølgende drabet og udpegede B, der fortsat nægtede, som medgerningsmand. B og C blev efterfølgende begge idømt 13 års fængsel for manddrab.

5.3.5. Organiseret narkohandel

I forbindelse med en narkoefterforskning blev der iværksat en aflytning af en 17-årig mand (A), som politiet havde mistænkt for at ville transportere og videregive en større mængde narkotika til en ukendt person. Transporten skulle foregå med tog fra Sjælland til Jylland.

Forinden havde politiet foretaget en telefonaflytning af en 31-årig mand (B), og af aflytningen fremgik det, at det var B, der havde arrangeret A's

togtur. A sendte under togturen en SMS til en tredjeperson (C) og oplyste, hvornår toget ville være fremme.

Politiet etablerede herefter en aktion med henblik på anholdelse af A og den endnu ukendte modtager af stoffet. Da A ankom til togstationen i Jylland, mødtes han med C, til hvem han overdrog en rygsæk, der viste sig at indeholde 10 kg hash. A og C blev anholdt.

A tilstod forholdet, men ønskede ikke at udtale sig i øvrigt. Efter indhentning af loggede historiske teleoplysninger på A's mobiltelefon kunne politiet konstatere, at A 35 dage tidligere var rejst samme tur. Politiet mistænkte A for tillige at have forestået en levering af hash på den tidligere foretagne tur, hvilket A tilstod. Han ønskede dog fortsat ikke at udtale sig om medgerningsmænd.

Ved indhentning af loggede historiske teleoplysninger på B og C's telefoner kunne politiet konstatere, at den kommunikation, de havde haft indbyrdes og med A i forbindelse med en anden leverance, svarede nøje til den kommunikation, som fandt sted 35 dage forinden.

A, B og C blev på grundlag af de loggede teleoplysninger sammenholdt med A's tilståelse, dog fortsat uden at angive sine medgerningsmænd, dømt for begge leverancer.

5.3.6. Hjemmerøverier mv.

I forbindelse med efterforskning af et hjemmerøveri blev der via en aflytning af en mobiltelefon, der blev stjålet under hjemmerøveriet, udfundet en østeuropæisk familie.

Ved en ransagning hjemme hos familien blev der fundet en større mængde tyvekoster samt effekter fra hjemmerøveriet. Familien oplyste, at de gennem det sidste års tid havde haft besøg af fire familiemedlemmer fra Balkan. De pågældende familiemedlemmer havde dog forladt Danmark på tidspunktet for ransagningen. Politiets efterforskning afdækkede imidlertid, hvilket telefonnummer den ene af de besøgende familiemedlemmerne havde benyttet under sit ophold i Danmark.

Politiet indhentede loggede historiske teleoplysninger for en længere periode på den nævnte telefon. Ved analysen af de historiske teleoplysninger kunne politiet identificere de telefonnumre, som de resterende tre besø-

gende familiemedlemmer havde benyttet i forbindelse med deres ophold i Danmark. Politiet kunne endvidere kortlægge, hvilke perioder telefonerne ikke havde været aktive i Danmark.

Oplysningerne om perioder, hvor telefonerne ikke havde været aktive i Danmark, var af betydning for en drabsefterforskning i et andet EU-land, idet efterforskningen viste, at de samme familiemedlemmer, i de perioder hvor de ikke var i Danmark, havde begået alvorlige forbrydelser i det pågældende EU-land.

På baggrund af analysen af loggede kaldsdata fra de pågældende familiemedlemmers telefoner kunne politiet konstatere, at de fire familiemedlemmer med stor sandsynlighed stod bag flere berigelsesforbrydelser, herunder endnu et hjemmerøveri. Politiet udfandt endvidere endnu et telefonnummer, som de fire familiemedlemmer havde været i tæt kontakt med.

Efter længere tids efterforskning, herunder gennemgang af 30.712 kaldsdata, kunne politiet foretage anholdelse af en mistænkt. Ved en ransagning hos den pågældende fandt politiet en container med tyvekoster til en værdi af 2.700.000 kr.

Gennemgangen af de 30.712 kaldsdata medførte endvidere, at politiet kunne bevise, at de fire familiemedlemmer havde haft kontakt med den anholdte, ligesom de havde været ved flere af gerningsstederne, herunder hjemmerøveriet.

På baggrund af beviserne i sagen, herunder den store mængde loggede teleoplysninger, blev den ene af de fire familiemedlemmer anholdt og udleveret til Danmark, hvor han efterfølgende blev idømt 3 års fængsel for deltagelse i to hjemmerøverier. De resterende tre familiemedlemmer er ikke udleveret, idet de befinder sig i deres hjemland, der ikke udleverer egne statsborgere.

Herudover blev to af de herboende familiemedlemmer dømt for medvirken til størstedelen af den berigelseskriminalitet, som de fire besøgende familiemedlemmer havde begået i Danmark, og den anholdte, hos hvem politiet fandt en container med tyvekoster, blev idømt 3 år og 6 måneders fængsel samt udvisning for bestandig for organiseret berigelseskriminalitet.

5.3.7. Hjemmerøveri

Et ældre ægtepar blev udsat for hjemmerøveri, idet fire delvist maskerede mænd trængte ind i deres hjem og truede manden til at udlevere pinkoderne til ægteparrets kreditkort samt papirerne på deres bil, hvorefter røverne tog nøglerne til bilen og forlod gerningsstedet.

Politiet fandt hurtigt den ene gerningsmand, idet han to dage forinden var blevet pågrebet i et forsøg på at begå indbrud hos ægteparret.

Politiet indhentede loggede historiske teleoplysninger på gerningsmandens mobiltelefon og kunne ud fra disse oplysninger kortlægge, hvem han havde været i kontakt med før, under og efter hjemmerøveriet.

På baggrund af disse oplysninger udpegede politiet yderligere tre mistænkte, og politiet indhentede herefter loggede historiske kaldsdata med masteoplysninger på de mistænkte. Disse oplysninger viste, at de pågældende havde været i området ved gerningsstedet omkring gerningstidspunktet samt dagen forinden. Det blev efterfølgende konstateret, at de dagen forinden havde forsøgt at gennemføre hjemmerøveriet.

Politiets egen udlæsning af mobiltelefonerne viste, at nogle af telefonerne ikke var indstillet med korrekt tidsindstilling. Såfremt politiet alene havde haft disse udlæsninger, ville dette have medført oplysninger om en anden fysisk placering på gerningstidspunktet, end tilfældet var.

Det var under hele sagen af afgørende betydning for sagens opklaring, at politiet var i besiddelse af de loggede oplysninger, idet oplysningerne kunne placere gerningsmændene på gerningsstedet på gerningstidspunktet, ligesom oplysningerne kunne placere gerningsmændene ved de hæveautomater, hvor de stjålne kort senere blev misbrugt.

De fire gerningsmænd blev alle dømt for hjemmerøveriet, og de tre af dem, der var over 18 år, blev straffet med fængsel i 5 år, mens den 17-årige gerningsmand blev straffet med fængsel i 4 år. Dommen er p.t. under anke.

5.3.8. Organiseret narkohandel

I forbindelse med efterforskning af en narkosag modtog politiet en oplysning fra en kilde om, at en person A forestod indsmugling af store mængder kokain fra Holland til Danmark.

På baggrund af denne oplysning påbegyndte politiet en efterforskning rettet mod A. A var imidlertid meget sikkerhedsbevidst, men efter politiet havde efterforsket mod personkredsen omkring A, herunder via telefonaflytninger, lykkedes det politiet at beslaglægge ca. 9 kg kokain. Ud fra de under aflytningerne fremkomne oplysninger var politiet af den opfattelse, at der tidligere var indsmuglet yderligere 10 kg kokain.

Umiddelbart efter beslaglæggelsen af de 9 kg kokain foretog politiet anholdelse af fem personer, der alle blev sigtet og varetægtsfængslet for medvirken til de to indsmuglinger. På daværende tidspunkt var det dog ikke muligt for politiet at påvise, at det var A, der var bagmanden for indsmuglingerne, idet han havde sørget for at holde sig på afstand af selve indsmuglingerne, og således ikke selv havde været i direkte berøring med kokainen.

Ved anholdelsen af de fem gerningsmænd fandt politiet flere telefoner, som politiet ikke tidligere havde været bekendt med. Politiet indhentede loggede historiske teleoplysninger samt masteoplysninger på telefonerne og kunne herefter sammenstykke et billede, der viste A's rolle i forbindelse med indsmuglingerne.

Alene på baggrund af de loggede historiske teleoplysninger, herunder masteoplysningerne, var anklagemyndigheden i stand til at bevise, at A var bagmanden.

Han blev idømt 12 års fængsel for de to indsmuglinger.

5.3.9. Flere forhold af drab, våbenbesiddelse og vold

I forbindelse med efterforskning af en større rockersag indhentede politiet mere end 730.000 loggede historiske kaldsdata på i alt ca. 85 telefonnumre.

Foruden vidneforklaringer udgjorde de historiske teleoplysninger en meget stor del af de afgørende beviser i sagen. De loggede historiske teleoplysninger understøttede således afgørende vidneforklaringer under den meget omfattende sag.

Der blev i sagen rejst tiltale mod i alt 16 personer med relation til rockermiljøet. 14 ud af de 16 tiltalte blev ved Østre Landsret idømt langvarige fængselsstraffe for bl.a. seks drabsforsøg.

5.4. Eksempler på brug af loggede internetoplysninger

På grund af tekniske udfordringer ved den praktiske anvendelsen af loggede internetoplysninger (beskrevet nærmere nedenfor under pkt. 5.5) har der hidtil kun i sparsomt omfang været indhentet loggede internetoplysninger, og der er som følge heraf kun få eksempler på konkrete sager, hvor internetlogning har haft betydning for bevisførelsen.

5.4.1. Databedrageri

Den pågældende politikreds modtog en anmeldelse fra en dansk online betalingsformidler, der oplyste, at flere af deres kunders konti var blevet hacket og efterfølgende benyttet til at indsætte penge på under anvendelse af stjålne kreditkortoplysninger. Pengene var efterfølgende blevet overført fra kundernes konti til et online pokerspil i udlandet. Det kunne konstateres, at en mindre del af udbyttet var overført til en dansk bank som gevinst fra online spil.

Den danske online betalingsformidler kunne til politiet oplyse, at der på de forskellige hackede konti var benyttet flere forskellige IP-adresser, men én bestemt IP-adresse var benyttet til at logge ind på alle de hackede konti, hvorfor der var en formodning om, at der var tale om én gerningsmand.

Gerningsmanden havde benyttet både hotmail-adresser og gmail-adresser, hvorfor Rigspolitiets IT-Efterforskningssektion anmodede Microsoft og Google om logningsoplysninger vedrørende de IP-adresser, der var benyttet til indlogning på de omhandlede mailkonti.

Efter indhentelse af en editionskendelse blev det pålagt to internetudbydere at oplyse, hvilke kundeforhold der lå til grund for anvendelse af IP-adresserne. Dette medførte, at politiet fik oplysninger om, hvilke personer der benyttede de pågældende IP-adresser.

På baggrund af de loggede oplysninger kunne politiet konstatere, at den pågældende person afsonede en fængselsstraf for ligeartet kriminalitet. Den pågældende blev på denne baggrund samt sagens øvrige omstændigheder identificeret som værende gerningsmanden.

I den efterfølgende efterforskning førte de indhentede oplysninger om IP-adresser til, at gerningsmanden blev sigtet for yderligere forhold vedrørende hacking, databedrageri, bedrageri og udbredelse af kreditkortoplysninger.

Den pågældende politikreds har oplyst, at det i den indledende efterforskning var af afgørende betydning, at internetudbyderne var i stand til at udlevere loggede oplysninger om de kundeforhold, der lå bag IP-adresserne. Såfremt politiet ikke havde kunnet modtage disse oplysninger, havde politiet sandsynligvis ikke haft mulighed for at identificere gerningsmanden.

Sagen resulterede i, at gerningsmanden blev idømt 1 år og 9 måneders fængsel for bl.a. hacking, databedrageri og udbredelse af kreditkortoplysninger.

5.4.2. Røverier

En politikreds har i en verserende sag om røveri af særlig farlig karakter, hvor to gerningsmænd i flere tilfælde har truet butikspersonale med et skarpladt oversavet jagtgevær til at udlevere kontantbeløb, rekvireret data fra en sessionslogning hos TDC, der netop har implementeret et nyt system (nærmere herom nedenfor under pkt. 5.5.1.2).

Sessionslogningen kunne anvendes til at stedfæste den ene gerningsmands færden, idet hans mobiltelefon løbende har haft automatiske internetsessioner, der er logget hos TDC. Sessionsdata indeholder i medfør af logningsbekendtgørelsen geografisk information, og gerningsmandens færden kan dermed kortlægges i videre omfang, end det ville have været muligt ved hjælp af historiske teleoplysninger, da telemasterne kun registrerer trafik, der genereres ved aktiv anvendelse af telefonen. Denne sessionslogning har således haft afgørende indflydelse på sagen.

5.4.3. Netbankindbrud

En person anmeldte tyveri af 100.000 kr. via sin netbank. De indledende undersøgelser i sagen viste, at pengeoverførslen var sket fra anmelderens egen IP-adresse, og politikredsen indhentede herefter sessionslogning fra anmelderens internetudbyder i et forsøg på at afklare, hvorvidt hans påstand om ikke selv at have overført pengene var troværdig.

Da der var tale om en mindre internetudbyder med et begrænset antal brugere, var udbyderens sessionslogning opsat til at registrere den enkelte brugers internetkommunikation (nærmere herom nedenfor under pkt. 5.5.1.1). Det har som følge heraf været muligt for Rigspolitiets IT-Efterforskningssektion at anvende oplysningerne i sessionslogningen til fremsøgning af det tidspunkt, hvor banken har oplyst, at overførslen fandt sted. Samtidig med, at bankens kunde selv har overført et mindre beløb, har kundens computer været tilgået fra en udenlandsk IP-adresse, der er tidligere kendt i forbindelse med økonomisk internetkriminalitet.

Der er hermed etableret en efterforskningsmulighed, der ellers ikke ville have været tilgængelig, da denne type kriminalitet ofte udøves på en måde, der ikke efterlader digitale spor.

5.5. Tekniske udfordringer ved logning og brug af internetoplysninger

Der har som anført ovenfor vist sig at være en del tekniske udfordringer forbundet med den praktiske anvendelse af internetlogning. Under pkt. 5.5.1 beskrives de udfordringer, der er forbundet med internetudbydernes implementering af logningsbekendtgørelsens regler om internetlogning, og under pkt. 5.5.2 beskrives de tekniske udfordringer i dansk politi.

5.5.1. Udbydernes logning af internetoplysninger

Logningsbekendtgørelsens § 5 om internetoplysninger omhandler både såkaldt 'sessionslogning' efter stk. 1 og oplysning om en brugers adgang til internettet efter stk. 2. Ved sessionslogning efter bekendtgørelsens § 5, stk. 1, tages der udgangspunkt i den enkelte bruger med henblik på at identificere dennes internetkommunikation, og ved logning efter bekendtgørelsens § 5, stk. 2, tages der udgangspunkt i en given internetkommunikation med henblik på at identificere den relevante bruger.

5.5.1.1. Sessionslogning

Sessionslogning kan anvendes i forbindelse med 'intelligence-led policing', som omtalt ovenfor under pkt. 5.2, og som efterforskningsredskab i sager om organiseret kriminalitet og terrorsager, hvor man er interesseret i at klarlægge en mistænkts eventuelle kontakt til ekstremistiske fora på internettet. I takt med at kommunikationsformerne bliver stadigt mere virtuelle, kan sessionslogning også være relevant som supplement til telefonilogning efter logningsbekendtgørelsens § 4. Der er imidlertid alvorlige praktiske problemer forbundet med anvendelsen af den sessionslogning, som internetudbyderne er forpligtede til at foretage.

For at en sessionslogning skal kunne anvendes til at identificere en bestemt brugers internetkommunikation, skal den være tilknyttet den pågældende bruger, som tilfældet er vedrørende telefonilogning, dvs. man skal kunne tage udgangspunkt i den enkelte brugers IP-adresse og identificere, hvilke andre IP-adresser brugeren har været i kontakt med. Dette er også udgangspunktet i logningsbekendtgørelsens § 5, stk. 1, der fastslår en forpligtelse til at registrere afsendende og modtagende IP-adresse ved en internetsessions initierende og afsluttende pakke, tidspunkt for kommunikationen samt oplysninger om transportprotokol og portnumre, der kan bruges til at identificere kommunikationens nærmere karakter.

Som omtalt ovenfor er der i bekendtgørelsens § 5, stk. 4, indsat en undtagelse til hovedreglen om sessionslogning efter § 5, stk. 1, hvorefter udbyderne kan nøjes med at logge hver 500. datapakke, der indgår i en slutbrugers kommunikation på internettet. Da logningsbekendtgørelsen trådte i kraft den 15. september 2007, var de tekniske muligheder anderledes, end de er i dag, og efter Rigspolitiets opfattelse valgte en stor del af internetudbyderne derfor at gøre brug af undtagelsesbestemmelsen i stk. 4 i stedet for hovedreglen i stk. 1.

Implementeringen af logningen blev imidlertid gennemført på en sådan måde, at den stort set blev uanvendelig, hvilket stod klart for politiet, da man første gang ønskede at gøre brug af sessionslogning i forbindelse med efterforskningen af en straffesag.

Problemet med logningen er, at internetudbyderne, jf. bekendtgørelsens § 5, stk. 5, foretager registreringen af internetkommunikation på kanten til andre net i deres netværk, dvs. lige inden deres brugere sendes videre til de

modtagende IP-adressers servere. Her registrerer de i overensstemmelse med bekendtgørelsens § 5, stk. 4, hver 500. pakke, der passerer serveren, men da datatrafikken på kantserveren er genereret af flere hundrede brugeres internetkommunikation, er det vilkårligt, hvilke brugeres data der logges i hver 500. pakke. På denne måde kan manglende fund af data fra en brugers IP-adresse hverken bruges til at be- eller afkræfte, om den pågældende rent faktisk har været aktiv på internettet i det pågældende tidsrum, og den foretagne logning er hermed som udgangspunkt i praksis uanvendelig i politiets efterforskning, når bortses fra de 'heldige' tilfælde, hvor den pågældende brugers internetkommunikation tilfældigvis er blevet fanget i en logget datapakke.

De mindre udbydere har dog i dag i et vist omfang mulighed for at sessionslogge den enkelte brugers kommunikation. De mindre udbyderes tekniske løsninger hertil kan ikke anvendes af de store udbydere på grund af datamængdernes størrelse og infrastrukturens indretning. TDC har imidlertid for nylig implementeret en løsning, som indebærer, at udbyderen sessionslogger den enkelte brugers sessioner for så vidt angår mobil datatrafik, mens trafik, der udgår fra TDCs fastnet-internetprodukter, ikke på nuværende tidspunkt er omfattet.

Et eksempel på de mindre udbyderes muligheder for at sessionslogge fremgår af sagen omtalt i pkt. 5.4.2, og et eksempel på TDCs nye muligheder for at sessionslogge mobil datatrafik fremgår af sagen omtalt i pkt. 5.4.3.

5.5.1.2. Oplysning om en brugers adgang til internettet

For at politiet kan efterforske, hvem der står bag f.eks. distribution af børneporno, hacking af netbank, identitetstyveri mv. er det nødvendigt at kunne henføre en bestemt IP-adresse til en fysisk internetabonnent, hvorfor internetudbyderne ifølge logningsbekendtgørelsens § 5, stk. 2, er forpligtet til at logge deres brugeres IP-adresser.

Internetudbyderne leverer både *internet via kabler* til husstande, offentlige institutioner mv. og *mobilt internet* via master til bl.a. mobiltelefoner. For så vidt angår kabelinternet er det ikke problematisk for internetudbyderne at identificere abonnenten – om end ikke den enkelte bruger – bag en anvendt IP-adresse, da man ved angivelse af dato og tidspunkt for den relevante internetkommunikation vil kunne finde frem til, hvilken abonnent der på det pågældende tidspunkt var tildelt den pågældende IP-adresse.

Situationen er imidlertid en anden vedrørende mobilt internet, da en lang række brugere i forbindelse med deres samtidige internetkommunikation tildeles den samme IP-adresse på det samme tidspunkt. På denne måde fremstår de pågældende brugernes identitet 'ens' i forbindelse med oprettelse af kontakt til den modtagende internetsides IP-adresse. Den eneste måde, hvorpå man efterfølgende kan adskille brugerne fra hinanden og finde frem til deres oprindelige individuelle IP-adresser, er ved angivelse af, hvilke porte der har været anvendt i forbindelse med internetkommunikationen. En port kan nemlig kun benyttes af én bruger/IP-adresse ad gangen.

Problemet opstår herefter ved, at internetudbyderne – på trods af kravet herom ifølge logningsbekendtgørelsens § 5, stk. 1 – ikke registrerer, hvilke portnumre der har været anvendt ved den mobile internetkommunikation. Da den modtagende internetsides server som udgangspunkt heller ikke registrerer oplysninger om anvendte porte, er det således ikke muligt for udbyderen at fremfinde brugeren af en bestemt IP-adresse på et bestemt tidspunkt. TDC har imidlertid netop implementeret en ny løsning til håndtering og logning af mobildatatrafik. Dette system lagrer data i fuld overensstemmelse med logningsbekendtgørelsens regler, og er allerede anvendt i flere tilfælde (se pkt. 5.4.2).

5.5.2. Tekniske udfordringer i dansk politi

Den begrænsede anvendelse af loggede data vedrørende internettrafik kan tilskrives flere årsager. Ud over de implementeringsmæssige udfordringer er én af hovedårsagerne det teknologiske modenhedsniveau i dansk politi.

Håndtering af data fra indgreb i meddelelseshemmeligheden vedrørende internet kan i denne sammenhæng ske på to forskellige måder; som internetaflytning eller som historiske internetoplysninger.

Aflytning af internettrafik håndteres i systemet Evident Operator, der varetages af Rigspolitiet. Dette system er primært udviklet til at håndtere telefonaflytninger, og er derfor i praksis uanvendeligt til håndtering af internetaflytninger. Anvendelse af internetaflytning sker derfor kun i sager, hvor Politiets Efterretningstjeneste forestår efterforskningen, eller hvor Rigspolitiets IT-Efterforskningssektion bistår politikredsene med indgrebet.

Loggede historiske internetoplysninger håndteres i systemet RAVEN, der også varetages af Rigspolitiet. Dette system blev indkøbt umiddelbart inden logningsbekendtgørelsen trådte i kraft, men var reelt først funktionsdygtigt i 2010. Dette skyldtes bl.a. et længere forløb efter logningsbekendtgørelsens ikrafttræden vedrørende det såkaldte 'fælles format'[5]. Forløbet drejede sig om etableringen et fælles dataformat, som de loggede data skulle afleveres i fra teleudbyderne, når de blev overført til Rigspolitiet. Der viste sig imidlertid ikke at være hjemmel til at pålægge udbyderne at aflevere data i et sådant fælles format, hvilket medførte, at systemet måtte ombygges og først var funktionsdygtigt i 2010. Det viste sig dog hurtigt, at systemet ikke kunne understøtte de efterforsknings- og styringsmæssige visioner, der oprindeligt lå bag logningsbekendtgørelsen, og systemet anvendes derfor i dag kun som lagringsplads for historiske telefoni- og internetdata.

5.6. Sammenfatning

Oplysninger om tele- og internettrafik, der registreres og opbevares i medfør af logningsbekendtgørelsen, er generelt af meget væsentlig betydning for politiets efterforskning og opklaring af alvorlige forbrydelser. Loggede oplysninger kan navnlig være af afgørende betydning i forhold til at kortlægge mistænktes færden samt kontakt til sagens øvrige personer.

Den teknologiske udvikling har medført, at brug af internet opfattes som en naturlig del af de fleste menneskers hverdag. Internettet anvendes således i stadigt større omfang, herunder også som kommunikationsmiddel.

Der anvendes endvidere i stigende grad kryptering af den internetbaserede kommunikation med henblik på at sikre privatlivets fred samt sløring af kriminelle aktiviteter. Krypteringen betyder, at det ikke er muligt for politiet igennem aflytning at gøre sig bekendt med indholdet af en mistænkts kommunikation, og værdien af aflytningsindgreb reduceres hermed væsentligt. For at imødegå udfordringerne ved den øgede brug af krypteret internetkommunikation er det af afgørende betydning for politiet at kunne analysere internettrafikdata, som i vidt omfang alene sikres i kraft af logningsbekendtgørelsens regler.

For yderligere kvantitative oplysninger om den hidtidige brug af logningsdata kan henvises til Justitsministeriets breve af 29. maj 2012, 8. december

[5] Se 'Regeringens handlingsplan for terrorbekæmpelse' fra november 2005, pkt. 24.

2011, 5. oktober 2010 og 19. juni 2009, hvorved Retsudvalget orienteres om statistik vedrørende logningsdirektivets anvendelse i 2011, 2010, 2009 og 2008 udarbejdet til brug for afrapportering til EU-Kommissionen.

6. Efterretningstjenesternes erfaringer med logningsreglerne

Retsudvalget har ved sin betænkning af 31. maj 2012 anmodet Justitsministeriet om at sikre, at der for efterretningstjenesternes vedkommende fremlægges en kvalitativ opgørelse over, hvor effektive de forskellige elementer af logning indtil nu har været i kampen mod terror og kriminalitet, så vidt dette er muligt uden at kompromittere efterretningstjenesternes arbejde.

Justitsministeriet har i den forbindelse indhentet oplysninger fra Politiets Efterretningstjeneste og Forsvarsministeriet.

Forsvarsministeriet har oplyst, at logningsdirektivet og logningsbekendtgørelsen ikke ses at have relevans for Forsvarsministeriet.

Politiets Efterretningstjeneste har oplyst følgende:

> ”Politiets Efterretningstjeneste kan oplyse, at efterretningstjenesten anvender oplysninger om teletrafik i betydeligt omfang navnlig i forbindelse med længerevarende efterforskninger inden for terrorområdet, og oplysningerne om teletrafik har i flere tilfælde haft afgørende betydning for at kunne afdække terrorrelationer i både ind- og udland.
>
> Politiets Efterretningstjeneste kan endvidere oplyse, at oplysninger om telekommunikation (fastnet- og mobiltelefoni) og oplysninger om internetkommunikation, der registreres og opbevares i medfør af logningsbekendtgørelsen, generelt er af væsentlig betydning og i nogle tilfælde har været af afgørende betydning for efterforskning og retsforfølgning af alvorlige forbrydelser.
>
> For så vidt angår anvendelse af teledata fra sessionslogning kan det oplyses, at det i meget begrænset omfang har været relevant at indhente sådanne oplysninger i forbindelse med efterforskning.”