

Afrapportering fra den tekniske arbejdsgruppe om terrorbekæmpelse

Indholdsfortegnelse

1	Baggrund.....	1
2	Overordnet konklusion	3
3	Tværgående spørgsmål.....	3
4	Gennemgang af anbefalingerne.....	11
4.1	Anbefaling 15.....	11
4.2	Anbefaling 17.....	15
4.3	Anbefaling 18.....	19
4.4	Anbefaling 25.....	22
5	Forslag til lovtekst og specielle bemærkninger.....	24
6	Bilag.....	38
6.1	Definitioner.....	38
6.2	Redegørelse for arbejdsgruppens arbejde.....	41
6.3	Skøn over omkostninger (branchebidrag).....	42

1 Baggrund

Regeringen fremlagde den 16. november 2005 en handlingsplan for terrorbekæmpelse på baggrund af rapporten ”Det danske samfunds beredskab og indsats mod terror” fra en tværministeriel arbejdsgruppe nedsat af Statsministeriet.

Af ”Regeringens handlingsplan for terrorbekæmpelse” fremgår det, at det er regeringens opfattelse, at der skal arbejdes videre med arbejdsgruppens anbefalinger, at en betydelig del af arbejdet vil bestå i at konkretisere anbefalingerne samt at en række af initiativerne vil kræve yderligere overvejelser, før regeringen vil kunne tage politisk stilling.

I regeringens handlingsplan fremhæves det, at regeringen er meget opmærksom på at holde balancen mellem sikkerhed og retssikkerhed for at beskytte de værdier, vores samfund bygger på.

Særligt på teleområdet bliver der i handlingsplanen taget højde for behovet for at iværksætte et udredningsarbejde i samarbejde med branchen med henblik på afklaring af de tekniske konsekvenser af de forskellige anbefalinger – og i muligt omfang omkostningsskøn.

På den baggrund har der været gennemført en proces, hvor der, i en teknisk arbejdsgruppe under Videnskabsministeriet, har været arbejdet med konkretisering af anbefaling 15, 17, 18 og 25 i samarbejde med de relevante parter i branchen, Justitsministeriet, Politiets Efterretningstjeneste og IT- og Telestyrelsen. Øvrige anbefalinger på teleområdet, som tænkes gennemført ved lovgivning i foråret 2006, har ikke været drøftet.

Videnskabsministeriets tekniske arbejdsgruppe har således særligt haft til formål at konkretisere rammerne for mulige tekniske løsninger, herunder at estimere omkostningsniveauerne med henblik på at identificere afbalancerede løsninger.

Videnskabsministeriets tekniske arbejdsgruppe har i første omgang fokuseret på følgende 4 anbefalinger:

Anbefaling 15. *Arbejdsgruppen anbefaler, at § 15 i lov om konkurrence- og forbrugerforhold på telemarkedet ændres, så udbydere af elektroniske kommunikationsnet og -tjenester får pligt til at indrette deres tekniske udstyr på en måde, der gør indgreb i meddelelseshemmeligheden muligt uanset teknologisk fremføringsform.*

Anbefaling 17. *Arbejdsgruppen anbefaler, at der i telelovgivningen fastsættes krav om, at politiet hos alle teleudbydere skal have mulighed for at indhente fremadrettede tele- og masteoplysninger, samtidig med at disse registreres, hvilket vil sige samtidig med, at en person foretager et opkald, aktiverer en sendemast og lignende. Forpligtelsen bør kunne opfyldes ved out-sourcing.*

Anbefaling 18. *Arbejdsgruppen anbefaler, at der i telelovgivningen fastsættes krav om, at politiet hos alle teleudbydere skal have mulighed for at indhente historiske tele- og masteoplysninger. Der er behov for, at teleudbyderne forpligtes til at iværksætte sådanne indgreb straks og på en måde, så hensigten med indgrebet ikke forspildes.*

Anbefaling 25. *Arbejdsgruppen anbefaler, at teleudbydere pålægges løbende at opdatere relevante teledatabaser med oplysninger om telefonnummer, rette operatør og nummerets bruger.*

Denne afrapportering vedrører således alene disse 4 anbefalinger.

Den tekniske arbejdsgruppe har drøftet anbefalingernes formål og omfang, har identificeret problemstillinger i forhold til de enkelte anbefalinger, og fremkommet med løsningsforslag, herunder præciseringer.

Der forventes fremsat lovforslag ved udgangen af første kvartal 2006.

Efter fremsættelse af lovforslaget vil Videnskabsministeriets tekniske arbejdsgruppe fortsætte med at behandle enkelte yderligere anbefalinger med henblik på at kunne afgive en teknisk og økonomisk udredning 1. juli 2006.

2 Overordnet konklusion

Det må på baggrund af arbejdsgruppens drøftelser konkluderes, at der i dag generelt eksisterer eller i de fleste tilfælde kan findes tekniske metoder, der kan imødekomme de hensyn, der ønskes tilgodeset med de 4 anbefalinger. Med de meget forskelligartede produktionsmetoder, der benyttes i telesektoren, har det dog ikke været muligt at undersøge alle forhold. Det må derfor forudses, at udmøntningen ikke kan gennemføres ensartet. Det vil i øvrigt være af stor betydning at afgrænse forpligtelsen, jf. også afsnit 3.4, 3.5 og 3.6 nedenfor.

Det skal bemærkes, at de investeringer, der vil være behov for, især er afhængige af udmøntningen af logningsbekendtgørelsen, jf. afsnit 3.1. om logningsbekendtgørelsen nedenfor.

Arbejdsgruppen konstaterer, at den manglende tidsmæssige sammenhæng mellem lovpakken i foråret 2006 og logningsbekendtgørelsen skaber en usikkerhed.

Arbejdsgruppen lægger derfor vægt på, at der sikres en tidsmæssig sammenhæng mellem ikrafttrædelsestidspunktet for de to regelsæt.

Det manglende tidsmæssige sammenfald mellem lovpakken i foråret 2006 og færdiggørelsen af logningsbekendtgørelsen og den deraf afledte tekniske og økonomiske usikkerhed gør efter telebranchens (TI, ITEK og ITB) opfattelse en udskydelse af logningsdelen i § 15 hensigtsmæssig, medmindre den udvidede forpligtelse i Teleloven baseres på en fuld omkostningsdækning.

3 Tværgående spørgsmål

3.1 Relationen til logningsbekendtgørelsen

Arbejdet omkring terrorbekæmpelse består af to dele: dels implementering af regeringens terrorpakke fra 2002 (logningsbekendtgørelsen), hvor Justitsministeriet er ansvarligt ressortministerium, dels implementering af regeringens nye handlingsplan for bekæmpelse af terror.

I forbindelse med implementeringen af handlingsplanen har Videnskabsministeriet ansvaret for implementeringen af en række af de initiativer i handlingsplanen, der vedrører it- og teleområdet. I andre tilfælde yder ministeriet teknisk bistand til anbefalinger, som Justitsministeriet skal implementere, ligesom det er tilfældet med logningsbekendtgørelsen.

De anbefalinger, som har været behandlet i Videnskabsministeriets tekniske arbejdsgruppe, har dog nær sammenhæng med de spørgsmål, der behandles som en del af logningsbekendtgørelsen. Handlingsplanen indeholder en række yderligere anbefalinger, der har sammenhæng med logningsforpligtelsen. Disse anbefalinger har ikke været drøftet i denne arbejdsgruppe.

Udmøntningen af logningsforpligtelsen forventes at ligge klar i efteråret 2006, mens de anbefalinger, som Videnskabsministeriet skal udmønte, indgår i en forårspakke.

Det har den konsekvens, at det lovforslag, der skal udmønte de 4 anbefalinger på Videnskabsministeriets område, har karakter af rammeforpligtelser, der for så vidt angår registrering af bagudrettede oplysninger, først udfyldes, når Justitsministeriet udsteder logningsbekendtgørelsen.

Det har endvidere den konsekvens, at det er vanskeligt at estimere de økonomiske konsekvenser af lovforslaget, fordi konsekvenserne vil være meget afhængige af udmøntningen af logningsforpligtelsen.

Endelig betyder det, at dele af Videnskabsministeriets lovforslag vil træde i kraft samtidig med logningsbekendtgørelsens ikrafttræden, da det ikke vil være muligt for udbyderne at vide, hvad deres systemer skal indrettes til at kunne, før denne bekendtgørelse er endelig.

I den forbindelse må der forventes at være en rimelig overgangsperiode i logningsbekendtgørelsen, som vil gælde tilsvarende for Videnskabsministeriets lovforslag, af hensyn til at udbyderne skal have mulighed at indrette deres systemer efter kravene i logningsbekendtgørelsen.

Såfremt sammenhængen mellem anbefalingerne og den kommende logningsbekendtgørelse giver anledning til overvejelser om at udskyde lovforslaget, kunne en løsning være at udskyde lovforslag om de relevante dele af anbefalingerne 15 og 18, indtil indholdet af bekendtgørelsen er kendt.

Arbejdsgruppen har ikke vurderet fordele og ulemper ved en sådan udskydelse, men vurderer, at det vil være teknisk og juridisk muligt at afgrænse forpligtelserne knyttet til logning fra den øvrige del, således at gennemførelsen af handlingsplanens anbefalinger ikke ville blive forsinket heraf.

3.2. Samarbejde

Der blev på møderne om udmøntning af anbefalingerne på teleområdet tilkendegivet udbredt enighed om, at der i fremtiden vil være behov for at fortsætte det hidtidige gode løbende samarbejde mellem branchen og politiet/PET om den praktiske håndtering af forpligtelserne til at bistå politiet i deres efterforskningsarbejde. Dette samarbejde skal sikre den fælles forståelse af forventningerne til den bistand, der skal ydes til politiets efterforskningsarbejde

På baggrund af den hastige teknologiske udvikling vil der desuden være et behov for løbende ad hoc drøftelser i et forum med myndighederne (Videnskabsministeriet og Justitsministeriet). Der vil i et sådan forum blive behov for drøftelser f.eks. i forbindelse med udviklingen af nye teknologier og tjenester, så det sikres at reglerne om kriminalitetsbekæmpelse, herunder terrorbekæmpelse, kan opfyldes.

I lighed med de konklusioner, der drages i en svensk udredning på området¹, skønnes det ikke hensigtsmæssigt med en fuldstændig udtømmende opremsning af, hvordan forpligtelserne skal udmøntes i f.eks. en bekendtgørelse. Det skyldes

¹ Jf. "Tillgång till elektronisk kommunikation i brottsutredningar m.m." - SOU 2005:38. Rapporten kan findes på <http://www.regeringen.se/sb/d/5073/a/44989>.

dels hensynet til den teknologiske udvikling, der ville indebære behov for jævnlige opdateringer, dels hensynet til, at udbydernes net er indrettet forskelligt, og at målene mest økonomisk opnås ved individuelle løsninger.

Disse løsninger foreslås derfor tilvejebragt gennem drøftelser i det foreslåede forum med myndighederne.

3.3. Definitioner

Det skal bemærkes, at for så vidt angår definitioner af en række nøglebegreber i forbindelse med implementeringen af anbefalingerne 15, 17 og 18 er det de gældende definitioner i Retsplejelovens kapitel 71, der finder anvendelse.

Definitionerne fremgår af vedlagte bilag.

Dette skyldes, at anbefalingerne 15, 17 og 18 drejer sig om at sikre rammerne for politiets mulighed for indgreb i meddelelshemmeligheden, jf. Retsplejeloven.

Det skal desuden bemærkes, at til brug for udmøntningen er de 4 anbefalinger vurderet ud fra deres formål og ikke ud fra en ordlydsfortolkning. Dette skyldes, at en streng ordlydsfortolkning kunne føre til en for snæver fortolkning af anbefalingerne, i forhold til sammenhængen til resten af handlingsplanen.

3.4. Pligtssubjekt

Pligtssubjektet i forhold til alle fire anbefalinger kan efter arbejdsgruppens vurdering afgrænses til udbydere af elektroniske kommunikationsnet og – tjenester til slutbrugere, jf. § 6, stk. 1, i lov om konkurrence- og forbrugerforhold på telemarkedet. Der henvises til oversigten over definitioner, jf. bilag 1.

For så vidt angår den bagudrettede forpligtelse afgrænses pligtssubjektet yderligere af regler udstedt i medfør af den første ”terrorlov-pakke”, jf. L 35, forslag til 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. Dette forklares nærmere i svar fra Justitsministeren på spørgsmål 63 og 123 fra Retsudvalget til lovforslaget.

Det fremgår af rapporten ”Det danske samfunds indsats og beredskab mod terror”, at det kan overvejes at give udbyderne mulighed for at out-source forpligtelsen, således at indgrebet rent faktisk finder sted hos f.eks. den netværksudbyder, hvis net den pågældende mindre udbyder eller en tjenesteudbyder benytter.

Arbejdsgruppen har ligeledes vurderet, at det vil være hensigtsmæssigt at udbyderen kan out-source forpligtelsen til indretning af udstyr og systemer, således at indgreb i meddelelshemmeligheden er mulig. Den udbyder, som forpligtelsen påhviler, bør have mulighed for at aftale med f.eks. en anden udbyder, at de praktiske indgreb kan ske i den anden udbyders domæne. Det kan f.eks. gøre sig gældende for gensalgsubydere og bolignet.

Efter arbejdsgruppens vurdering kan forpligtelsen afgrænses således, at den udbyder, der har slutbrugerforholdet, som udgangspunkt har ansvaret for at sikre, at der kan gives adgang til indgreb i meddelelshemmeligheden. Umiddelbart kunne der være økonomiske og sikkerhedsmæssige fordele ved, at indgrebene kun fandt sted hos nogle få, større udbydere. Fordelene kan høstes via out-sourcing, men det er vigtigt at sikre en klar placering af ansvaret, herunder for, at al trafik kan gøres til genstand for et indgreb i meddelelshemmeligheden.

Det er stadig den udbyder, som out-sourcer forpligtelsen, der er ansvarlig for, at den udbyder, forpligtelsen er out-sourcet til, indretter systemet, så indgreb i meddelelshemmeligheden kan finde sted.

3.5. Omfang af udbyderbegrebet

Som det fremgår af besvarelsen af de ovenfor nævnte spørgsmål, kan bl.a. arbejdsgivere ikke anses for at være udbydere af elektroniske kommunikationsnet- og tjenester i forhold til de ansatte, som man stiller intern teleinfrastruktur og tjenester til rådighed for i forbindelse med ansættelsesforholdet. Dette gælder både computere, infrastruktur m.v., der benyttes på arbejdspladsen, og evt. hjemmearbejdspladser, jf. også svaret på spørgsmål 123.

Det er i den forbindelse uden betydning, hvorvidt arbejdsgiveren selv forestår (etablerer, overvåger og driver) den omhandlede interne infrastruktur og de omhandlede interne tjenester (såvel telefoni som data), eller om virksomheden har outsourcet driften heraf til en ekstern outsourcing-leverandør, herunder teleudbydere. Heller ikke outsourcing-leverandøren kan således anses for udbyder af elektroniske kommunikationsnet eller -tjenester.

Outsourcing-leverandører kan antage flere former, afhængigt af deres forretningsmodel, og kan således omfatte virksomheder, der udover den interne teleinfrastruktur og de basale interne tjenester overvåger, driver og vedligeholder virksomhedens øvrige centrale IT-systemer og applikationer, virksomhedens hjemmesider, herunder hjemmesider til internethandel, email-adresser og -applikationer m.v. Det outsourcete udstyr og de outsourcete funktioner kan fysisk enten være placeret hos virksomheden (kunden) selv eller hos leverandøren. Uanset hvor udstyret er placeret, vil der i den samlede installation nødvendigvis indgå en eller flere dedikerede forbindelser (typisk faste kredsløb), med henblik på at sikre outsourcing-leverandøren, henholdsvis virksomheden, adgang til det omhandlede interne net med tilhørende interne tjenester.

For så vidt angår de ovenfor beskrevne interne net, vil politiet via oplysninger fra udbydernes net og tjenester således kunne komme frem til det punkt, hvor det private net herunder det interne net er forbundet med et offentligt net, der formidler virksomhedens kommunikation med omverdenen. Derfra er det politiets opgave at komme videre indenfor det interne net. Det skal bemærkes, at kommunikation i interne net kun er undtaget, så længe der alene er tale om intern kommunikation modsat den situation, at kommunikationen går ud af det interne net til det offentlige net

Arbejdsgruppen er af den opfattelse, at den udbyder, som det interne net anvender til kommunikation med omverdenen, imidlertid er forpligtet til f.eks. at

stille oplysninger om, hvem et givent nummer, IP-adresse eller lignende er tildelt, til rådighed for politiet. Branchen anfører, at for elektronisk post og internet kan en virksomhed kommunikere med omverdenen uden at benytte en udbyder af de pågældende tjenester.

Udover ovennævnte afgrænsning af udbyder-begrebet er det – af hensyn til at undgå usikkerhed- relevant at slå fast, at heller ikke virksomheder, der via internettet udbyder den stadigt voksende liste af web-baserede applikationer, som eksempelvis computerspils-applikationer, søgetjenester, email-tjenester af samme type som f.eks. ”hotmail”, videokonference-applikationer, meddelelsetjenester som f.eks. MS Messenger og LotusSameTime, download af software og lign., IP-telefoni applikationer der ikke omfatter udveksling af trafik med den offentlige nummerplan og de traditionelle taletefonitjenester (PSTN), kan anses for udbydere af elektroniske kommunikationsnet eller -tjenester.

For de ovenfor nævnte afgrænsninger af udbyder-begrebet gælder i sagens natur, at virksomheder, der både leverer denne type ydelser (outsourcing og/eller webbaseret udbud af applikationer), og tillige er udbydere af elektroniske kommunikationsnet eller -tjenester i telelovgivningens forstand, for så vidt angår den sidstnævnte del af deres virksomhed vil være omfattet af udbyder-begrebet.

3.6. Undtagelser til anvendelsesområdet

Det fremgår af rapporten ”Det danske samfunds indsats og beredskab mod terror”, at: ”Da behovet for at kunne foretage indgreb primært retter sig mod de større udbydere, og da omkostningerne ved at ændre de tekniske systemer vil kunne virke meget byrdefulde for især mindre udbydere, bør det efter arbejdsgruppens opfattelse – med henblik på at sikre et bredt konkurrence- og innovationspræget telemarked – overvejes at undtage de helt små udbydere, herunder f.eks. andelsbolig- og antenneforeninger.”

Fremadrettede oplysninger

For så vidt angår de fremadrettede oplysninger vil det efter arbejdsgruppens vurdering være hensigtsmæssigt at skabe en bemyndigelse til at fastsætte regler, hvorefter de krav, der stilles til indretningen af udstyr og systemer, kan fraviges i særlige tilfælde, hvor tekniske eller praktiske hensyn nødvendiggør dette.

Det fremgår af bemærkningerne til lov om konkurrence og forbrugerforhold på telemarkedet, at den nuværende bemyndigelsesbestemmelse i lovens § 15, stk. 4, bl.a. er nødvendiggjort af, at pligten i § 15 til at indrette udstyr og systemer er rettet mod alle udbydere af elektroniske kommunikationsnet og -tjenester.

Det fremgår desuden af bemærkningerne, at bemyndigelsen bl.a. vil ”kunne anvendes til at fastsætte regler, hvorefter visse udbydere af telenet eller teletjenester, der ikke er offentlige, fritages for de nævnte krav til indretning af centraler. Anvendelsesområdet for sådanne regler vil som udgangspunkt være mindre udbydere af ikke offentlige telenet, herunder eksempelvis boligforeninger og virksomheder, hvor en opfyldelse af de stillede krav vil virke uforholdsmæssigt byrdefuldt.”

I sådanne tilfælde vil trafikken ofte gå til/fra én bestemt udbyder af offentlige elektroniske kommunikationsnet, i hvis net, der vil være mulighed for at foretage indgreb i meddelelshemmeligheden.

På trods af at den kommende bestemmelse i § 15 bliver begrænset til at gælde for udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, vil der stadig være behov for en bemyndigelsesbestemmelse til fravigelse af forpligtelsen til at indrette udstyr og systemer.

På grund af den udvidede bestemmelse i § 15 til at omfatte indretningen af andet udstyr og systemer end centraler, vil bemyndigelsesbestemmelsen fremover også kunne anvendes til at fravige forpligtelsen for visse offentlige elektroniske kommunikationsnet eller -tjenester, hvor det ikke teknisk giver mening eller er uforholdsmæssigt byrdefuldt for mindre udbydere at pålægge en forpligtelse til at kunne foretage en bestemt type indgreb i meddelelshemmeligheden.

Arbejdsgruppen har i den forbindelse drøftet for hvilke udbydere/tjenester, en fritagelse fra forpligtelsen til indretning af udstyr og systemer vil kunne være relevant. Det er blevet påpeget, at det i flere tilfælde ikke giver mening at lade pligten være gældende. Telebranchen har nævnt et eksempel såsom radiobaserede systemer og andre systemer med mulighed for direkte kommunikation mellem terminaler, f.eks. TETRA. Telebranchen har desuden nævnt muligheden for at kunne fritage broadcasting-tjenester fra forpligtelsen.

Det kan bemærkes, at den svenske udredning på området indgående behandler muligheden for, at visse udbydere kan undtages fra forpligtelsen til at indrette nettet, således at indgreb i meddelelshemmeligheden gøres muligt.

Det konkluderes i udredningen, at undtagelser bør kunne tildeles visse små udbydere. Der lægges i den svenske udredning vægt på, at reguleringen skal være tydelig, hvorfor undtagelse kun kan tildeles i særlige tilfælde. Da det er politiet, der i bund og grund ved, hvilke oplysninger de har behov for eller ej, anfører udredningen, at beslutning om undtagelse bør træffes af politiet.

Historiske oplysninger

Den nærmere afgrænsning af anvendelsesområdet i forhold til historiske (bagudrettede) oplysninger vil blive fastsat i forbindelse med udstedelsen af den såkaldte "logningsbekendtgørelse". Der er i forbindelse med udarbejdelsen af denne bekendtgørelse nedsat en arbejdsgruppe under Justitsministeriet med repræsentanter fra IT- og telebranchen og boligforeninger og -selskaber. Arbejdet forventes tilendebragt i løbet af sommeren 2006.

Logningsbekendtgørelsen udstedes med hjemmel i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence og forbrugerforhold på telemarkedet m.v. blev der bl.a. indsat nye bestemmelser i retsplejelovens § 786 om registrering og opbevaring af oplysninger om teletrafik og om telenet- og teletjenesteudbyderes praktiske bistand til politiet.

Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af elektroniske kommunikationsnet eller -tjenester at foretage registrering og opbevaring i 1 år af

oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justitsministeren fastsætter i henhold til bestemmelsen efter forhandling med ministeren for videnskab, teknologi og udvikling nærmere regler om denne registrering og opbevaring.

Det fremgår af forarbejderne til anti-terror lovforslaget, at det i forbindelse med indførelsen af bestemmelsen i retsplejelovens § 786, stk. 4, var forudsat, at ikke enhver udbyder skulle omfattes af logningspligten.

I besvarelsen af spørgsmål nr. 63 fra Folketingets Retsudvalg (L 35 – bilag 43) anførte Justitsministeriet således bl.a., at det ikke vil være hensigtsmæssigt, at enhver udbyder af elektroniske kommunikationsnet og -tjenester omfattes af den foreslåede regulering, og at der i forbindelse med den nærmere regelfastsættelse efter den bestemmelse i § 786, stk. 4, derfor vil skulle foretages en hensigtsmæssig afgrænsning af den omfattede personkreds gennem eksempelvis en ”bagatelgrænse”, hvorefter mindre udbydere ikke generelt skal logge trafikdata i 1 år.

Justitsministeriet uddybte spørgsmålet om en bagatelgrænse i besvarelsen spørgsmål nr. 127 (L 35 – bilag 100), hvoraf det bl.a. fremgår, at den fastsættelse af bagatelgrænsen vil afhænge af den nærmere tekniske udmøntning af logningsforpligtelsen, men at det efter Justitsministeriets foreløbige vurdering må antages, at bagatelgrænsen vil komme til at ligge nærmere omkring 100 tilsluttede brugere end omkring de 1.000.

Det fremgår endvidere af forarbejderne, at logningspligten som udgangspunkt ikke vil skulle omfatte arbejdspladser og offentlige institutioner, f.eks. biblioteker og uddannelsesinstitutioner, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter i form af lånere, studerende, patienter o.lign.

Det fremgår endelig af forarbejderne, at det kan overvejes at undtage særlige typer af tjenester fra logningspligten. Blandt de tjenester, der kan indgå i disse overvejelser, er ældre tjenester så som teksttefontjenesten til handicappede, hvor den tekniske indretning ikke muliggør en egentlig logning.

Tjenester med lokale og isolerede infrastrukturnet så som FWA-net eller WLAN-net, der kræver, at der etableres en tilslutning til andre elektroniske kommunikationsnet, før der kan tilbydes egentlige tjenester til slutbrugerne, kan også tænkes undtaget fra logningspligten. Tilsvarende gælder for lukkede landmobile radionet, der benyttes af eksempelvis politiet, beredskabstjenester, vognmænd og taxifirmaer, og datanet der udelukkende benyttes til opsamling og videreendelse af data fra person til maskine eller fra maskine til maskine. Det sker eksempelvis ved overvågning og styring af processer i produktionsanlæg.

3.7. Bemærkninger vedrørende økonomi

Arbejdsgruppen har drøftet det økonomiske aspekt i forhold til indretning af systemer og driften heraf. Det er således både blevet drøftet, hvor store omkostningerne til indretning af systemerne vil være og desuden, hvem omkostningerne skal pålægges, herunder sondringen mellem, hvad der kan

forstås ved deciderede ”politiopgaver”, og hvad der kan forstås som opgaver indenfor telebranchens sædvanlige driftsområde.

Der henvises til bemærkningerne i forbindelse med gennemgangen af de enkelte anbefalinger nedenfor.

Telekommunikationsindustrien i Danmark (TI) har udarbejdet et skøn over omkostningerne for den samlede branche, jf. vedlagte bilag 6.3, hvor de nærmere forudsætninger for skønnene er beskrevet. Størrelsen af investeringerne vil typisk afhænge af, hvor meget de eksisterende net og systemer skal ændres. Omkostningerne kan således fordele sig meget forskelligt fra udbydere til udbydere.

Omkostningerne til udvidelse af kravene til aflytning skønnes at udgøre i størrelsesordenen 50-100 mio.kr. Gennemførelse af krav om logning, ikke mindst af internettrafik, skønnes væsentligt mere omkostningstung. En gennemførelse af det kommende EU-direktivs krav skønnes at koste i størrelsesordenen 100-500 mio.kr., mens omkostningerne til en gennemførelse af de krav, der ligger i et udkast til logningsbekendtgørelse, der blev forelagt Justitsministeriets ekspertgruppe i februar 2005, skønnes at udgøres 1-2 mia.kr.

TI finder, at merudgifter, der pålægges udbydere til formål, der udelukkende tilgodeser politiets ønsker, ikke skal dækkes af udbydere og deres kunder. Det gælder især på områder, hvor politiets ønsker er mere vidtgående end etableret international norm. Der kan henvises til kompensationsmuligheder i eksempelvis USA og UK.

TI anfører endvidere, at uden kompensation vil konkurrenceforholdet til tjenester udbudt fra udlandet forvrides. Teletjenesterne konkurrerer også med interne landsdækkende virksomhedsnet og applikationer som eksempelvis IP-telefoni uden for reglernes rækkevidde. Også dette konkurrenceforhold vil blive forvredet uden en kompensationsmekanisme. Endelig vil mindre undtagne udbydere få komparative fordele i det omfang der defineres sådanne undtagelser som foreslået i forbindelse med foreliggende udkast til logningsbekendtgørelse. Uden kompensation kan brugen af metoder og ydelser, hvor hjælp til politiet ikke kan stilles til rådighed, dermed blive mere udbredt. TI henviser til vedlagte skøn over omkostninger forbundet med de udvidede krav til aflytning og logning.

Det er desuden TI's vurdering, at vidtgående særlige danske krav uden kompensation på såvel kort som lang sigt vil øge omkostninger og begrænse systemvalg i den danske telesektor. Dermed er det ikke foreneligt med den gældende målsætning om ”bedst og billigst”.

3.8. Ikrafttræden

Anbefalingerne 15, 17 og 18 kan implementeres i § 15 i lov om konkurrence- og forbrugerforhold på telemarkedet. Der må dog gælde forskellige ikrafttrædelsesbestemmelser for de dele af den nye bestemmelse, der vedrører henholdsvis bagudrettede indgreb (i forhold til historiske tele- og masteoplysninger) og fremadrettede indgreb (aflytning hhv. fremadrettede tele- og masteoplysninger).

Dette skyldes blandt andet, at ikrafttrædelse af bestemmelsen, for så vidt angår de bagudrettede teleoplysninger og udvidet teleoplysninger (masteoplysninger), hænger nøje sammen med ikrafttrædelse af logningsbekendtgørelsen, jf. afsnit 3.6 ovenfor.

Det er nødvendigt at sikre sammenhæng til ikrafttrædelse af logningsbekendtgørelsen således, at udbydere ikke forpligtes til at indrette deres systemer med henblik på logning, før omfanget af forpligtelserne i logningsbekendtgørelsen kendes og er trådt i kraft.

Dette foreslås gjort ved at lade bestemmelsen træde i kraft ved udstedelse af en bekendtgørelse, der ”times” i forhold til udstedelse af logningsbekendtgørelsen, for så vidt angår de bagudrettede teleoplysninger og udvidede teleoplysninger (masteoplysninger). Det skal i den forbindelse bemærkes, at der, på grund af manglende tekniske systemer, kan være leveringstider på over 1 år for nogle af de systemer, der vil være behov for at anskaffe.

For så vidt angår de fremadrettede indgreb i meddelelshemmeligheden, foreslås det at lade bestemmelsen træde i kraft med et varsel på 12-18 måneder for udstyr, der etableres efter lovens ikrafttræden og med et varsel på 18-24 måneder for udstyr, der er idriftsat efter hidtil gældende regler. Dermed gives der mulighed for, at ændringerne kan gennemføres i sammenhæng med løbende større opgraderinger på en smidig måde. Også for de systemer, der vil være behov for at anskaffe til understøttelse af kravet om fremadrettede oplysninger, kan der være leveringstider på over 1 år

4 Gennemgang af anbefalingerne

4.1 Anbefaling 15

Af anbefaling 15 i Regeringens handlingsplan for terrorbekæmpelse fremgår, at:

15. Arbejdsgruppen anbefaler, at § 15 i lov om konkurrence- og forbrugerforhold på telemarkedet ændres, så udbydere af elektroniske kommunikationsnet og -tjenester får pligt til at indrette deres tekniske udstyr på en måde, der gør indgreb i meddelelshemmeligheden muligt uanset teknologisk fremføringsform.

Det er i rapporten ”Det danske samfunds indsats og beredskab mod terror” anført, at: ”Formålet med reglerne i § 15 er at fastslå en pligt for udbydere af elektroniske kommunikationsnet og -tjenester til at sikre, at politiet kan få adgang til at foretage indgreb i meddelelshemmeligheden på de pågældende udbyderes centraler. Udbydere af elektroniske kommunikationsnet og -tjenester har således pligt til at indrette centraler, så det er teknisk muligt at foretage indgreb i meddelelshemmeligheden, og til ved anskaffelse af centraludstyr at sikre, at dette er indrettet således, at aflytning er mulig.

Store dele af nutidens elektroniske kommunikation transporteres ikke via centralbaserede netværk, men via pakkebaseret kommunikation, som er en særlig teknologisk fremføringsform af informationen. Således anvendes der pakkebaseret kommunikation i forbindelse med mobiltelefoni, voice-over IP,

internet- og andre former for datakommunikation mv.

Det må antages, at pligten for udbydere af elektroniske kommunikationsnet og -tjenester efter ordlyden af telekonkurrenceovens § 15 ikke omfatter pakkebaserede netværk. Der gælder derfor ikke en pligt for de omfattede udbydere til at sikre (uden udgift for staten, herunder politiet), at det tekniske udstyr er indrettet således, at det er teknisk muligt at foretage indgreb i meddelelseshemmeligheden i relation til pakkebaseret kommunikation.”

4.1.1. Formål

I rapporten ”Det danske samfunds indsats og beredskab mod terror” er formålet med anbefalingen præciseret nærmere. I det indledende afsnit til kap. 4 om efterforskningsredskaber på teleområdet er anført, at: ”Arbejdsgruppen vil nedenfor komme med en række anbefalinger knyttet til efterforskningsredskaber på teleområdet. En række af disse anbefalinger er udtryk for, at der efter arbejdsgruppens opfattelse er behov for, at myndighedernes efterforskningsredskaber tilpasses den teknologiske udvikling. Der er således efter arbejdsgruppens opfattelse ikke principiel forskel på aflytning af nye kommunikationsformer via internettet og en almindelig fastnettelefon, og det bør derfor sikres, at myndighedernes mulighed for aflytning er til stede.”

På grund af det forhold, at den nuværende § 15 i teleloven kun vedrører indretning af centraler (til aflytning), har bestemmelsen hidtil alene omfattet aflytning (herunder samtidig fremadrettede teleoplysninger), jf. de hidtidige lovforslagsbemærkninger til bestemmelsen og ikke etablering af it- og efterbehandlingsudstyr (til logning af tele- og udvidet teleoplysninger).

Hensigten med anbefalingen er fremover at sikre, at udbydere af elektroniske kommunikationsnet og -tjenester, forpligtes til at indrette deres systemer således, at et indgreb i meddelelseshemmeligheden er muligt. Dette skal være muligt uanset den teknologi, der anvendes til fremføring af kommunikationen.

Formålet er desuden at sikre, at udbydere skal kunne give politiet adgang til aflytning, teleoplysninger og udvidet teleoplysninger vedrørende en kommunikation til/fra en bestemt kunde eller et bestemt fælles radiobaseret accesspunkt uafhængig af den teknologi, der anvendes til fremføring af kommunikationen.

Umiddelbart kan anbefalingen gennemføres ved at udvide det eksisterende krav til at indrette centraler, således at det bliver teknologineutralt og dermed uafhængigt af, om trafikken passerer centraler eller andet teknisk udstyr.

4.1.2. Hvem er forpligtet

For en gennemgang af hvem, der er forpligtet af bestemmelsen henvises til det tidligere afsnit om pligtsubjektet.

4.1.3. Udstyr og systemer

Det følger af handlingsplanen, at det hidtidige anvendelsesområde for § 15 udvides. Det nuværende indhold videreføres således, at udbydere af elektroniske kommunikationsnet og -tjenester stadig med den nye bestemmelse har pligt til at

indrette centraler, så det er teknisk muligt at foretage indgreb i meddelelseshemmeligheden, og til ved anskaffelse af centraludstyr at sikre, at dette er indrettet således, at indgreb i meddelelseshemmeligheden er mulig.

Som det fremgår af rapporten ”Det danske samfunds indsats og beredskab mod terror” transporteres store dele af nutidens elektroniske kommunikation ikke via centralbaserede netværk som traditionel telefoni, men via andre teknologiske løsninger som f.eks. via IP-servere over internettet.

På denne baggrund udvides bestemmelsen til også at omfatte andet teknisk udstyr og andre tekniske systemer end centraler og andre teknologiske fremføringstyper, der måtte opstå fremover. Konkret vil udvidelsen bl.a. indebære, at udbydere af IP-baserede taletelefonitjenester samt udbydere af datatransmission, som ikke benytter centraludstyr i traditionel forstand, vil blive omfattet af forpligtelsen. Forpligtelsen gælder dog ikke taleapplikationer over internettet, med mindre disse tilbyder opkald til og fra taletelefonitjenester, hvorved de pågældende applikationer reelt bliver taletelefonitjenester.

Med teknisk udstyr og tekniske systemer skal forstås det udstyr, der er nødvendigt for at foretage indgreb i meddelelseshemmeligheden. Præcis hvilket udstyr, der vil være relevant at indrette, så et indgreb er muligt, vil variere en del mellem net og teknologier. Mens gældende pligter efter § 15 alene vedrører indretning af udstyr med trafikafvikling (centraler) vil specielt pligt til logning stille krav til de af teleudbydere anvendte administrative systemer og systemer til opbevaring af data.

Faciliteterne i udstyret og systemerne til indgreb i meddelelseshemmeligheden bør, så vidt det er muligt, være baseret på fælleseuropæiske standarder. Sådanne standarder foreligger imidlertid indtil videre kun for aflytning af telefoni og data i et vist omfang, mens standardisering af overdragelse af historiske data endnu ikke er påbegyndt. Selvom systemerne er indrettet i overensstemmelse med omtalte standarder på området, er systemerne ofte meget komplekse og delvist proporetære, hvilket gør, at systemerne er forskelligt implementeret afhængigt af leverandøren.

Dette emne behandles også i den svenske udredning, der konstaterer, at det ikke vil være muligt at stille krav om ensartet udstyr, da nettene ofte vil være implementeret på forskellig vis.

4.1.4. Indgreb i meddelelseshemmeligheden

Den nuværende § 15 indeholder en forpligtelse for udbydere til at indrette centraler, så det er muligt at foretage indgreb i meddelelseshemmeligheden. På grund af, at forpligtelsen har været begrænset til at omfatte indretningen af centraler har den praktiske udmøntning af § 15 hidtil været, at sikre politiet mulighed for at kunne foretage aflytning og få udleveret fremadrettede teleoplysninger.

Med den udvidelse af bestemmelsen, der nu lægges op til, vil alle indgreb i meddelelseshemmeligheden imidlertid være relevante. Fremover stilles derfor krav om, at udstyr og systemer indrettes således, at indgreb i

meddelelshemmeligheden bliver mulige både fremadrettet (real tid) og bagudrettet (historisk).

Ved indgreb i meddelelshemmeligheden forstås de typer af indgreb i meddelelshemmeligheden, som findes i retsplejelovens § 780 vedrørende teleområdet. Disse typer indgreb er: Telefonaflytning, teleoplysning (f.eks. hvilke telefonnumre der har været sat i forbindelse med et bestemt telefonnummer), udvidet teleoplysning (f.eks. masteoplysninger).

Begreberne teleoplysning og udvidet teleoplysning er ikke nærmere beskrevet i selve Retsplejeloven, men for den nærmere fortolkning af begreberne henvises til bemærkningerne til Retsplejeloven. Der henvises i øvrigt til bilaget om definitioner.

Det fremgår af rapporten: ”Det danske samfunds indsats og beredskab mod terror”, at: ”Tilladelse til at indhente teleoplysninger kan ske såvel fremadrettet som bagudrettet (historiske teleoplysninger).”

Videre fremgår af rapporten: ”Retsplejelovens § 780, stk. 1, nr. 3 og 4, giver alene politiet adgang til at indhente oplysninger vedrørende trafikdata i forbindelse med telekommunikation og omfatter således ikke selve indholdet af kommunikationen.”

4.1.5. Bruttodatastrøm og taletelefoni

Den information, der kan tilvejebringes ved et indgreb i meddelelshemmeligheden, vil afhænge af tjenesten. Hvis der er tale om traditionel taletelefoni, SMS og kredsløbskoblet datatransmission, vil både teleoplysninger, udvidet teleoplysninger og for så vidt angår fremadrettede oplysninger selve indholdet af kommunikationen umiddelbart være tilgængeligt i de for disse tjenester standardiserede formater. I forbindelse med andre typer datatransmission, vil indholdet af kommunikationen og teleoplysninger knyttet til kommunikationen skulle udtages af bruttodatastrømmen. For så vidt angår kravene til at udtage fremadrettede data henvises til afsnittet om anbefaling 17.

Det følger af nævnte principper, at hvis en taletelefonitjeneste benytter en transmissionstjeneste, som udbydes af samme udbyder, er det muligt for udbyderen at stille oplysninger til rådighed fra både taletelefonitjenesten og transmissionstjenesten i samme omfang som et tilsvarende tilfælde, hvor de pågældende udbydere ikke er sammenfaldende.

Hvis en VoIP-tjeneste (en applikation) udbydes af en anden end selve transmissionstjenesten, kan udbyderen af transmissionstjenesten kun stille oplysninger til rådighed fra transmissionstjenesten. Dette er f.eks. gældende med en applikation som SKYPE, når opkaldsmulighed til almindelige telefonnumre ikke indgår. Det er således ikke muligt for udbyderen at dekryptere data for så vidt angår en sådan VoIP-tjeneste. Udbyderen af transmissionstjenesten kan i denne situation således ikke forpligtes til at stille oplysninger til rådighed fra selve VoIP-tjenesten, herunder indholdet heraf. Se også om kryptering under afsnittet om anbefaling 17.

4.1.6. Sammenhæng til andre bestemmelser

I forbindelse med udmøntningen af anbefalingerne 17 og 18 er kravene til de fremadrettede og historiske oplysninger, der skal stilles til rådighed nærmere fastlagt.

4.1.7. Problemer

Der er ikke identificeret problemer i forbindelse med indretning af udstyr og tekniske systemer til aflytning og monitorering. Alle udbud på markedet har ikke været analyseret, men de mest udbredte og væsentlige tjenester har været analyseret af arbejdsgruppen. Problemstillingerne relaterer sig også til, om oplysninger kan stilles til rådighed i realtid, hvor hurtigt historiske oplysninger kan stilles til rådighed, og hvorvidt det er muligt at analysere en bruttodatastrøm og tage relevante IP-trafikdata ud for enkeltkunder i alle tilfælde. Disse problemstillinger er behandlet under anbefalingerne 17 og 18.

4.1.8. Økonomi

Der henvises til vedlagte bilag, hvor TI på det foreliggende grundlag har angivet skøn for involverede omkostninger. Som det fremgår heraf, er det især de fremtidige logningskrav, der kan involvere store omkostninger, og skønnet for disse omkostninger varierer en faktor 20 afhængigt af den endelige udformning af kravene. Omkostninger til aflytning af bruttodatastrømme har været baseret på, at de i disse strømme indeholdte data om kundernes anvendelse af tjenesterne ikke udtrages. Dette er i overensstemmelse med gældende internationale principper og fælleseuropæiske standarder for ydelser til LEA (Law Enforcement Agencies).

4.2 Anbefaling 17

Af anbefaling 17 i Regeringens handlingsplan for terrorbekæmpelse fremgår, at:

17. Arbejdsgruppen anbefaler, at der i telelovgivningen fastsættes krav om, at politiet hos alle teleudbydere skal have mulighed for at indhente fremadrettede tele- og masteoplysninger, samtidig med at disse registreres, hvilket vil sige samtidig med, at en person foretager et opkald, aktiverer en sendemast og lignende. Forpligtelsen bør kunne opfyldes ved out-sourcing.

Af ”Regeringens handlingsplan for terrorbekæmpelse” fremgår det, at regeringen vil arbejde videre med denne anbefaling og har til hensigt – efter den fornødne tekniske konkretisering og afklaring – at fremsætte lovforslag herom.

Den nærmere fremgangsmåde vil skulle koordineres med de igangværende forhandlinger om EU-regulering om logningspligt for teleudbydere. Lovforslaget forventes at indgå i regeringens antiterrorlovpakke, der fremsættes i foråret 2006. Lovændringen vil have til formål at tilvejebringe hjemmel til at fastsætte nærmere regler ved bekendtgørelse.

4.2.1. Formål

Det følger af den tværministerielle embedsmandsgruppes rapport, at ”politiet, herunder Politiets Efterretningstjeneste, i såvel overvågnings- som

efterforskningsmæssig henseende har et udpræget behov for at kunne indhente teleoplysninger og udvidede teleoplysninger. I en række tilfælde vil det således være af afgørende betydning for muligheden for at efterforske og retsforfølge strafbare forhold, at der indhentes oplysning om, hvordan, hvornår og med hvem en person kommunikerer/har kommunikeret. Det er endvidere væsentligt at få disse oplysninger så hurtigt som muligt.”

Formålet er således at give politiet mulighed for ved hjælp af en kendelse, at overvåge et bestemt geografisk område eller en bestemt person, fra et bestemt tidspunkt og fremadrettet.

Fremadrettet skal således i denne sammenhæng forstås som 'fra det tidspunkt der fastslås i en retskendelse og fremad'. Udbydere vil kunne opfylde politiets behov med friske historiske data om hvem, der har været på en bestemt mast eller et andet radiobaseret fælles accesspunkt for mobile eller nomadiske tjenester på et givent tidspunkt. Målsætningen må dog være at tilnærme sig en leveringstid på højst 1 time.

4.2.2. Hvem forpligtes

Forpligtelsen påhviler de i § 15, stk. 1, nr. 1, nævnte udbydere.

4.2.3. Omfanget af bestemmelsen – hvad er omfattet

Det fremgår af den tværministerielle embedsmandsgruppes rapport, at ”i takt med at der opstår flere og flere udbydere af elektroniske kommunikationsnet og -tjenester, og at der er udsigt til, at flere udbydere i fremtiden vil være i stand til at etablere eget net, er der efter arbejdsgruppens opfattelse behov for via regulering i telekonkurrenceloven at sikre, at der skabes adgang for politiet til hos samtlige udbydere at kunne indhente fremadrettede teleoplysninger og udvidede teleoplysninger, samtidig med at disse registreres, hvilket vil sige samtidig med at en person foretager et opkald, aktiverer en sendemast o.lign. Det bør i den forbindelse som udgangspunkt være tilstrækkeligt, at den enkelte udbyder ved out-sourcing af forpligtelsen sikrer, at politiet kan få adgang on-line i relation til fremadrettede oplysninger, evt. hos den netværksudbyder, hvis netværk den pågældende udbyder benytter.”

Ifølge rapporten omfatter forpligtelsen således en mulig adgang til fremadrettede teleoplysninger og udvidede teleoplysninger samtidig med, at disse registreres, hvilket vil sige samtidig med at en person foretager et opkald, aktiverer en sendemast o.lign.

Dette har været drøftet i arbejdsgruppen, og branchen har oplyst, at en person ikke kan ”aktivere en sendemast”, idet der alene sker en aktivering ved skift fra et trafikområde til et andet. Branchen har oplyst, at det vil være muligt for en udbyder at registrere i de tekniske systemer, at en udpeget mobilterminal foretager et opkald eller sender en sms.

Det vil også teknisk være muligt for en udbyder at registrere i de tekniske systemer, at en mobiltelefon tændes eller slukkes, forudsat at telefonen er indenfor dækningsområde og befinder sig i eget net. Eksisterende systemer understøtter imidlertid ikke i almindelighed mulighed for videregivelse af disse

oplysninger til politiet og de konkrete muligheder herfor har ikke kunnet analyseres nærmere inden for den tid, der har været til rådighed.

Teknisk vil det også være muligt at sikre, at en tændt telefon, som ikke er aktivt kommunikerende, som ovenfor beskrevet, kan aktiveres udefra, således at dens aktivitet kan registreres. Denne situation er imidlertid omfattet af anbefaling 30, som først vil skulle implementeres via lovgivning i efteråret 2006.

Formålet med anbefalingen er ikke, at udbyder skal kunne dekryptere data. Det vil være politiets opgave at dekryptere data. Udbyder skal imidlertid forpligtes til at udtage trafikdata, som er omfattet af kendelsen.

Hvis der således er tale om en kendelse til indhente teleoplysninger og udvidede teleoplysninger, er udbyderen forpligtet til at videregive de relevante oplysninger i læsbar form fra bruttodatastrømmen. Der vil her typisk være tale om IP- eller MAC-adresser i de dataenheder, som udveksles via udbyderens netværkstjeneste (lag 3 netværksinformation).

Der findes i dag tilgængeligt udstyr, der tillader dybere analyse af en IP-baseret datastrøm alene baseret på header-information. Systemerne giver ikke brugere, administratorer eller andre adgang til selve dataindholdet². Hvis der er tale om en kendelse til aflytning, er det udbyders pligt at udtage den del af bruttodatastrømmen, der relaterer sig til det aflyttede objekts IP-adresse, MAC-adresse eller lignende.

I forbindelse med en kendelse om aflytning kan teleudbydere videregive hele bruttodatastrømmen f.eks. knyttet til en given kunde eller et givent punkt. Hvis en kendelse derimod alene omfatter adgang til teleoplysninger eller udvidede teleoplysninger, kan anbefalingen indebære, at udbyderen af elektroniske kommunikationsnet eller -tjenester må udtage de relevante teleoplysninger fra bruttodatastrømmen. Det vil sige, at hver udbyder må sikre muligheden for at udtage disse data, selv om det ud fra en teknisk synsvinkel udmærket kunne ske centralt hos modtageren. Forskellen mellem de to alternativer er dels en mangedobling af investeringsomkostningerne, såfremt hver enkelt udbyder skal etablere udstyr og software til at foretage en sådan efterbehandling af de aflyttede data, dels en forskel i den spredning af den fortrolige databehandling, som vil være konsekvensen af, at den sker flere steder decentralt, henholdsvis centralt ét sted.

Branchen har tilkendegivet, at man både ud fra økonomiske, juridiske og tekniske forhold finder det betænkeligt at udtage teleoplysninger, der ikke er trafikdata for egne tjenester, og at yderligere undersøgelser derfor vil være nødvendige.

De videregivne data, som ikke er trafikdata, i forbindelse med en aflytning kan være krypterede. I relation til en kendelse om aflytning er det udbyders pligt at påse, at der kan stilles relevante data til rådighed for politiet. Det er politiets

² Gartner har oplyst, at det er muligt med standardudstyr at udtage data, således at det alene er data vedrørende en bestemt IP-adresse, MAC-adresse, punkt eller lignende, der stilles til rådighed for politiet i henhold til retskendelsen.

opgave at fortolke de leverede data som beskrevet oven for. Data relateret til en bestemt IP-adresse, MAC-adresse, punkt eller lignende kan ved hjælp af standardudstyr af udbyderen udtages ud af en datastrøm.

Anbefalingen kan efter arbejdsgruppens vurdering gennemføres ved, at der indføres en pligt for udbydere til at indrette deres systemer og tekniske udstyr sådan, at teleoplysninger og udvidede teleoplysninger kan opsamles og videregives efter kendelse herom – fortrinsvis via de mekanismer og grænseflader, der også stilles til rådighed ved aflytning.

4.2.4. ”Samtidig”

En forpligtelse for udbydere til at sikre, at politiet får mulighed for at indhente fremadrettede teleoplysninger og udvidede teleoplysninger, samtidig med at disse registreres, giver ikke problemer for så vidt angår fastnet, hvor denne mulighed for at indhente data i forvejen eksisterer.

Imidlertid mener branchen, at det kan være vanskeligt at gøre det muligt for politiet i alle tilfælde at indhente oplysningerne samtidig med den tekniske registrering af disse i udbyderens udstyr, idet det i praksis vil tage lidt tid, før en registrering som følge af en konkret kendelse er indsamlet og kan ’leveres’ til politiet. Da oplysningerne i mange tilfælde kun kan stilles til rådighed via en aflytning, er de af politiet modtagne oplysninger reelt ikke et udtræk af de oplysninger, som ligeledes registreres med henblik på opbevaring af historiske data. Det er arbejdsgruppens vurdering, at der ved ’samtidig’ ikke skal opfattes en overførsel af oplysninger i realtid, da dette ikke vil være teknisk muligt. Oplysninger skal overføres så hurtigt som det kan kræves af et standardsystem med de almindeligt anvendte service levels, og sådan at formålet med indgrebet ikke forspildes.

For mobilkommunikation vil det f.eks. ikke være muligt at levere udvidede teleoplysninger ”online”. Der findes ikke en teknisk løsning til i realtid at kunne se, hvilken abonnent der er på en bestemt mast. Dette skyldes, at oplysningerne, som genereres, opsamles i såvel kaldende som kaldte kundes centraler, hvor disse oplysninger ikke er organiseret efter celleoplysninger. Først herefter kan man med analyseværktøjer udtage de ønskede oplysninger. Fremadrettede masteoplysninger kan således ikke stilles til rådighed hurtigere end friske historiske masteoplysninger (jf. anbefaling 18)

4.2.5. Oplysninger fra hot spots, WLAN, mv.

Ved hot spots er det muligt at få oplysninger om, hvor hot spottet er placeret geografisk. Størrelsen på området afhænger af dækningsområdets størrelse.

Endvidere har branchen fremhævet, at der er en del tekniske problemer i relation til, at aflytte den/de relevante abonnent(er) alene i forbindelse med hot spots, WLAN mv., idet der kan være tale om en datastrøm, som vedrører en række personer på det pågældende sted (internetcafé, hot spot mv.) I sådanne tilfælde følger det imidlertid allerede af anbefaling 15, at den enkelte kundes trafik og de til tjenesten hørende trafikdata skal kunne udtrages.

Det forudsættes, at enten bruger-ID eller oplysningerne vedr. det

forudbetalte kort er kendt.

I modsætning til egentlige mobiltjenester er der ved brug af hot spots ikke hos udbyderen data om tilknytning til systemet for en terminal, der ikke er logget på. Brug af hot spots minder således om adgang til internet via PSTN/ISDN. Kun mens kunden er aktivt logget på, kan adfærden følges. Det har alene været muligt inden for den tid, der har været til rådighed, at undersøge en enkelt udbyders system. Denne undersøgelse indikerer, at det skulle være muligt at følge en udpeget kundeidentitets opkoblinger til udbyderens hot spots.

Det er ligeledes vurderet, at opkoblinger på en given hot spot kan følges fremadrettet.

Da hot spot tjenester kan opbygges meget forskelligartet er dette ikke udtryk for, at der ikke kan være vanskeligheder i andre systemer, herunder systemer udbudt i Danmark som en del af et internationalt system.

4.2.6. Økonomi

Med udvidelsen af pligten til at foretage aflytning udvides adgang til fremadrettede data tilsvarende. Under forudsætning af, at de ønskede data opfanges af politiet efter hidtil gældende principper for telefoni, data og mail, og under forudsætning af respekt af begrænsninger ved særlige produktionsforhold, skønnes de selvstændige omkostninger til levering af fremadrettede data begrænsede.

4.3 Anbefaling 18

Af anbefaling 18 i ”Regeringens handlingsplan for terrorbekæmpelse” fremgår, at:

Arbejdsgruppen anbefaler, at der i telelovgivningen fastsættes krav om, at politiet hos alle teleudbydere skal have mulighed for at indhente historiske tele- og masteoplysninger. Der er behov for, at teleudbyderne forpligtes til at iværksætte sådanne indgreb straks og på en måde, så hensigten med indgrebet ikke forspildes.

Af handlingsplanen fremgår endvidere, at:

”Regeringen vil arbejde videre med at konkretisere denne anbefaling og har til hensigt at fremsætte lovforslag herom. Lovforslaget vil nærmere gå ud på at tilvejebringe hjemmel til at fastsætte nærmere bestemmelser. Bekendtgørelsen vil blive udstedt efter forhandling med telebranchen og i lyset af de igangværende forhandlinger om EU-regulering på området.

Videnskabsministeriet vil straks iværksætte et udredningsarbejde i samarbejde med branchen med henblik på afklaring af de tekniske og økonomiske konsekvenser. Formålet er i første omgang at nedbringe leveringstiden for de nævnte oplysninger og på længere sigt at kunne fremskaffe oplysningerne straks. Udredningsarbejdet vil søges afsluttet i foråret 2006”.

4.3.1. Formål

Der er ved indhentelse af historiske tele- og masteoplysninger tale om et indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71.

Som nævnt, jf. regeringens handlingsplan, er formålet med anbefalingen både, at teleudbyderne bistår politiet ved at iværksætte indhentelse af historiske tele- og masteoplysninger straks efter en konkret anmodning, og at oplysningerne udleveres til politiet så hurtigt som muligt indenfor en rimelig tidsfrist, således at hensigten med indgrebet ikke forspildes. Der er således ikke tale om, at en udbyder med det samme (straks) skal kunne levere data, men blot at udbyder straks skal gå i gang.

Målsætningen med bestemmelsen er at optimere leveringstiden på efterspurgte oplysninger, jf. nedenfor. Arbejdsgruppen er enig om, at det er vigtigt, at udbyderne, i forhold til en enkeltstående hændelse og i forhold til den store efterforskningsmæssige betydning, kan levere friske/nye data hurtigt.

4.3.2. Pligtsubjekt

Forpligtelsen påhviler udbydere af elektroniske kommunikationsnet- og tjenester. Det skal bemærkes, at den nærmere afgrænsning af forpligtede udbydere i relation til anbefaling 18 vil følge af den kommende logningsbekendtgørelse, jf. de tidligere bemærkninger om sammenhængen til logningsarbejdet i kap. 3.1.

I forhold til afgrænsning af udbyderbegrebet og endvidere, hvilke data, der skal udleveres, har der i arbejdsgruppen været enighed om, at bemærkningerne til lovbestemmelsen, der implementerer anbefaling 18, skal sikre, at bestemmelsens indhold afgrænses i forhold til retsplejeloven ved henvisning/delvis afskrivning af bemærkningerne til retsplejeloven (jf. terror-pakken fra 2002). For at undgå unødigt usikkerhed, skal slås fast i vejledningen til den kommende bekendtgørelsesregulering, at de indledningsvis omtalte outsourcingleverandører og applikationsleverandører ikke er omfattet af udbyderbegrebet.

4.3.3. Problemer og løsninger

Arbejdsgruppen noterer sig en mere generel problemstilling i forhold til, at anbefaling 18 alene kan betegnes som et proceskrav, mens substansen ligger i den kommende logningsbekendtgørelse. Det er således ikke muligt at skabe sig et fuldstændigt overblik over det nærmere omfang af de data, som teleudbyderne forpligtes til at udlevere forud for fremsættelsen af lovforslaget.

Arbejdsgruppen har endvidere noteret sig en konkret problemstilling i forhold til det tidsmæssige perspektiv for udlevering af data, jf. anbefalingens ordlyd ”på en måde, så hensigten ikke forspildes” sammenholdt med praksis for opdatering af systemerne.

Historiske data vil sige data frem til tidspunktet for henvendelsen. Det vil også sige data fra de sidste 24 timer. Teleudbyderne opdaterer typisk systemerne én gang i døgnet ved midnat. I forhold til de data, der er genereret siden midnat, og som altså er yngre end de data, der er omfattet af den sidste opdatering, vil der efter omstændighederne kunne laves specifikke indgreb og særkørsler, så politiet

kan få udvalgte oplysninger så hurtigt, at hensigten med indgrebet ikke forspildes.

Der kan for at opfylde forpligtelsen imidlertid også være behov for at optimere de nuværende generelle systemer eller opbygge parallel-systemer.

Det er vurderingen i arbejdsgruppen, at det generelt vil være teknisk muligt at fremskaffe disse oplysninger. Der er dog identificeret udstyr i mindre dele af fastnettet, hvor der endnu ikke er kendte løsninger til at skaffe oplysninger dagens trafik i løbet af tilstrækkelig kort tid. Det vil formentlig kræve nærmere dialog med udstyrsleverandøren at vurdere, om der kan findes en teknisk løsning.

Det skal bemærkes, at tidsrammen, jf. ”på en måde, så hensigten med indgrebet ikke forspildes”, må knytte sig til, hvad der er praktisk muligt i forhold til den teknologiske udvikling på et givet tidspunkt. Teknologien og de forskellige datatyper er i stadig udvikling, og der skal ved fortolkning af, hvor hurtigt teleudbyderne skal levere de efterspurgte oplysninger, ske en konkret graduering både i forhold til bestemte datatyper og bestemte teknologityper. Til eksemplificering kan nævnes, at der i dag er store variationer på leveringstider for fastnet og mobiltelefoni, der spænder fra 24 timer til 1 time. Målsætningen må dog være at tilnærme sig en leveringstid på højst 1 time.

Det skal endvidere bemærkes, at der i forhold til tidsrammen for udlevering af oplysninger til politiet må tages hensyn til, at de systemer, der genererer oplysningerne, ikke vil være søgbare hele tiden. Dette kan skyldes forhold som behovet for opdatering af databaser, opgradering af systemerne, vedligeholdelse el. lign. Der kan således ikke med rimelighed fastsættes en bestemt, generel tidsramme.

Der er dog ud fra en samlet betragtning en generel forventning om, at der kan ske en fortsat nedbringelse af leveringstiden.

Udlevering af data vil typisk ske på baggrund af en anmodning, der vedrører et geografisk område eller et bestemt nummer (afhængig af situationen). Indgangen til en datasøgning vil være en anmodning om oplysninger vedr. et nummer/ en person eller et geografisk punkt (f.eks. en mast). Det er de sidst registrerede oplysninger, der er de vigtigste - der er i den forbindelse behov for at kunne levere både A/B-nummer, IP-adresse, Mac-adressen og masteoplysninger i relevant omfang.

Vedr. telefoni er der behov for både at kunne få en tilkalds- og en opkaldsliste.

4.3.4. Økonomi

Omkostningerne vil variere alt afhængig af indretningen af de nuværende systemer, herunder om disse i tilstrækkeligt omfang giver mulighed for specifikke indgreb til indhentning af udvalgte data. Der kan for at opfylde forpligtelsen være behov for at optimere de nuværende generelle systemer eller opbygge parallel-systemer.

TI har alene kunnet vurdere effekterne for de trafikdata, der gemmes i dag. Analyserne har vist, at forudsætningerne varierer stærkt fra system til system, og omkostningerne vil ligeledes være afhængige af udfaldet af andre af arbejdsgruppens anbefalinger – herunder om kravet til kontaktpunkt i Danmark implicit medfører, at oplysningerne både skal findes og være friske på dansk jord.

Med disse usikkerheder har det ikke været meningsfuldt at angive et skøn, men der er dog identificeret mulighed for punktvis forbedringer for mobiltelefoni og fastnettelefoni for visse større udbydere.

4.3.5. Ikrafttrædelse

Ikrafttrædelse af bestemmelsen skal synkroniseres med ikrafttrædelse af logningsbekendtgørelsen.

4.4 Anbefaling 25

Af anbefaling 25 i Regeringens handlingsplan for terrorbekæmpelse fremgår, at:

25. Arbejdsgruppen anbefaler, at teleudbydere pålægges løbende at opdatere relevante teledatabaser med oplysninger om telefonnummer, rette operatør og nummerets bruger.

Lovforslaget vil nærmere gå ud på at tilvejebringe hjemmel til at fastsætte regler om etablering og opdatering af relevante databaser.

4.4.1. Formål

Politiet har behov for at kunne forbinde et telefonnummer med en udbyder, så de kan henvende sig det rigtige sted, når de skal videre med efterforskningen. Formålet med denne anbefaling er at sikre, at der til enhver tid findes et opdateret register over nummertildeling.

Politiet anvender i dag følgende to kilder til oplysninger:

1. 118-databasen (oplysninger om telefonnummer og kundens oplysninger)
2. OCH-databasen (oplysninger om netudbyder og tjenesteudbyder)

Politiet har dog ved flere lejligheder konstateret, at OCH ikke opdateres løbende.

For så vidt angår 118-databasen skal udbydere anmelde slutbrugeroplysninger hertil (også hemmelige numre). Databasen indeholder ikke oplysninger om udbydere.

Teleselskaberne TDC, SONOFON og Telia har oprettet selskabet, Operator's Clearing House A/S, der står for driften af en database, som indeholder oplysninger om udbydertilknytning for alle telefonnumre her i landet. OCH's database indeholder oplysninger om netudbyder og tjenesteudbyder. Databasen er nødvendig af hensyn til dirigering af trafik, oplysninger om nummerportering mm., hvorfor oplysningerne bør være til stede. De tekniske dirigeringsoplysninger opdateres umiddelbart efter ændring i kundeforholdet,

men oplysningerne vedrørende udbyderen har hidtil ikke været opdateret fuldstændigt.

Anbefalingen kan efter arbejdsgruppens vurdering gennemføres ved at indføre en pligt for udbydere til at til umiddelbart efter en slutbrugers skift af udbyder at indberette de ændrede oplysninger til en database, som i praksis formentlig kan være OCH-databasen. Politiet vil herefter ved at sammenholde denne database med 118-databasen kunne finde frem til, hvilken udbyder et telefonnummer er tilknyttet.

4.4.2. Hvem omfattes af pligten

Pligten i bestemmelsen påhviler alene udbydere af offentlige elektroniske kommunikationsnet og -tjenester, jf. lov om konkurrence- og forbrugerforhold på telemarkedet.

4.4.3. Outsourcing

Der er ikke behov for at kræve, at alle indrapporterer direkte til OCH, idet det vil være tilstrækkeligt at indrapportere til en mellemoperatør, som sørger for en samlet indrapportering til OCH. Pligten til at indrapportere påhviler dog udbyderen.

4.4.4. Hvad er omfattet af forpligtelsen

Forpligtelsen vedrører alle 8-cifrede telefonnumre anvendt til taletelefonitjenester.

4.4.5. Økonomi

Arbejdsgruppen vurderer, at denne forpligtelse vil kunne indføres for relativt beskedne omkostninger.

5. Forslag til lovtæst og specielle bemærkninger (*Videnskabsministeriet bemærker, at nedenstående lovtæst/specielle bemærkninger ikke er fuldstændig identisk med det udkast til lovforslag, der er sendt i hring. Der er overordnet tale om lovtækniske ændringer og tilfjelse af tilsyns- og strafbestedemmelser*).

Ændring af lov om konkurrence- og forbrugerforhold p telemarkedet jf. lovbekendtgrelse nr. 784 af 28. juli 2005

Anbefaling 15, 17 og 18 er indarbejdet i den eksisterende § 15 i lov om konkurrence- og forbrugerforhold p telemarkedet, jf. lovbekendtgrelse nr. 784 af 28. juli 2005, idet der er en naturlig sammenhæng, jf. ogs anbefaling 15. Anbefaling 25 krver en helt ny paragraf.

§ 15. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere som nævnt i § 6, stk. 1, skal uden udgift for staten³, herunder for politiet, sikre,

- 1) at det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet sledes, at politiet kan f adgang til at foretage indgreb i meddelelshemmeligheden, jf. retsplejelovens kapitel 71,
- 2) at det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet sledes, at politiet kan f adgang til at foretage indgreb i meddelelshemmeligheden, jf. retsplejelovens kapitel 71, i form af fremadrettet tele- og udvidet teleoplysning, umiddelbart efter at disse registreres.
- 3) at det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet sledes, at det efter anmodning fra politiet er muligt at foretage aflytning og øjeblikkelig overfrelse af telekommunikation til en anden medlemsstat efter artikel 18, stk. 5, litra a, sammenholdt med stk. 2, litra a og c, i konvention af 29. maj 2000 om gensidig retshjlp i straffesager mellem Den Europiske Unions medlemsstater,
- 4) at de gateway-stationer, udbyderen anvender, er indrettet sledes, at udbydere af elektroniske kommunikationstjenester i andre medlemsstater, der benytter gateway-stationen, har direkte adgang til denne, s det gennem sdanne udbydere er muligt at foretage direkte aflytning af telekommunikation p gateway-stationen vedrrende personer, der befinder sig i den pgældende medlemsstat, jf. artikel 19 i konvention af 29. maj 2000 om gensidig retshjlp i straffesager mellem Den Europiske Unions medlemsstater, og
- 5) at udbyderen har direkte adgang til gateway-stationer, der befinder sig i andre medlemsstater, og som udbyderen benytter, sledes at politiet gennem udbyderen har mulighed for at foretage direkte aflytning af telekommunikation p gateway-stationen vedrrende personer, der befinder sig her i landet, jf. retsplejelovens kapitel 71 og konvention af 29. maj 2000 om gensidig retshjlp i straffesager mellem Den Europiske Unions medlemsstater.

³ Som det fremgr af teksten er branchen af den opfattelse, at merudgifter, der plgges udbydere til forml, der udelukkende tilgodeser politiets ønsker, ikke skal dkkes af udbyderne og deres kunder. Sfremt dette besluttes kan flgende tekstforslag indg i love: ”Stk. 1a. Omkostninger til etablering og drift af det i stk. 1 nævnte udstyr dkkes helt eller delvist af politiet, hvis udstyret alene eller overvejende etableres og drives af hensyn til politiets efterforskningsmuligheder, og krav om funktionaliteten ikke var gældende pr. 31.01.06.”

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan efter forhandling med justitsministeren fastsætte nærmere regler om de tekniske krav til udstyr, systemer og gateway-stationer som nævnt i stk. 1.

Stk. 3. Det påhviler udbyderen at bistå politiet ved gennemførelse af indgreb i meddelelseshemmeligheden i de i stk. 1, nr. 3, nævnte tilfælde.

Stk. 4. Det påhviler udbyderen at sikre, at politiets anmodninger om fremskaffelse af historisk tele- og udvidet teleoplysning, jf. stk. 1, nr. 1, behandles straks og på en måde, så hensigten med indgrebet ikke forspildes.

Stk. 5. Ministeren for videnskab, teknologi og udvikling kan efter forhandling med justitsministeren fastsætte regler, hvorefter de i stk. 1, nr. 1, 2 og 3, nævnte krav til indretning af udstyr kan fraviges i særlige tilfælde, hvor tekniske eller praktiske hensyn nødvendiggør dette.

§ 15 a. Udbydere af elektroniske kommunikationsnet eller -tjenester skal til en fælles database, jf. § 56, stk. 3, indberette og opdatere oplysninger om telefonnummer og aktuel udbyder. Oplysninger skal indberettes umiddelbart efter en slutbrugers skift af udbyder, jf. § 36 om nummerportabilitet. Forpligtelsen påhviler den udbyder, der modtager slutbrugeren, og den gælder også i de tilfælde, hvor slutbrugeren overføres uden anvendelse af procedurerne for nummerportabilitet.

Stk. 2. IT- og Telestyrelsen fører tilsyn med og træffer afgørelse i sager om udbydere af elektroniske kommunikationsnet eller -tjenesters overholdelse af stk. 1.

Bemærkninger:

Til §15

Stk. 1

Bestemmelsen i § 15, stk. 1, finder anvendelse på alle udbydere til slutbrugere, men er ikke begrænset således, at udbyderen alene skal stille oplysninger til rådighed om egne slutbrugere. Politiet bør gå til den udbyder, som har det pågældende slutbrugerforhold, men der kan i særlige tilfælde være behov for at gå til andre udbydere.

Ved 'udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere' forstås i denne lov parter, som på kommercielt grundlag stiller net eller tjenester til rådighed for flere slutbrugere, jf. lovens § 6, stk. 1.

Stk. 1, nr. 1

Pligten i bestemmelsen påhviler udbydere af elektroniske kommunikationsnet og -tjenester til slutbrugere, jf. lov om konkurrence- og forbrugerforhold på telemarkedet.

Det er den udbyder, der har slutbrugerforholdet, der har ansvaret for at sikre, at der kan gives adgang til indgreb i meddelelseshemmeligheden.

Arbejdsgivere kan ikke anses for udbydere af telenet eller teletjenester i forhold til de ansatte, som man stiller intern teleinfrastruktur og tjenester til rådighed for i forbindelse med ansættelsesforholdet. Dette gælder både computere, infrastruktur m.v., der benyttes på arbejdspladsen, og evt. hjemmearbejdspladser.

Det er i den forbindelse uden betydning, hvorvidt arbejdsgiveren selv forestår (etablerer, overvåger og driver) den omhandlede interne infrastruktur og de omhandlede interne tjenester (såvel telefoni som data), eller om virksomheden har outsourcet driften heraf til en ekstern outsourcing-leverandør. Heller ikke outsourcing-leverandøren kan således anses for udbyder af telenet eller teletjenester.

Outsourcing-leverandører kan antage flere former, afhængigt af deres forretningsmodel, og kan således omfatte virksomheder, der udover den interne teleinfrastruktur og de basale interne teletjenester overvåger, driver og vedligeholder virksomhedens øvrige centrale IT-systemer og applikationer, virksomhedens hjemmesider, herunder hjemmesider til internethandel, email-adresser og -applikationer m.v. Det outsourcete udstyr og de outsourcete funktioner kan fysisk enten være placeret hos virksomheden (kunden) selv eller hos leverandøren.

Uanset hvor udstyret er placeret, vil der i den samlede installation nødvendigvis indgå en eller flere dedikerede forbindelser (typisk faste kredsløb), med henblik på at sikre outsourcing-leverandøren, henholdsvis virksomheden, adgang til det omhandlede interne net med tilhørende interne tjenester.

For så vidt angår de ovenfor beskrevne interne net, vil politiet via oplysninger fra udbydernes net og tjenester således kunne komme frem til det punkt, hvor det interne net er koblet til det offentlige net, dvs. til det punkt, hvor igennem eksempelvis virksomhedens kommunikation med omverdenen formidles. Derfra er det politiets opgave at komme videre indenfor det interne net. Det skal bemærkes, at kommunikation i interne net kun er undtaget, så længe der alene er tale om intern kommunikation modsat den situation, at kommunikationen går ud af det private net til det offentlige net.

Den udbyder, som det private net anvender til kommunikation med omverdenen, er imidlertid forpligtet til f.eks. at stille oplysninger om, hvem et givent nummer, IP-adresse eller lignende er tildelt, til rådighed for politiet.

Udover ovennævnte afgrænsning af udbyder-begrebet er det – af hensyn til at undgå usikkerhed- relevant at slå fast, at heller ikke virksomheder, der via internettet udbyder den stadigt voksende liste af web-baserede applikationer, som eksempelvis computerspils-applikationer, søgetjenester, email-tjenester af samme type som f.eks. "hotmail", videokonference-applikationer, meddelelsetjenester som f.eks. MS Messenger og LotusSameTime, download af software og lign., IP-telefoni applikationer, der ikke omfatter udveksling af trafik med den offentlige nummerplan og de traditionelle taletefonitjenester (PSTN), kan anses for udbydere af elektroniske kommunikationsnet eller -tjenester .

For de ovenfor nævnte afgrænsninger af udbyder-begrebet gælder i sagens natur, at virksomheder, der både leverer denne type ydelser (outsourcing og/eller webbaseret udbud af applikationer), og tillige er udbydere af elektroniske kommunikationsnet eller -tjenester i telelovgivningens forstand, for så vidt angår den sidstnævnte del af deres virksomhed, vil være omfattet af udbyder-begrebet.

For så vidt angår interne net, vil politiet via oplysninger fra de offentlige net kunne komme til det punkt, hvor det interne net termineres i det offentlige net. Derfra er det politiets opgave at komme videre indenfor det interne net.

Det er muligt for udbyderen af elektroniske kommunikationsnet eller -tjenester at out-source forpligtelsen til indretning af udstyr og systemer, forpligtelsen påhviler dog stadig den udbyder, som out-sourcer forpligtelsen. Det kan f.eks. gøre sig gældende for gensalgsudbydere og bolignet.

Det er stadig den udbyder, som out-sourcer forpligtelsen, der er ansvarlig for, at den udbyder, forpligtelsen er out-sourcet til, indretter systemet, så indgreb i meddelelseshemmeligheden kan finde sted.

Bestemmelsens anvendelsesområde udvides til at omfatte mere end bestemmelsens nuværende indhold. Det nuværende indhold videreføres således, at udbydere af elektroniske kommunikationsnet og -tjenester stadig med den nye bestemmelse har pligt til at indrette centraler, så det er teknisk muligt at foretage indgreb i meddelelseshemmeligheden, og til ved anskaffelse af centraludstyr at sikre, at dette er indrettet således, at indgreb i meddelelseshemmeligheden er mulig.

På grund af, at forpligtelsen har været begrænset til at omfatte indretningen af centraler, har den praktiske udmøntning af § 15 hidtil været at sikre politiet mulighed for at kunne foretage aflytning og få udleveret fremadrettede teleoplysninger.

Med den udvidelse af bestemmelsen, der nu lægges op til, vil flere indgreb i meddelelseshemmeligheden imidlertid være relevante. Fremover stilles derfor krav om, at udstyr og systemer indrettes således, at indgreb i meddelelseshemmeligheden bliver mulige både fremadrettet og bagudrettet .

Bestemmelsen udvides til også at omfatte andet teknisk udstyr og andre tekniske systemer end centraler og andre teknologiske fremføringstyper, der måtte opstå fremover.

Med teknisk udstyr og tekniske systemer skal forstås det udstyr, der er nødvendigt for at foretage indgreb i meddelelseshemmeligheden.

Faciliteterne i udstyret og systemerne til indgreb i meddelelseshemmeligheden bør, så vidt det er muligt, være baseret på fælleseuropæiske standarder. Sådanne standarder foreligger imidlertid indtil videre kun i begrænset omfang.

Med indgreb i meddelelseshemmeligheden forstås de typer af indgreb i meddelelseshemmeligheden, som findes i retsplejelovens § 780 vedrørende teleområdet. Disse typer indgreb er: Telefonaflytning, teleoplysning (f.eks. hvilke telefonnumre der har været sat i forbindelse med et bestemt telefonnummer),

udvidet teleoplysning (masteoplysninger). For en nærmere fortolkning af § 780 henvises til bemærkningerne til Retsplejeloven.

Det nærmere omfang af de data, som teleudbydere forpligtes til at udlevere efter en kendelse om indgreb i meddelelshemmeligheden i form af teleoplysning, afhænger af udmøntningen af hjemmelen i Retsplejeloven § 786, stk. 4, 2. pkt. til at udstede "logningsbekendtgørelsen", jf. bemærkningerne til § 15, stk. 4 nedenfor.

Den information, der kan tilvejebringes ved et indgreb i meddelelshemmeligheden, vil afhænge af tjenesten. Hvis der er tale om traditionel taletelefoni, SMS og kredsløbskoblet datatransmission, vil både teleoplysninger, udvidede teleoplysninger og, for så vidt angår fremadrettede oplysninger, selve indholdet af kommunikationen umiddelbart være tilgængeligt i de for disse tjenester standardiserede formater. [I forbindelse med andre typer datatransmission, vil indholdet af kommunikationen og teleoplysninger knyttet til kommunikationen skulle udledes af bruttodatastrømmen. For så vidt angår kravene til udtagelse af fremadrettede data, henvises til bemærkningerne til § 15, stk. 1, nr. 2.

Hvis en taletelefonitjeneste benytter en transmissionstjeneste, som udbydes af samme udbyder, er det muligt for udbyderen at stille oplysninger til rådighed fra både taletelefonitjenesten og transmissionstjenesten i samme omfang som et tilsvarende tilfælde, hvor de pågældende udbydere ikke er sammenfaldende.

Hvis en VoIP-tjeneste (en applikation) udbydes af en anden end selve transmissionstjenesten, kan udbyderen af transmissionstjenesten kun stille oplysninger til rådighed fra transmissionstjenesten. Dette er f.eks. gældende med en applikation som SKYPE, når opkaldsmulighed til almindelige telefonnumre ikke indgår. Det er således ikke muligt for udbyderen at dekryptere data for så vidt angår en sådan VoIP-tjeneste. Udbyderen af transmissionstjenesten kan i denne situation således ikke forpligtes til at stille oplysninger til rådighed fra selve VoIP-tjenesten, herunder indholdet heraf.

Til stk. 1, nr. 2

Denne bestemmelse skal sikre, at det er muligt at foretage indgreb i meddelelshemmeligheden for så vidt angår fremadrettede tele- og masteoplysninger.

Fremadrettet skal i denne sammenhæng forstås som 'fra det tidspunkt der fastslås i en retskendelse og fremad'.

Adgang til fremadrettede teleoplysninger sker automatisk ved etablering af en aflytning og udleveres til politiet mod kendelse. For så vidt angår telefonitjenester, giver en aflytning således adgang til viden om A-nummer og B-nummer. For så vidt angår pakkekoblet datatransmission, herunder internetadgang, giver en aflytning i form af adgang til bruttodatastrømmen politiet mulighed for adgang til viden om, hvad kunden foretager sig via tjenesten.

Formålet er ikke, at udbyder skal kunne dekryptere data. Det vil være politiets opgave at dekryptere data. Udbyder er imidlertid forpligtet til at udtage data, således at politiet alene modtager de oplysninger, som er omfattet af kendelsen (aflytning, teleoplysning eller udvidet teleoplysning). I relation til de fremadrettede oplysninger er det dermed udbyders pligt at påse, at der kan stilles relevante data til rådighed for politiet – det er politiets opgave at fortolke de leverede data.⁴

På den baggrund er det hensigten, at der i bestemmelsen stilles krav om, at det pågældende udstyr og de pågældende systemer skal være således indrettet, at udbydere, som anvender kryptering som en integreret del af deres net, er i stand til at stille den kommunikerede information til rådighed for politiet i ukrypteret form.

Kryptering, der ikke udgør en integreret del af de pågældende udbyderes basale tjenester, herunder kryptering der tilføjes af andre, er det derimod ikke den pågældende net- eller tjenestes udbyders ansvar at sikre indgreb i meddelelseshemmeligheden i i ukrypteret form, idet dette ikke i praksis vil være muligt for net- eller tjenesteudbyderen.

Det bemærkes, at for mobilkommunikation vil det ikke være muligt at levere udvidede teleoplysninger ”online”. Der findes ikke en teknisk løsning til i realtid at kunne se, hvilken abonnent der er på en bestemt mast. Dette skyldes, at oplysningerne, som genereres, skal opsamles fra en given mast og sendes til et centralt sted, før disse kan anvendes. Dette kan dog ske meget hurtigt, og oplysningerne vil derfor være friske historiske oplysninger. Dette opfylder dog politiets behov for fremadrettede udvidede teleoplysninger (masteoplysninger).

Stk. 1, nr. 3-5 samt stk. 2-3 er indholdsmæssigt uændrede videreførelser af gældende regler.

Til stk. 4

Bestemmelsen skal både sikre, at teleudbyderne bistår politiet ved at iværksætte indhentelse af historiske tele- og masteoplysninger straks efter en konkret anmodning, og ved at oplysningerne udleveres til politiet så hurtigt som muligt indenfor en rimelig tidsfrist, således at hensigten med indgrebet ikke forspildes. Der er således ikke tale om, at en udbyder med det samme (straks) skal kunne levere data, men blot at udbyder straks skal gå i gang.

Målsætningen med bestemmelsen er at optimere leveringstiden på efterspurgte oplysninger. Det skal bemærkes, at tidsrammen, jf. ”på en måde, så hensigten med indgrebet ikke forspildes”, må knytte sig til, hvad der er praktisk muligt på baggrund af den teknologiske udvikling på et givet tidspunkt.

⁴ Gartner har oplyst, at det er muligt med standardudstyr at udtage data, således at det alene er data vedrørende en bestemt IP-adresse, MAC-adresse, punkt eller lignende, der stilles til rådighed for politiet i henhold til retskendelsen.

Teknologien og de forskellige datatyper er i stadig udvikling, og der skal ved fortolkning af, hvor hurtigt teleudbyderne skal levere de efterspurgte oplysninger, ske en konkret graduering både i forhold til bestemte datatyper og bestemte systemer. Det nærmere omfang af de data, som teleudbyderne forpligtes til at udlevere, afhænger af udmøntningen af hjemmelen i Retsplejeloven § 786, stk. 4, 2. pkt. til at udstede ”logningsbekendtgørelsen”. Forpligtelsen vil komme til at omfatte krav om udlevering af flere forskellige datatyper, som skal udtrækkes fra forskellige teknologier.

”Historiske data” vil sige data frem til tidspunktet for henvendelsen. Det vil også sige data fra de sidste 24 timer. Teleudbyderne opdaterer typisk systemerne én gang i døgnet ved midnat. I forhold til de data, der er genereret siden midnat, og som altså er yngre end de data, der er omfattet af den sidste opdatering, vil der efter omstændighederne kunne laves specifikke indgreb og særkørsler, så politiet kan få udvalgte oplysninger så hurtigt, at hensigten med indgrebet ikke forspildes.

Der kan imidlertid for at opfylde forpligtelsen være behov for at optimere de nuværende systemer/ lave parallel-systemer.

Det skal bemærkes, at det generelt vil være teknisk muligt at fremskaffe disse oplysninger. Der er dog identificeret udstyr i mindre dele af fastnettet, hvor der endnu ikke er kendte løsninger til at skaffe oplysninger om dagens trafik i løbet af tilstrækkelig kort tid. Det vil formentlig kræve nærmere dialog med udstyrsleverandøren at vurdere, om der kan findes en teknisk løsning.

Det skal endvidere bemærkes, at der i forhold til tidsrammen for udlevering af oplysninger til politiet må tages hensyn til, at de systemer, der genererer oplysningerne, ikke vil være søgbare hele tiden. Dette kan skyldes forhold som behovet for opdatering af databaser, opgradering af systemerne, vedligeholdelse el. lign. Der kan således ikke med rimelighed fastsættes en bestemt, generel tidsramme.

Udlevering af tele- og masteoplysninger vil typisk ske på baggrund af en anmodning, der vedrører et geografisk område eller et bestemt nummer (afhængig af situationen). Indgangen til en datasøgning vil være en anmodning om oplysninger vedr. et nummer/ en person eller et geografisk punkt (f.eks. en mast). Det er de sidst registrerede oplysninger, der er de vigtigste for politiet - der er i den forbindelse behov for at kunne levere både A/B-nummer, IP-adresse eller MAC-adresse og masteoplysninger i relevant omfang.

Vedrørende telefoni er der behov for både at kunne få en tilkalds- og en opkaldsliste.

Bestemmelsen i § 15, stk. 4, skal således bl.a. sikre rammerne for politiets indgreb i medfør af retsplejelovens regler om indgreb i meddelelseshemmeligheden.

De oplysninger, som udbydere skal indrette deres systemer til at logge med henblik på indgreb i meddelelshemmeligheden i form af teleoplysning og udvidet teleoplysning, fremgår af retsplejelovens § 786, stk. 4, og de i medfør heraf fastsatte regler.

Det betyder ligeledes, at undtagelser fra selve pligten til logning vil fremgå af regler udstedt i medfør af retsplejelovens § 786, stk. 4.

Da der endnu ikke er fastsat regler i medfør af retsplejelovens § 786, stk. 4, gengives her, som bidrag til forståelsen af omfanget af logningsforpligtelsen samt pligtssubjektet, uddrag af bemærkningerne til lovforslaget, der ligger til grund for bemyndigelsen.

Desuden gengives Justitsministerens svar til Retsudvalget på spørgsmål 63 og 123 til lovforslaget.

(uddrag af bemærkninger til lovforslag L35, fremsat den 13. december 2001, vedr. 'Lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige').

Til § 2

Retsplejeloven

Til nr. 2 og 3 (retsplejelovens § 786, stk. 1, 4, 5, 6 og 7)

- udbyderbegrebet:

"Den foreslåede ændring af retsplejelovens § 786, stk. 1, indebærer, at det vil påhvile også udbydere af telenet og teletjenester, der henvender sig til afgrænsede kundesegmenter, at bistå politiet ved gennemførelsen af indgreb i meddelelshemmeligheden. Som det fremgår under pkt. 3.1.3. ovenfor finder Justitsministeriet, at både hensynet til en effektiv regulering og hensynet til konkurrenceforholdene i branchen tilsiger, at der skal kunne stilles krav til udbydere, uanset til hvilke kunde grupper de udbyder telenet og teletjenester."

Udbyderbegrebet – altså pligtssubjektet for logningsforpligtelsen - var i øvrigt genstand for diskussion i forbindelse med fremsættelsen af den første terrorlovpakke. I besvarelsen af spørgsmål 63 og 123 fra udvalget er begreberne yderligere præciseret:

Spørgsmål nr. 63:

Vil ministeren få udarbejdet et teknisk notat vedrørende dataovervågningen, jf. de foreslåede ændringer af retsplejelovens § 786, hvori det bliver oplyst (...)

b) hvem der bliver omfattet af registreringspligten, om det kun er teleselskaber, som TDC, Sonofon m.v., eller om det også bliver alle arbejdsgivere, boligselskaber m.v., der udbyder internetadgang?

Svar:

(...)

Afgrænsningen af den persongruppe, der bliver omfattet af den foreslåede regulering, må i første omgang foretages i forhold til begrebet "udbydere af telenet og teletjenester", jf. den foreslåede bestemmelse i § 786, stk. 4, 1. pkt.

Efter Justitsministeriets opfattelse vil eksempelvis en arbejdsgiver ikke være udbyder af en teletjeneste i forhold til den ansatte, der anvender en af arbejdsgiverens computere på arbejdspladsen. Som et yderligere eksempel kan nævnes, at en skole eller et universitet efter Justitsministeriets opfattelse ikke vil være at anse som teleudbyder i forhold til studenterne, når de anvender uddannelsesinstitutionens computere til internettrafik og anden elektronisk kommunikation.

Der stilles ikke krav om udbud af offentlige telenet og teletjenester. Det indebærer, at også udbydere, der kun henvender sig til en på forhånd afgrænset kundekreds vil være omfattet. Således vil eksempelvis et boligselskab være at anse som udbyder af en teletjeneste, såfremt man mod betaling tilbyder f.eks. adgang til Internet eller telefon til beboerne. Dette vil som udgangspunkt gælde uanset, hvor mange brugere boligselskabet udbyder teletjenesten til.

Efter Justitsministeriets opfattelse vil det imidlertid ikke være hensigtsmæssigt, at enhver udbyder af telenet og teletjenester omfattes af den foreslåede regulering. I forbindelse med den nærmere regelfastsættelse efter den foreslåede bestemmelse i § 786, stk. 4, 2. pkt., vil der derfor skulle foretages en hensigtsmæssig afgrænsning af den omfattede personkreds gennem eksempelvis en »bagatelgrænse«, hvorefter mindre udbydere ikke generelt skal logge trafikdata i 1 år.

Justitsministeriet har endvidere til brug for besvarelsen af spørgsmålet anmodet Ministeriet for Videnskab, Teknologi og Udvikling om en udtalelse om teknologispecifik afgrænsning af logningsforpligtelsen.

Ministeriet for Videnskab, Teknologi og Udvikling har oplyst følgende:

»I forbindelse med regelfastsættelsen vil der ligeledes være behov for nærmere at undersøge i hvilket omfang det er nødvendigt at undtage særlige typer af tjenester fra logningspligten. Det skyldes, at det som følge af tjenesternes tekniske konstruktion eller lignende ikke vil være hensigtsmæssigt eller tjene til opfyldelse af lovforslagets formål om styrkelse af politiets efterforskningsmuligheder at kræve logning af trafikdata.

Blandt de tjenester, der kan indgå i disse overvejelser, er ældre tjenester så som teksttefontjenesten til handicappede, hvor den tekniske indretning ikke muliggør en egentlig logning.

Tjenester med lokale og isolerede infrastrukturnet så som FWA-net eller WLAN-net, der kræver, at der etableres en tilslutning til andre telenet, før der kan tilbydes egentlige teletjenester til slutbrugerne, kan også tænkes undtaget fra logningspligten. Tilsvarende gælder for lukkede landmobile radionet, der benyttes af eksempelvis politiet, beredskabstjenester, vognmænd og taxifirmaer, og datanet der udelukkende benyttes til opsamling og videres endelse af data fra

person til maskine eller fra maskine til maskine. Det sker eksempelvis ved overvågning og styring af processer i produktionsanlæg.

Flere udenlandske teleselskaber har fiberforbindelser gående igennem Danmark uden at drive televirksomhed i Danmark. Disse er uden tilslutningsmuligheder for trafikopsamling eller fordeling i Danmark og bør ikke nødvendigvis omfattes af pligten til at logge trafikdata.

Ved luftbåren radio- og TV-broadcast, der, selvom disse systemer er envejssystemer, er omfattet af definitionen af telekommunikation, vil det formentlig heller ikke være hensigtsmæssigt at kræve nogen form for logning.

Eksemplificeringen er ikke udtømmende. Udviklingen i kommunikationssektoren kan medføre et behov for løbende at kunne undtage tjenester fra registreringspligten. Det giver den foreslåede § 786, stk. 4, 2. pkt. mulighed for.«

Spørgsmål nr. 123:

Er det korrekt forstået, at de i det foreslåede § 786, stk. 4, 1. pkt., nævnte udbydere ikke skal være arbejdsgivere, andelsboligforeninger, foreninger og lignende?

Svar:

1. Det fremgår af pkt. 3.1.3.3. i de almindelige bemærkninger til lovforslaget, at de nærmere regler om logningspligten vil være af en sådan karakter og detaljeringsgrad, at det ikke vil være hensigtsmæssigt at fastsætte dem ved lov. Samtidig har de tidsmæssige rammer ikke muliggjort, at der har kunnet skabes klarhed over alle de tekniske aspekter af forslaget, herunder gennem inddragelse af tele- og internetbranchen.

(...)

2. Mere generelt kan det oplyses, at en arbejdsgiver – som anført i Justitsministeriets besvarelse af spørgsmål nr. 63, jf. L 35 – bilag 71 – efter Justitsministeriets opfattelse ikke vil være udbyder af en teletjeneste i forhold til den ansatte, der anvender en af arbejdsgiverens computere på arbejdspladsen. Det samme må gælde, hvis den ansatte fra sin bopæl – eksempelvis gennem en såkaldt hjemmearbejdsplads hedens computernetværk og herigennem kan tilslutte sig Internettet.

Det må herved forudsættes, at den ansatte ikke skal yde betaling til arbejdsgiveren for internetadgangen. I modsat fald kan arbejdsgiverens formidling af internetadgang ikke siges at have sammenhæng med varetagelsen af den ansattes arbejdsopgaver, og arbejdsgiveren vil da kunne sidestilles med andre internetudbydere. Stiller arbejdsgiveren eksempelvis en computer og et internetabonnement hos en teleudbyder til den ansattes rådighed, således at tilslutningen til Internettet ikke sker via arbejdsgiverens computernetværk, vil pligten til at logge internettrafikken påhvile den pågældende udbyder, hvis denne i øvrigt er omfattet af logningspligten.

3. Endvidere fremgår det af den nævnte besvarelse, at en skole eller et universitet efter Justitsministeriets opfattelse ikke vil skulle anses som teleudbyder i forhold til elever og studenter, som anvender uddannelsesinstitutionens computere til internettrafik og anden elektronisk kommunikation. Her vil tilsvarende gælde, at

der ikke skal foretages logning af den internettrafik, som de studerende vederlagsfrit foretager via en ekstern tilslutning til uddannelsesinstitutionens computernetværk.

4. Om andelsboligforeninger, foreninger og lignende skal foretage logning, vil afhænge af, om foreningen reelt svarer til en teleudbyder i forhold til brugerne. Dette må som udgangspunkt antages at være tilfældet, idet der – som det fremgår af den ovenfor nævnte besvarelse af spørgsmål nr. 63 – ikke stilles krav om udbud af offentlige telenet og teletjenester. Det indebærer, at også udbydere, der kun henvender på forhånd afgrænset kundekreds, vil være omfattet.

Således vil eksempelvis et boligselskab være at anse som udbyder af en teletjeneste, hvis selskabet mod betaling tilbyder f.eks. adgang til Internet eller telefon til beboerne. Dette vil som udgangspunkt gælde uanset, hvor mange brugere boligselskabet udbyder teletjenesten til.

5. Efter Justitsministeriets opfattelse vil det imidlertid ikke være hensigtsmæssigt, hvis enhver udbyder af telenet og teletjenester bliver omfattet af den foreslåede regulering.

I forbindelse med den nærmere regelfastsættelse efter den foreslåede bestemmelse i § 786, stk. 4, 2. pkt., vil der derfor skulle foretages en hensigtsmæssig afgrænsning af den omfattede personkreds gennem eksempelvis en »bagatelgrænse«, hvorefter mindre udbydere ikke generelt skal logge trafikdata i 1 år.

En sådan »bagatelgrænse« vil ikke være udtryk for, at de oplysninger, som den pågældende boligforening ellers ville skulle logge, på forhånd kan siges ikke at ville være af efterforskningsmæssig interesse i en given sag. Undtagelsen vil være begrundet i, at en logningspligt for mindre udbydere må forventes at være forbundet med navnlig administrative omkostninger, der ikke vil modsvares af det efterforskningsmæssige behov for logoplysninger fra mindre udbydere.

- logningspligtens omfang (datatyper):

”Den foreslåede bestemmelse i retsplejelovens § 786, stk. 4, fastsætter i 1. pkt. en pligt for udbydere af telenet og teletjenester til at foretage registrering og opbevaring (logning) i 1 år af de oplysninger om tele- og internetkommunikation, der er relevante for politiets efterforskning og retsforfølgning af strafbare forhold. Endvidere gives der i 2. pkt. hjemmel til, at justitsministeren ved bekendtgørelse kan fastsætte nærmere regler om logningspligtens indhold og omfang..

Både udbydere af offentlige telenet og teletjenester og udbydere, der henvender sig til specifikke, på forhånd afgrænsede kundesegmenter, vil kunne omfattes af den foreslåede regulering.

For så vidt angår teletrafik vil de oplysninger, som logningspligten kan omfatte, navnlig være de oplysninger, som politiet har brug for i forbindelse med indgreb i meddeleleshemmeligheden i form af teleoplysning og udvidet teleoplysning, jf. retsplejelovens § 780, stk. 1, nr. 3 og 4. Det kan eksempelvis være det kaldende og det kaldte nummer (A- og B-nummer), opkaldstidspunkter og varigheden af

samtaler samt – for mobiltelefoners vedkommende – oplysninger om anvendte sendemaster/celler.

For så vidt angår internettrafik vil der kunne fastsættes regler om logning af den dynamiske tildeling af IP-adresser, tidspunkt for opkobling og nedkobling samt opkoblingens varighed. I praksis vil udbyderen kun være i stand til at levere oplysninger om, hvem der har efterladt et elektronisk spor på Internettet, hvis udbyderen er i besiddelse af præcise oplysninger om, hvilken kunde, der på det pågældende tidspunkt har anvendt en tildelt IP-adresse.

Det må overvejes i forbindelse med den nærmere regelfastsættelse, om der er behov for at stille krav om, at internetudbydere ved opkobling via telefonnettet skal logge A og B-nummeret. Som anført under pkt. 3.1.3.2. ovenfor har det over for Justitsministeriet været fremført, at der i praksis vil kunne være tekniske hindringer for internetudbyderes registrering af det kaldende nummer (A-nummeret).

Hvor forbindelsen til Internettet ikke etableres via telefonnettet, men etableres via en fast forbindelse, f.eks. såkaldte ADSL-forbindelser, vil der ikke være teknisk grundlag for at opstille krav om, at internetudbyderen logger A-nummeret. I stedet vil der skulle registreres de tilsvarende oplysninger, der gør det muligt at føre det elektroniske spor tilbage til en bestemt kunde.

(...).”

- hvad er IKKE omfattet af logningsbekendtgørelsen:

”Der vil ikke kunne fastsættes regler om, at internetudbydere løbende skal foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger. Hensigten med forslaget er alene at kunne føre elektroniske spor, der findes på Internettet i forbindelse med kriminelle aktiviteter, tilbage til gerningsmændene.

For så vidt angår elektronisk post stilles der ikke forslag om en generel logning af indholdsdata, men alene af oplysninger svarende til teleoplysninger, dvs. oplysninger som f.eks. afsender, modtager og tidsangivelse vedrørende kommunikationen. Den nærmere regulering vedrørende elektronisk post vil således ikke kunne forpligte internetudbydere til generelt at gemme indholdet af elektroniske breve.”

- opbevaringsperiode:

”Opbevaringsperioden vil være 1 år for de oplysninger, der ikke opbevares med henblik på debitering. Trafikdata, der gemmes med henblik på debitering, vil – uanset om de pågældende data omfattes af den lovbestemte logningspligt – som hidtil kunne opbevares indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger, jf. artikel 6, stk. 2, i direktivet og § 30, stk. 2, i bekendtgørelse om udbud af telenet og teletjenester. Dette indebærer i praksis, at oplysningerne kan gemmes i op til 5 år.

Det forudsættes, at de nærmere regler fastsættes efter dialog med tele- og internetudbydere. Dette er ikke mindst afgørende for at sikre en hensigtsmæssig teknologisk udformning af reglerne.

Der henvises i øvrigt til pkt. 3.1.2. og 3.1.3. i de almindelige bemærkninger til lovforslaget.”-

(...)

- strafbestemmelser:

Efter den foreslåede bestemmelse i retsplejelovens § 786, stk. 6, vil forsætlig eller uagtsom overtrædelse af logningspligten kunne straffes med bøde. Der kan endvidere pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Efter den foreslåede bestemmelse i retsplejelovens § 786, stk. 7, vil der kunne fastsættes regler om bødestraf for forsætlig eller uagtsom overtrædelse af de udfyldende regler om logningspligten, jf. stk. 4, 2. pkt., og om praktisk bistand til politiet i forbindelse med indgreb i meddelelshemmeligheden, jf. stk. 5. Der kan endvidere fastsættes bestemmelser om at pålægge selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til stk. 5

Det fremgår af rapporten ”Det danske samfunds indsats og beredskab mod terror”, at: ”Da behovet for at kunne foretage indgreb primært retter sig mod de større udbydere, og da omkostningerne ved at ændre de tekniske systemer vil kunne virke meget byrdefulde for især mindre udbydere, bør det efter arbejdsgruppens opfattelse – med henblik på at sikre et bredt konkurrence- og innovationspræget telemarked – overvejes at undtage de helt små udbydere, herunder f.eks. andelsbolig- og antenneforeninger.”

Efter den foreslåede bestemmelse vil ministeren for videnskab, teknologi og udvikling efter forhandling med justitsministeren kunne fastsætte regler, hvorefter de krav, der efter § 15, stk. 1, nr. 1, 2 og 3, stilles til indretningen af udstyr og systemer, fraviges i særlige tilfælde, hvor tekniske eller praktiske hensyn nødvendiggør dette.

På trods af at den kommende bestemmelse i § 15 bliver begrænset til at gælde for udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, vil der stadig være behov for en bemyndigelsesbestemmelse til fravigelse af forpligtelsen til at indrette udstyr og systemer.

Det vil fortsat være muligt at undtage udbydere som beskrevet i bemærkningerne til den tidligere § 15, stk. 4.

På grund af den udvidede bestemmelse i § 15 til at omfatte indretningen af andet udstyr og systemer end centraler, vil bemyndigelsesbestemmelsen fremover også kunne anvendes til at fravige forpligtelsen for visse offentlige elektroniske kommunikationsnet eller -tjenester, hvor det ikke teknisk giver mening at pålægge en forpligtelse til at kunne foretage indgreb i meddelelshemmeligheden.

Det kan f.eks. gælde radiobaserede systemer og andre systemer med mulighed for direkte kommunikation mellem terminaler, f.eks. TETRA, ligesom det kan være relevant at kunne fritage broadcasting-tjenester fra forpligtelsen.

Til § 15a

I rapporten ”Det danske samfunds indsats og beredskab mod terror” anbefales det, det at politiet, herunder Politiets Efterretningstjeneste, får mulighed for at indhente oplysninger om, hvem en telefon tilhører, samt hvilken operatør et telefonnummer er tilknyttet.

Politiet anvender i dag følgende to kilder til oplysninger:

1. 118-databasen (oplysninger om telefonnummer og kundens oplysninger)
2. OCH-databasen (oplysninger om operatør og udbyder)

Politiet har dog ved flere lejligheder konstateret, at OCH ikke opdateres løbende.

For så vidt angår 118-databasen skal udbydere anmelde slutbrugeroplysninger hertil (også hemmelige numre). Databasen indeholder ikke oplysninger om udbydere.

OCH's database indeholder oplysninger om netoperatører og serviceoperatører. Databasen er nødvendig af hensyn til videregivelse af trafik, nummerportering mm., hvorfor oplysningerne bør være tilstede. De tekniske dirigeringsoplysninger opdateres umiddelbart efter ændring i kundeforholdet, men oplysningerne vedrørende udbyderen har hidtil ikke været opdateret fuldstændigt.

Bestemmelsen pålægger udbyderne en pligt til umiddelbart efter en ændring af et slutbrugerforhold at indberette de ændrede oplysninger til OCH-databasen. Politiet vil herefter ved at sammenholde denne database med 118-databasen og evt. IT- og Telestyrelsens fortegnelse over nummerserier kunne finde frem til, hvilken udbyder et telefonnummer er tilknyttet.

Der er ikke behov for at kræve, at alle indrapporterer direkte til OCH, idet det vil være tilstrækkeligt at indrapportere til en mellemoperatør, som sørger for en samlet indrapportering til OCH. Pligten til at indrapportere påhviler dog udbyderen.

Det forudsættes, at telebranchen selv etablerer en teledatabase til brug for oplysningerne. Udbyderne kan vælge at anvende OCH A/S' database, idet denne database allerede i dag indeholder de relevante oplysninger. Alternativt kan udbyderne vælge at etablere en anden database til brug for oplysningerne. Dette kan eventuelt aftales i et branchesamarbejde.

IT- og Telestyrelsen fører tilsyn med bestemmelsens overholdelse.

Bilag 6.1.

Definitioner

I nedenstående defineres en række af de nøglebegreber, der anvendes i afrapporteringen, herunder i lovforslaget.

Indgreb i meddelelseshemmeligheden

Indgreb i meddelelseshemmeligheden er beskrevet i Retsplejelovens § 780.

Retsplejelovens § 780 indeholder følgende typer af indgreb i meddelelseshemmeligheden: Telefonaflytning, anden aflytning (rumaflytning), teleoplysning (f.eks. hvilke telefonnumre der har været sat i forbindelse med et bestemt telefonnummer), udvidet teleoplysning (f.eks. masteoplysninger), brevåbning og brevstandsning.

Bestemmelsen definerer begreberne som følger:

§ 780. Politiet kan efter reglerne i dette kapitel foretage indgreb i meddelelseshemmeligheden ved at

- 1) aflytte telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning),
- 2) aflytte andre samtaler eller udtalelser ved hjælp af et apparat (anden aflytning),
- 3) indhente oplysning 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),
- 4) 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),
- 5) tilbageholde, åbne og gøre sig bekendt med indholdet af breve, telegrammer og andre forsendelser (brevåbning) og
- 6) standse den videre befordring af forsendelser som nævnt i nr. 5 (brevstandsning).

Stk. 2. Politiet kan foretage optagelser eller tage kopier af de samtaler, udtalelser, forsendelser m.v., som er nævnt i stk. 1, i samme omfang som politiet er berettiget til at gøre sig bekendt med indholdet heraf.

Aflytning:

På baggrund af Retsplejelovens § 780, stk. 1, nr. 1, forstås aflytning således:

Telefonaflytning

”aflytte telefonsamtaler eller anden tilsvarende telekommunikation”

Begrebet er desuden beskrevet i den tværministerielle arbejdsgruppes rapport, der ligger til grund for regeringens handlingsplan for terrorbekæmpelse:

”Telefonaflytning

Det følger af retsplejelovens § 780, stk. 1, nr. 1, at der ved telefonaflytning er tale om aflytning af telefonsamtaler eller anden tilsvarende telekommunikation. Det vil først og fremmest sige aflytning af samtaler på fastledningsnettet og mobiltelefonnettet. For så vidt angår anden tilsvarende telekommunikation er der typisk tale om telefax, SMS, e-mail, Internet, voice-over IP, mv.

Det bemærkes, at kommunikation, der ikke føres over det offentlige net, ikke er omfattet af bestemmelserne om telefonaflytning, og aflytning heraf kan derfor foretages uden retskendelse. Det vil sige, at politiet kan foretage aflytning af egentlig radiokommunikation uden forudgående retskendelse. Det kan f.eks. være en skibsradio eller walkie-talkies.”

Teleoplysning

På baggrund af Retsplejelovens § 780, stk. 1, nr. 3, forstås teleoplysning således:

”indhente oplysning 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”

Udvidet teleoplysning

På baggrund af Retsplejelovens § 780, stk. 1, nr. 4, forstås udvidet teleoplysning således:

”indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater”

Begreberne ’teleoplysning’ og ’udvidet teleoplysning’ er desuden beskrevet i den tværministerielle arbejdsgruppes rapport, der ligger til grund for regeringens handlingsplan for terrorbekæmpelse:

Teleoplysning og udvidet teleoplysning

Ved teleoplysning forstås oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes (eller har været sat) i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil.

Tilladelse til at indhente teleoplysninger kan ske såvel fremadrettet som bagudrettet (historiske teleoplysninger).

Ved udvidet teleoplysning forstås oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater, dvs. oplysning om, hvilke mobiltelefoner der i et givet tidsrum har benyttet sig af en bestemt sendemast.

Retsplejelovens § 780, stk. 1, nr. 3 og 4, giver alene politiet adgang til at indhente oplysninger vedrørende trafikdata i forbindelse med telekommunikation og omfatter således ikke selve indholdet af kommunikationen.

Det bemærkes, at hvis der foreligger samtykke fra telefonens indehaver, anses indhentelse af oplysninger ikke for et indgreb i meddelelseshemmeligheden.

Masteoplysning

Ved masteoplysning forstås udvidet teleoplysning jf. ovenfor.

Udbydere af elektroniske kommunikationsnet- og tjenester

Udbydere af elektroniske kommunikationsnet og –tjenester er defineret i lov om konkurrence- og forbrugerforhold på telemarkedet, § 6, stk. 1.

”Ved udbydere af elektroniske kommunikationsnet og –tjenester til slutbrugere forstås i denne lov parter, som på kommercielt grundlag stiller net og tjenester som nævnt i § 3, stk. 1. og 2 til rådighed for flere slutbrugere.”

I bemærkningerne til loven er begrebet uddybet:

Til § 6

Denne bestemmelse omhandler udbydere af telenet eller teletjenester til slutbrugere.

Stk. 1 og 2 svarer til § 5, stk. 1 og 2, idet der dog er tale om underkategorier af de heri nævnte parter. § 6, stk. 1 og 2, afgrænser således udbydere af telenet eller teletjenester til slutbrugere i forhold til udbydere, der f.eks. alene udbyder telenet eller teletjenester i form af samtrafikprodukter til andre udbydere af telenet eller teletjenester. Afgrænsningen af denne gruppe er af betydning for afgrænsningen af, hvilke selskaber der er omfattet af dele af lovforslaget, der omhandler sikring af slutbrugernes rettigheder (forbrugerbeskyttelse) og bestemmelserne om, hvilke selskaber der kan udpeges som forsyningspligtudbydere.

Som det fremgår af bemærkningerne til § 4, defineres slutbrugere i modsætning til udbydere af telenet eller teletjenester, og formålet hermed er bl.a. at afgrænse, hvilke parter, der er forpligtede til at overholde de af lovens bestemmelser, der har et forbrugerbeskyttende sigte og omhandler udbud, og dermed udbydere, af telenet eller teletjenester til slutbrugere.

På tværs af denne kategorisering er der imidlertid også i loven nogle få, afgrænsede bestemmelser med forbrugerbeskyttende sigte (§§ 9 og 13, om hemmeligholdelse af telekommunikation og sikring af adgang til at foretage opkald til 112 og lignende), der ikke alene forpligter udbydere af telenet eller teletjenester til slutbrugere, men tillige slutbrugere, der samtidig er ejere af telenet, men som ikke foretager kommercielt udbud af tjenester.

Sigtet er at sikre, at de pågældende helt grundlæggende forbrugerbeskyttende regler også overholdes, hvor der er tale om, at en slutbruger eller en kreds af slutbrugere har besluttet at etablere et lokalt telenet til eget brug, og dermed selv bliver ejere af deres telenet. Der vil således i denne situation ikke være nogen kommerciel udbyder, der kan forpligtes til at overholde de pågældende regler.

De bestemmelser, der også retter sig til ejere af telenet, omfatter også ejere af såkaldte »interne net«, der er etableret »bag ved« det eller de pågældende abonnentnumre, herunder eksempelvis et internt tele- og omstillingsanlæg mellem flere geografisk adskilte filialer af en virksomhed.

Bilag 6.2.

Redegørelse for arbejdsgruppens arbejde

Mødeplan:

Den tekniske arbejdsgruppes møderække startede i december 2005, og gruppen har i løbet af december og januar holdt ugentlige møder.

Der har i alt været holdt 8 møder.

Gruppens første afrapportering vedrører 4 anbefalinger fra "Regeringens handlingsplan for terrorbekæmpelse". Gruppen skal i løbet af foråret 2006 genoptage møderækken med henblik på teknisk afklaring af yderligere 2 anbefalinger.

Deltagere:

TI:	Ib Tolstrup
ITEK:	John Kristensen
IT-B:	Jane Eis Larsen
TeliaSonera:	Camilla Nazareth Jens Ottosen-Støtt Helene Askholt
Sonofon:	Lotte Abildgaard Morten Tarp
TDC:	Mogens Ritsholm Marianne Legare Holm Hans-Ole Plough Henrik H. Olsen Carsten Hviid
3:	Ann-Louise Hansen Trine Alberts Mikael Pettersson
IBM:	John E. Schou Claus Samuelson Michael Dahl
Cybercity:	Nicholai Pfeiffer
Justitsministeriet:	Mette Lyster Knudsen Tomas Frydenberg
PET:	Peter Hindsberger Jørgen Isalin Kim B. Larsen
ITST:	Jette Plenge Jakobsen Bente Forslund Annette Nielsen Cecile Christensen Henry Galle Stech
Videnskabsministeriet:	Sune Rahn Kristina Tranders Griet Storr-Hansen

Bilag 6.3

Skøn over omkostninger i tilknytning til foreslået ændring af § 15 i teleloven (31. januar 2006)

Telekommunikationsindustrien (TI) har efter anmodning fra VTU-ministeriet torsdag den 19. januar 2006 med svarfrist torsdag den 26. januar 2006 gennemført et skøn over involverede omkostninger til gennemførelse af udvidet pligt til aflytning og pligt til logning af historiske data. Skønnet er gennemført på basis af de involverede virksomheders vurderinger af egne forhold, og der er på basis heraf foretaget en samlet vurdering for branchen.

Gennemgangen har vist, at omkostningerne for den enkelte virksomhed kan overstige de tilsvarende gennemsnitlige omkostninger for branchen, og der kan for enkeltelementer være højst varierende forudsætninger afhængigt af valgte produktionsmetoder, størrelse og egenskaber i de anvendte efterbehandlingssystemer.

Henset til disse forhold og det foreliggende uafklarede grundlag for fremtidige specifikke krav – herunder især krav til logning af trafikdata mv. – er det derfor fundet misvisende at udspecificere skønnene yderligere.

Skønnene er således foretaget ud fra den forudsætning, at foreliggende forslag til regler gennemføres med de respektive tilkendegivne hovedsigter med samtidig respekt af afvigelser og undtagelser, som hensynet til en sammenhængende proportionalitet for gennemførelsen tilsiger. Det er således forudsat, at kravene ikke på enkeltområder gennemføres på en sådan måde, at de fysisk eller økonomisk er til hinder for anvendelse af eksisterende og forudsete produktionsmetoder – herunder net af særlige typer.

Udvidelse af krav til aflytning.

TI skønner, at omkostninger til sikring af aflytningsmuligheder for telefonitjenester, der ikke udbydes via centraler, og en udvidelse til sikring af aflytningsmulighed af kunders samlede datatrafik via enkelttilslutninger (bruttodatastrømmen) vil udgøre i størrelsesorden 50-100 mio. kr. Dette skøn omfatter ikke etablering af centraler eller lignende begrundet af andre anbefalinger i Regeringens handlingsplan. Det er efter det tidligere nævnte generelle princip forudsat, at de konkrete krav til aflytningen tilpasses hensigtsmæssigt for små udbydere. Det er ligeledes forudsat, at levering af fremadrettede teleoplysninger omfatter data, som den afgivende udbyder hidtil har udleveret i forbindelse med en aflytning, mens f.eks. data der indgår i en aflytning/monitorering af bruttodatastrømmen ikke sorteres eller dekrypteres af udbyderen. De angivne beløb indeholder ikke omkostninger hos politiet til opgradering af modtagekapacitet.

Det er samtidigt TI's vurdering, at en udvidelse af aflytningsmulighederne efter nævnte principper vil være på linie med fremtidige krav i andre lande. Hvis dette ikke bliver tilfældet vil meromkostningerne til sikring af aflytning også på længere sigt udgøre en væsentlig økonomisk byrde..

Gennemførelse af krav om logning i henhold til kommende EU-direktivs krav.

TI skønner, at en gennemførelse af logningsdirektivets krav tilpasset en kommende europæisk norm herfor vil udløse omkostninger til telenet og supportsystemer herfor på 100-500 millioner kr. inklusive omkostninger til sikring af hurtig levering af registrerede data. Det er herved forudsat, at logningskravet respekterer direktivets princip om afgrænsning til trafikdata for afgivende udbydere.

Den i skønnet angivne usikkerhed beror på usikkerhed om den kommende europæiske norm. Endvidere er omkostningerne til hurtig adgang til registrerede data inklusive "friske" data stærkt afhængige af de specifikke kravs udformning – herunder sikring af disse data og driftskrav.

Det er samtidigt TI's vurdering, at gennemførelse efter europæisk norm på sigt vil sikre tilgængelighed af udstyr med de nødvendige egenskaber, hvorved meromkostningerne ved logning vil reduceres for fremtidige systemer.

Gennemførelse af krav om logning i henhold til foreliggende bekendtgørelsesudkast.

TI skønner, at gennemførelse af foreliggende udkast til bekendtgørelse kan afføde omkostninger på 1-2 mia. kr. Den væsentligste merudgift i forhold til direktivet beror på kravet om en generel logning af kundernes adfærd på nettet i form af logning af besøgte URL-adresser og benyttede IP-tjenester. Dette indebærer, at de uforholdsmæssige store omkostninger vil kunne ramme særlig hårdt i forhold til rene internetudbydere. Hertil kommer usikkerhed om den praktiske gennemførlighed af krav om logning af alle mastepositioner under en kommunikation, logning af MAC-adresser og logning af data for e-mail. Med udgangspunkt i eksisterende systemer har det ikke været muligt for alle udbydere at forudse løsninger, der kan opfylde kravene som beskrevet i udkastet. TI forventer, at disse forhold kan blive nøjere afklaret, når en konkret drøftelse heraf gennemføres i Justitsministeriets ekspertgruppe.

Det er samtidigt TI's vurdering, at gennemførelse efter foreliggende udkast til bekendtgørelse vil begrænse og fordyre valgmulighederne for fremtidige anskaffelser af teleudstyr, idet det ikke er TI's forventning, at tilsvarende krav vil blive lagt til grund for logningspligten i andre lande. De relative meromkostninger vil derfor næppe kunne reduceres i samme grad som tilfældet vil være, hvis kravene tilpasses europæisk norm.