Justitsministeriet
Civil- og Politiafdelingen

RETSUDVALGET
Alm. del - bilag 1194 (offentligt)

ORIGINAL

Folketinget
Retsudvalget
Christiansborg
1240 København K.

MODTAGET
- 1 OKT. 2004 //
55

Den Centrale Indlevering

Dato: 30 SEP. 2004
Kontor: Politikontoret
Sagsnr.: 2002-945-0922
Dok.: RBL21016
+ bilag

Afsendt med
E-Post 30/9-04

Vedlagt fremsendes i 5 eksemplarer en oversigt over høringssvar vedrørende udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Justitsministeriet har den 10. juni 2004 tilsendt Retsudvalget kopi af de modtagne høringssvar.

Justitsministeriet kan i forbindelse hermed oplyse, at Frankrig, Irland, Sverige og Storbritannien den 28. april 2004 over for Det Europæiske Råd har fremlagt et forslag til rammeafgørelse om opbevaring af data, der behandles og lagres i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester og af data, der findes i offentligt tilgængelige kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme (dok.nr. 8958/04 CRIMORG 36 TELECOM 82).

Justitsministeriet har den 3. august 2004 tilsendt Retsudvalget et grundnotat om udkastet til rammeafgørelse.

I bemærkningerne til udkastet til rammeafgørelse henvises der til den erklæring om bekæmpelse af terrorisme, som Det Europæiske Råd vedtog den 25. marts 2004, og som pålægger Rådet at behandle foranstaltninger vedrørende opstilling af regler for tjenesteudbyderes lagring af kommunikationsdata med henblik på vedtagelse inden juni 2005.

Slotsholmsgade 10
1216 København K

Telefon: 33 92 33 40
Telefax: 33 93 35 10

E-post: jm@jm.dk
Internet: http://www.jm.dk

Det hollandske formandskab har tilkendegivet, at man vil arbejde for at afslutte forhandlingerne inden årsskiftet 2004/2005.

I lyset af det nævnte initiativ til fælleseuropæiske regler samt tilkendegivelsen fra det hollandske formandskab, finder Justitsministeriet det rigtigst, at der ikke udstedes danske regler på området, før rammeafgørelsen enten er vedtaget, eller forhandlingerne har vist, at der ikke er udsigt til, at der på kortere sigt vil kunne opnås enighed i Rådet.

Justitsministeriet kan endvidere oplyse, at ministeriet den 21. september 2004 har afholdt et møde med bl.a. IT- og telebranchen vedrørende udkastet til regler om logning. Justitsministeriet har i forbindelse hermed besluttet at nedsætte en arbejdsgruppe – med deltagelse af repræsentanter fra IT- og telebranchen – med henblik på at gennemgå og vurdere behovet for ændringer af det foreliggende udkast til bekendtgørelse og vejledning.

Lene Espersen

Mette Lyster Knudsen

Justitsministeriet
Civil- og Politiafdelingen

Kontor: Politikontoret
Sagsnr.: 2002-945-0922
Dok.: RBL21055

OVERSIGT

over

høringssvar vedrørende udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

I. Hørte myndigheder og organisationer mv.

Et udkast til bekendtgørelsen har været sendt til høring hos:

Præsidenterne for Østre og Vestre Landsret, præsidenterne for Københavns Byret og for retterne i Odense, Århus, Ålborg og Roskilde, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Rigsadvokaten, Statsadvokaten for Særlige Internationale Straffesager, Statsadvokaten for Særlig Økonomisk Kriminalitet, samt statsadvokaterne for København mv., Sjælland, Fyn mv. samt statsadvokaterne i Ålborg, Sønderborg og Viborg, Rigspolitichefen (herunder Politiets Efterretningstjeneste), Politidirektøren i København, Foreningen af Politimestre i Danmark, Politifuldmægtigforeningen, Politiforbundet i Danmark, Datatilsynet, Beskæftigelsesministeriet, Erhvervs- og Boligstyrelsen, Økonomi- og Erhvervsministeriet, Finansministeriet, Forsvarsministeriet, Indenrigs- og Sundhedsministeriet, Kirkeministeriet, Kulturministeriet, Miljø- og Energiministeriet, Ministeriet for Flygtninge, Indvandrere og Integration, Ministeriet for Fødevarer, Landbrug og Fiskeri, Fødevareministeriets Rådgivende Forskningsudvalg, Skatteministeriet, Socialministeriet, Statsministeriet, Trafikministeriet, Udenrigsministeriet, Undervisningsministeriet, Økonomi- og Erhvervsministeriet, AB

Slotsholmsgade 10
1216 København K
Telefon: 33 92 33 40
Telefax: 33 93 35 10
E-post: jm@jm.dk
Internet: http://www.jm.dk

Stc. Kjeldsgården, ABF, Advokatrådet, ALBO, Amtsrådsforeningen i Danmark, Andelsboligforeningernes Fællesrepræsentation, Arrownet A/S, Banestyrelsen, Beredskabsstyrelsen, Boligsikringen, Boligselskabernes Landsforening, BOSAM, Brancheorganisationen for Forbruger Elektronik, Broadcom, Catpipe Systems ApS. - Xenux, Center for Teleinformation, Cybercity, Danmarks Lejerforeninger, Danmarks Radio, Dansk EL-Forbund, Dansk Elektronik, Dansk Fagpresse, Dansk Handel og Service, Dansk Industri, DANSK IT, Dansk Magasinpresse, Dansk Management Råd (DMR), Dansk Metal, Dansk Retspolitisik Forening, Dansk Standard, Danske Dagblades Forening, Danske Energiselskabers Forening, Danske Fagblade, Danske Telecom, DATEA, Debitel, Demokratisk Lokalstation, DGI (Danske Gymnastik og Idrætsforeninger), Digital Rights, DSB, DTU, Ejerlejlighedernes Landsforening, Ementor Danmark A/S, Equant, Erhvervs- og Selskabsstyrelsen, FAEM, FDA, Forbrugerrådet, Forbrugerstyrelsen, Forenede Danske Antenneanlæg, Foreningen af Danske InternetMedier (FDIM), Foreningen af Danske Lokale Ugeaviser, Foreningen for Dansk Internet Handel, Frederiksberg Kommune, GN Store Nord, Global Connect, Grundejernes Landsorganisation, Hi3G Denmark ApS, HORESTA, HTS Interesseorganisationen, IASTAR Danmark, IBM Danmark, IDA, Indienet, Institut for Menneskerettigheder, ISPA DK (Foreningen af Internetleverandører), ITEK, Dansk Industri, IT- og Telestyrelsen, IT-Brancheforeningen, Jydske Grundejerforeninger, Kabelnettet.dk, Klarup Antenneforening, Kommunernes Landsforening, KMD A/S, Komm, c/o Kanal 2, Kommuneinformation A/S, Konkurrencestyrelsen, Københavns Kommune, Københavns Universitet (Det Retsvidenskabelige Institut A), Landsforeningen af Beskikkede Advokater, Lejernes Landsorganisation, Landsorganisationen i Danmark, SuperTEL Danmark, Mobiltelebranchen, NIRAS, PROSA, Parcelhusejernes Landsforening, Powercom, Powerline Communications, Repræsentantskabet ved Tele Danmark Landsdelsrådet for Jylland, Roskilde Universitetscenter, Samarbejdsforum for Danske Lytter og Seerorganisationer, Sammenslutningen af Lokale Radio- og TV-stationer, Service Partner Sjælland, Skydebanenet, Sonofon A/S, Koncerndirektør Allan Koch, Stofa, Tele 2, Tele Danmarks Kunders Landsråd, Tele-Punkt Søborg A/S, Telekommunikationsindustrien, Telia A/S, TetraStar A/S, Tiscali Danmark, Transcom Danmark A/S, Webpartner, Syddansk Universitet, TDC, TEKNIQ, TELE Greenland A/S, TELMORE A/S, TV 2, TV3, WorldCOM, Aalborg Universitet og Århus Universitet.

Ud over fra de af Justitsministeriet hørte myndigheder, har ministeriet endvidere modtaget høringssvar fra en række andre organisationer mv.

II. Høringssvarene

Præsidenterne for Østre og Vestre Landsret, præsidenterne for Københavns Byret og for retterne i Aalborg, Århus, Odense og Roskilde, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Rigsadvokaten, Statsadvokaten for Fyn, Sydøstsjælland, Lolland, Falster og Bornholm, Statsadvokaten i Aalborg, Statsadvokaten i Viborg, Statsadvokaten i Sønderborg, Statsadvokaten for Særlig Økonomisk Kriminalitet, Statsadvokaten for Særlige Internationale Straffesager, Politidirektøren i København, Foreningen af Politimestre i Danmark, Beskæftigelsesministeriet, Forsvarsministeriet, Indenrigs- og Sundhedsministeriet, Kirkeministeriet, Ministeriet for Flygtninge, Indvandrere og Integration, Danmarks Meteorologiske Institut, IT- og Telestyrelsen, Forbrugerstyrelsen, Landsforeningen af Beskikkede Advokater, Dansk Retspolitisk Forening, Horesta, Ejendomsforeningen Danmark, Dansk Energi og Sammenslutningen af Lokale Radio- og TV-stationer, har ikke haft bemærkninger til udkastet til bekendtgørelse.

A. GENERELLE BEMÆRKNINGER

Statsadvokaten for Sjælland oplyser, at Politimesteren i Gladsaxe og Politimesteren i Holbæk har udtalt betænkeligheder ved bekendtgørelsesudkastets undtagelser, idet disse kan indebære en risiko for, at personer med et kriminelt sigte etablerer sig som udbydere i en foreningsform mv., som ikke er omfattet af logningspligten. Statsadvokaten er enig i disse betænkeligheder.

Statsadvokaten for København, Frederiksberg og Tårnby er enig i en udtalelse fra Politimesteren i Tårnby, der påpeger, at teleselskabernes takster for videregivelse af oplysninger om en stedfunden kommunikation i visse sager udgør en økonomisk byrde for politiet. Det bør derfor overvejes at indføre en bestemmelse om, at teleselskabernes takster eventuelt kan forelægges Konkurrencestyrelsen. Statsadvokaten kan i øvrigt tilslutte sig høringssvaret fra Statsadvokaten for Sjælland.

Datatilsynet finder det hensigtsmæssigt, at der – ved siden af den revisionsbestemmelse i ændringslovens § 8, hvorefter Justitsministeriet i folketingsåret 2005/2006 fremsætter forslag om revision af retsplejelovens § 786, stk. 4 – ligeledes indsættes en revisionsbestemmelse i bekendtgørelsen. Tilsynet ligger imidlertid til grund, at der også uden en sådan udtrykkelig revisionsbestemmelse vil blive foretaget de ændringer af bekendtgørelsen, som revisionen af § 786, stk. 4, nødvendiggør.

Red Barnet finder det tilfredsstillende, at der nu foreligger et udkast til bekendtgørelse, der nærmere fastlægger teleudbyderes pligt til at registrere og opbevare teletrafikdata. Det er Red Barnets opfattelse, at enhver form for seksuelt misbrug af børn, som manifesterer sig gennem distribution af børnepornografisk materiale, skal bekæmpes målrettet ved bl.a. effektive efterforskningsmidler.

Institut for Menneskerettigheder anfører, at der ved vurderingen af, om et indgreb i beskyttelsen af personoplysninger er legitimt, skal tages udgangspunkt i, at der skal opnås en rimelig balance mellem samfundsinteressen og den enkelte borgers interesse. I de tilfælde, hvor indgrebet er begrundet i hensynet til politiets og efterretningstjenestens efterforskningsmuligheder og beskyttelse af den nationale sikkerhed, har Den Europæiske Menneskerettighedsdomstol (EMD) accepteret indgrebet, hvis lovhjemlens kvalitet og præcision var i orden. EMD har dog fremhævet, at kravene til de retssikkerhedsgarantier, der skal sikre mod misbrug og vilkårlig anvendelse af overvågning, er skærpet i forbindelse med indgreb, der foretages som led i efterretningstjeneste. EMD har endvidere understreget menneskerettens princip om proportionalitet.

I afvejningen mellem indgrebets omfang og dets effektivitet, finder Instituttet det hverken proportionalt eller effektivt, at logningspligten fritager en række aktører, herunder f.eks. skoler, biblioteker samt boligforeninger med under 100 beboere. Det vil således ikke være vanskeligt for kriminelle at undgå logning, mens en stor gruppe tilfældige borgere fremover vil få registreret og opbevaret oplysninger om deres elektroniske færden.

Økonomi- og Erhvervsministeriet har anmodet Konkurrencestyrelsen, Forbrugerstyrelsen og Erhvervs- og Selskabsstyrelsen om en udtalelse vedrørende udkastet til bekendtgørelse og vejledning. På baggrund af disse udtalelser er det Økonomi- og Erhvervsministeriets opfattelse, at reglerne vil medføre store administrative byrder for telenet- og teletjenesteudbydere. Erhvervs- og Selskabsstyrelsen, Center for Kvalitet i Erhvervsregulering (CKR), har rettet henvendelse til TDC med henblik på en vurdering af, hvilke dele af bekendtgørelsesudkastet der vil indebære de største byrder for erhvervet. På baggrund heraf vurderer Erhvervs- og Selskabsstyrelsen, at de største byrder består af telenet- og teletjenesteudbyderes registrerings- og opbevaringspligt og pligten til at etablere et døgnbetjent kontaktpunkt. Erhvervs- og Selskabsstyrelsen anbefaler, at bekendtgørelsesudkastet forelægges for et af Økonomi- og Erhvervsministeriets virksomhedspaneler, der kan fastlægge byrdens størrelse og eventuelt foreslå, hvordan byrden kan lettes. Derudover anbefaler Erhvervs- og Selskabsstyrelsen, at udbyderne modtager grundig information om den nye regler og tilbydes hjælp til at opfylde bestemmelserne.

Københavns Universitet, Det Juridiske Fakultet, professor Mads Bryde Andersen, anfører, at den valgte regulering, hvorefter bekendtgørelsesudkastets § 2 fastsætter den bredt formulerede hovedregel og § 3 nogle nærmere præciserede undtagelser, indebærer en risiko for, at man for det første får for meget med i hovedreglen og for det andet rammer skævt i reguleringen af undtagelserne. Begge dele er efter professor Mads Bryde Andersens opfattelse tilfældet med det foreliggende udkast til bekendtgørelse. For så vidt angår hovedreglen i § 2, er det uafklaret, om privatpersoner, der uden vederlag stiller telenet eller teletjenester til rådighed for en *ikke* afgrænset kreds af slutbrugere, er omfattet af logningspligten. Ordlyden tyder på, at dette er tilfældet, og reglen får da den konsekvens, at de talrige hjem, hvor der er installeret trådløse netværk i forbindelse med en ADSL-forbindelse, men som har valgt ikke at indbygge en adgangskontrolmekanisme i den forbindelse, vil være omfattet af registreringspligten. Denne konsekvens synes der ikke at være taget højde for i udkastet til bekendtgørelse og vejledning. For så vidt angår undtagelsesbestemmelsen, er det for så vidt sympatisk, at mindre private foreninger søges holdt ude af reguleringen. Afgrænsningen (bl.a. maksimumgrænsen på 100 slutbrugere) forekommer dog vanskeligt forståelig, da risikoen for, at en terrorist kommunikerer via en lille andelsboligforening er ligeså stor som risikoen for, at den pågældende gør det via en større andelsboligforening. Professor Mads Bryde Andersen erkender, at det er et vanskeligt afvejningsproblem, men foreslår, at problemet løses ved, at man på bekendtgørelsesniveau udpeger forskellige typer af teleudbydere mv., hvortil der knyttes forskellige registreringsforpligtelser. Det er f.eks. åbenbart, at teleoperatører, der befinder sig på det centrale niveau af telenettet (f.eks. Backbone Internet-leverandører) bør være underkastet en mere intens pligt til at logge teleoplysninger i realtid, hvorimod en sådan pligt måske kan nedtones (uden nødvendigvis at skulle bortfalde helt) for mindre teleudbydere og private teleudbydere. For så vidt angår udkastet til vejledning, er man efter professor Mads Bryde Andersens opfattelse meget langt fra en detaljeringsgrad og et sprog, som vil være til hjælp for ikke-professionelle praktikere.

IT-Brancheforeningen finder, at udkastet til bekendtgørelse og vejledning giver anledning til en række principielle betænkeligheder vedrørende såvel hjemmelsgrundlag som reguleringsomfang, herunder vedrørende forsvarligheden af at pålægge en så bred og forskelligartet kreds af selskaber pligt til løbende at registrere og opbevare en række stærkt følsomme nye former for data, som disse virksomheder ellers ikke ville have registreret eller opbevaret. Samtidig er der i branchen en voksende bekymring over, at den valgte implementering af terrorlovgivningen kan få fatale konsekvenser for digitaliseringen af det danske samfund. Der skal være en fornuftig balance mellem initiativer og regler, der muliggør bekæmpelse af terrorisme, og fremme af et digitaliseret, moderne og dermed konkurrencedygtigt videnssamfund. Brancheforeningen mener ikke, at denne balance er til stede i de fremlagte udkast. Brancheforeningen lægger i den

forbindelse vægt på, at især mindre udbydere vil opleve så massive ekstraomkostninger, at det kraftigt vil påvirke deres forretningsgrundlag og overlevelsesmuligheder. Hertil kommer, at der er tale om en rent dansk regulering, der ikke er koordineret med indsatsen i de øvrige EU-lande. Ligeledes er der en række forhold, der er uklare og ufuldstændigt behandlet og beskrevet. Brancheforeningen finder det endvidere beklageligt, at det ikke har været muligt allerede i høringsperioden at få afholdt et møde om udkastenes indhold og forståelsen af disse, og bemærker i den forbindelse, at det fremgår af lovbemærkningerne til retsplejelovens § 786, at reguleringen vil blive gennemført efter dialog med branchen. Brancheforeningen gør desuden opmærksom på, at indførelsen af de nye regler blot vil få personer med kriminelle hensigter til at vælge kommunikationsløsninger, der ikke kan logges. Da der i øvrigt forventes et EU-initiativ på området, foreslår Brancheforeningen, at logningspligten indtil videre begrænses til at omfatte pligt til opbevaring i 1 år af de trafikdata, der allerede logges. For at sætte ovennævnte i perspektiv har Brancheforeningen i samarbejde med branchen foretaget en foreløbig vurdering af de omkostninger, som vil være forbundet med logningspligten for en større outsourcing- og drift-leverandør. Det er vurderingen, at initialomkostningen ved at etablere de nødvendige faciliteter formentlig ville andrage ca. 18 mio. kr. Hertil kommer udgifter til løbende vedligeholdelse, opdatering mv., som skønnes at udgøre ca. 8 mio. kr. Brancheforeningen opfordrer til, at der snarest efter høringsfristens udløb gennemføres en møderække med de involverede brancheorganisationer med henblik på dels at drøfte de principielle spørgsmål, som udkastet til reglerne rejser, og dels at diskutere det praktisk-operationelle indhold af bekendtgørelsen. Samtidig bør der som led i møderækken fastlægges en tidsplan for gennemførelse af de nye danske regler, der sikrer koordinering med de kommende EU-regler. Møderækken bør gøres til et permanent samarbejdsforum for drøftelser mellem Justitsministeriet og IT- og telebranchen om den løbende tilpasning af bekendtgørelsen og vejledningen.

Handel, Transport og Serviceerhvervene, Orange A/S og **KMD A/S** tilslutter sig høringssvaret fra IT-Brancheforeningen.

Telekommunikationsindustrien i Danmark (TI) og **Cybercity** anfører, at udviklingen inden for telesektoren går særdeles hurtigt, og at det derfor er betænkeligt, at et meget omfattende logningskrav baseres på en betænkning, der er udarbejdet godt 7 år før udmøntningen af de foreslåede krav.

TI anfører endvidere, at udkastet til bekendtgørelse og vejledning er overraskende vidtgående, da det forpligter udbydere til at registrere og opbevare data om alle kunders trafik, selv om disse data slet ikke i dag registreres af de omfattede udbydere. Teleudbyderne skal således ikke alene undlade at slette eksisterende data for at kunne hjælpe politiet, men opsamle nye data,

der alene er af eventuel interesse for politiet. Dermed varetager udbyderne reelt egentlige overvågningsopgaver af hele befolkningen for politiet.

Udkastet går efter TI's opfattelse også på andre punkter langt ud over hjemmelsgrundlaget. Endvidere tager udkastet ikke højde for den praktiske rækkevidde af kravene for nye markeder med nye typer af tjenester. Dette medfører for disse tjenester betydelig usikkerhed i forhold til anvendelige produktionsmetoder og de omkostninger, der må indkalkuleres som følge af logningspligten.

Endvidere vil reglerne ifølge TI kun have begrænset efterforskningsmæssig værdi, idet de foreslåede undtagelser samt mulighederne for bevidst at undgå registrering vil betyde, at der i praksis kun vil ske registrering af en begrænset del af den samlede datatrafik.

TI finder desuden, at udkastet til bekendtgørelse og vejledning på flere punkter – eksempelvis i relation til Internet – er vanskelige at tolke i forhold til de i dag anvendte produktionsmetoder, og udkastet til regler rejser en række spørgsmål, som nødvendigvis må opklares, vurderes og udmøntes i nye tekniske krav til systemerne, hvis reglerne skal forsøges gennemført.

TI og Cybercity finder det endvidere meget betænkeligt, at den strafsanktionerede forpligtelse til at registrere og opbevare trafikdata, som nu indføres, i vidt omfang alene kan læses i vejledningen til bekendtgørelsen. Alle forpligtende krav – herunder bl.a. præcis og udtømmende angivelse af, hvilke data der skal registreres, og hvilke oplysninger politiet skal have udleveret – bør i stedet klart og tydeligt fremgå direkte af bekendtgørelsen.

Herudover finder TI og Cybercity ikke, at der – som forudsat i bemærkningerne til anti-terror lovforslaget – har været den fornødne dialog mellem Justitsministeriet og tele- og Internetudbyderne. Justitsministeriet har således ikke siden et møde i ministeriet den 19. december 2002 mellem Telekommunikationsindustrien og de involverede myndigheder, taget initiativ til at inddrage branchen yderligere.

På den nævnte baggrund finder TI og Cybercity det ikke muligt at gennemføre det foreliggende udkast til bekendtgørelse inden den 1. juli 2005. Det foreslås i stedet, at bekendtgørelsen udformes således, at udbyderne alene forpligtes til at opbevare allerede registrerede data i 1 år, hvorved hovedformålet med retsplejelovens bestemmelse opfyldes.

TI og Cybercity foreslår samtidig, at der iværksættes et udredningsarbejde med henblik på reglernes videre udvikling i lyset af en eventuel gennemførelse af fælleseuropæiske regler på området.

ITEK (Dansk Industris branchefællesskab for IT, elektronik og telekommunikation) anfører, at den mest effektive indsats i bekæmpelse af terrorisme opnås gennem etablering af et tæt og konstruktivt samarbejde mellem de relevante myndigheder og industrien og ikke gennem restriktive lovreguleringer. Samtidig bør de danske initiativer nøje koordineres med de øvrige EU-lande. Hvis der skal ske en regulering af området, anser ITEK det for væsentligt, at tiltagene i praksis opfylder formålet med reguleringen, at reguleringen er specifik, teknisk gennemførlig og i øvrigt harmonerer med lovgivningen på teleområdet og med den internationale udvikling. Reguleringen bør endvidere stille alle udbydere lige (såvel private som offentlige), reguleringen skal være gennemskuelig, ikke-diskriminerende og proportional, og den må ikke pålægge udbyderne en unødvendig økonomisk byrde. Reguleringen skal endvidere respektere persondatalovgivningen og må ikke skabe unødvendig usikkerhed om omfanget af logningsforpligtelsen, og den må ikke kunne omgås. Det foreliggende udkast til bekendtgørelse og vejledning opfylder efter ITEK's opfattelse ikke disse krav. ITEK finder det dybt beklageligt, at Justitsministeriet har været afvisende over for en dialog med branchen om de nævnte spørgsmål, og opfordrer til, at ministeriet snarest efter høringsfristens udløb indkalder til et møde om sagen. ITEK fremhæver endvidere, at den omfattende regulering, som der lægges op til i udkastet til bekendtgørelse og vejledning formentlig går videre, end hvad der har været hensigten med den tilgrundliggende ændring af retsplejeloven. Hertil kommer, at en væsentlig del af reguleringen kun er beskrevet i vejledningen til bekendtgørelsen. ITEK kan i øvrigt tilslutte sig høringssvaret fra Telekommunikationsindustrien i Danmark.

TDC henviser til, at selskabets bemærkninger fremgår af høringssvaret fra Telekommunikationsindustrien i Danmark.

Digital Rights anfører, at udkastet til bekendtgørelse etablerer en omfattende registrering af borgerne i Danmark, som udgør et alvorligt indgreb i den enkelte borgers privatliv og medfører betydelig risiko for, at oplysninger om borgerens personlige forhold misbruges eller kommer i uvedkommendes hænder. Samtidig stiller Digital Rights sig tvivlende over for den reelle efterforskningsmæssige effekt af bekendtgørelsen, da en række betydelige udbydere af teletjenester ikke er omfattet, ligesom en række tekniske alternativer til de omfattede tjenester ikke vil blive underlagt registrering. Udkastet til bekendtgørelse indebærer bl.a., at udbydere af e-mail tjenester skal registrere afsender- og modtageradresse på al e-mail sendt af alle brugere. Det svarer til, at postvæsenet blev pålagt at registrere modtager- og afsenderadresse på alle

breve sendt i Danmark, eller at viceværten i boligforeningen blev pålagt systematisk at registrere, hvem beboerne udveksler breve med. Registreringspligten går dog langt videre, idet mængden af udvekslet e-mail typisk er mange gange større end mængden af almindelige breve. En registrering af afsendte og modtagne e-mail vil dermed på en langt mere præcis måde kortlægge borgerens kommunikationsmønster. I takt med, at elektronisk kommunikation udbredes i samfundet, vil registreringen således også omfatte data, som kan afsløre helt private forhold omkring borgeren, f.eks. kommunikation med politiske partier, læger eller religiøse foreninger. På den nævnte baggrund finder Digital Rights, at bekendtgørelsen udgør et uproportionalt indgreb i borgernes privatliv, hvor den positive efterforskningsmæssige effekt ikke står mål med indgrebet i borgernes personlige frihed. Digital Rights opfordrer derfor til, at bekendtgørelsen trækkes tilbage, og at lovhjemmelen til at pålægge teleudbydere registrering af trafikdata implementeres på en væsentlig mindre indgribende måde.

Dansk IT betragter udkastet til bekendtgørelse som et markant skifte i retstilstanden, der gør det afgørende, at alle principielle aspekter er grundigt belyst. Det er derfor en mangel, at der ikke er udarbejdet en redegørelse om reglernes forventede effekt og omkostninger. Bekendtgørelsesudkastet indebærer en pligt for udbyderne til at registrere og opbevare enorme datamængder, hvilket vil medføre store omkostninger for den enkelte udbyder. På den anden side indeholder udkastet en så lang række undtagelser fra logningspligten, at reglerne næppe vil få større betydning for efterforskningen.

Banedanmark, der sælger begrænsede teleydelser primært til DSB i form af intern telefoni for medarbejderne, anfører, at Banedanmark som offentlig virksomhed, der udbyder telefoni på kommercielle vilkår, vil være omfattet af bekendtgørelsens logningspligt. Dette vil medføre større omkostninger for virksomheden - herunder til et døgnbetjent kontaktpunkt - der vil kunne få som konsekvens, at Banedanmark ikke længere kan udbyde ydelsen til DSB, medmindre der gives mulighed for dispensation.

Catpipe Systems anfører, at man anser udkastet til bekendtgørelse og vejledning for en klar udvidelse af de gældende regler, der vil indebære, at politiet rutinemæssigt vil forlange udskrift af kontakt-filen i forbindelse med efterforskningen af enhver sag, der implicerer mere end én gerningsperson.

Andelsboligforeningens Fællesrepræsentation (ABF) anfører, at det ikke fremgår tilstrækkelig klart af bekendtgørelsesudkastet, hvilke krav der stilles til andelsboligforeninger med hensyn til logning. ABF finder det således f.eks. ikke klart, hvad det konkret indebærer, at der skal etableres et døgnbetjent kontaktpunkt.

ABF fremhæver, at bekendtgørelsesudkastet medfører nogle forpligtelser for andelsboligforeninger, som indebærer øgede omkostninger, og som vil besværliggøre driften af de fælles netværk, som typisk drives af frivillige, der ikke nødvendigvis besidder ekspertisen til at håndtere bekendtgørelsens krav. Da hensynet til at bekæmpe terror og anden kriminalitet, som pligten til at registrere og opbevare teletrafikdata skal varetage, må anses for en samfundsmæssig opgave, finder ABF, at andelsboligforeningerne bør kompenseres for de øgede udgifter, som de nye regler vil indebære, herunder i hvert fald kompensation for etablerings- og driftsomkostninger.

ABF bemærker endvidere, at pligten til at foretage registrering og opbevaring af teletrafik mv., efter al sandsynlighed vil medføre, at arbejdet med at etablere og drive lokale netværk vil forekomme så ressourcekrævende, at ingen frivillige vil ønske at gå ind i dette arbejde.

Herudover finder ABF det meget ubehageligt, at foreningerne skal registrere oplysninger om beboernes brug af Internet og telefoni.

For så vidt angår den mere tekniske del af udkastet til bekendtgørelse og vejledning, tilslutter ABF sig høringssvaret fra Bolignetforeningen.

Bolignetforeningen anfører, at den politimæssige betydning af bekendtgørelsen vil blive marginal, men at konsekvenserne for bolignetforeningerne vil blive meget alvorlige. Bekendtgørelsesudkastet pålægger således bolignetforeninger og televirksomheder betragtelige meromkostninger til udførelse af en samfundsmæssig opgave. Hertil kommer, at bekendtgørelsen gennemgående er så uklart formuleret, at systemadministratorer ikke vil kunne være sikre på, om de overholder reglerne. Bekendtgørelsesudkastet lægger for det første op til at sikre, at der sker opbevaring i et år af de trafikdata, der allerede registreres. Herudover lægger udkastet imidlertid også op til, at der skal ske registrering og opbevaring af visse specifikke data, der i dag typisk ikke registreres. Disse data er ikke nødvendige for produktion af tjenesteydelsen, men vil alene skulle registreres og opbevares af hensyn til politiet. Da teleloven og persondataloven pålægger udbyderne at slette data, der ikke er omfattet af logningspligten, bør bekendtgørelsen klart definere, præcis hvilke oplysninger udbyderne har pligt til registrere og opbevare. Definitionerne i bekendtgørelsesudkastet - navnlig begreberne vedrørende datatransmission - er imidlertid meget uklare. På den anden side vil en meget præcis definition indebære, at bekendtgørelsen hurtigt vil blive utidssvarende. På den baggrund finder Bolignetforeningen, at bekendtgørelsen bør begrænses til alene at fastsætte en pligt for udbydere til at opbevare de trafikdata, der allerede registreres. Dette vil samtidig indebære, at bekendtgørelsen vil være

teknologineutral, ligesom omkostningerne for udbyderne vil være acceptable. Hvis der er politisk ønske om at udvide logningspligten, foreslår Bolignetforeningen, at der nedsættes et arbejdsudvalg med repræsentanter fra aktørerne, så det kan sikres, at kravene er juridisk entydige og teknisk gennemførlige.

Boligselskabernes Landsforening påpeger, at gennemførelse af udkastet til bekendtgørelse vil medføre en meget omfattende registrering, som sandsynligvis ikke vil blive opvejet af tilstrækkeligt gode efterforskningsmæssige resultater. Det er uklart, hvem der efter bekendtgørelsesudkastet er ansvarlig for, at registreringen finder sted, og de mange boligforeninger, frivillige bestyrelsesmedlemmer m.fl. efterlades derfor i et juridisk tomrum. Endvidere finder Landsforeningen det betænkeligt, at alle borgeres elektroniske kommunikation skal opbevares i 1 år af private virksomheder og foreninger. Der er desuden uafklarede spørgsmål i forhold til persondatalovgivningen, som ikke uden videre tillader videregivelse til politiet af borgernes elektroniske og telefoni-baserede kommunikation.

Netudvalget, Kollegiet Studentergården, mener, at bekendtgørelsesudkastet vil få væsentlige negative konsekvenser for de mindre teleudbydere samt boligforeninger og antennelav, hvilket vil medføre en uhensigtsmæssig konkurrenceforvridning. Omkostningerne står endvidere ikke mål med sandsynligheden for, at de registrerede oplysninger vil få efterforskningsmæssig værdi.

Digital Forbruger Danmark (DFD) finder, at bekendtgørelsesudkastet repræsenterer en uhørt krænkelse af borgernes privatliv. DFD peger i den forbindelse navnlig på 4 problemstillinger: 1) bekendtgørelsen betragter Internettets brugere som passive, 2) den giver grobund for utryghed og mistro, 3) den indebærer en økonomisk byrde og vil begrænse de mange positive aktiviteter, samt at 4) den er uigennemtænkt og virkningsløs. DFD anbefaler på den baggrund, at bekendtgørelsen trækkes tilbage.

Frederiksberg Kommune anmoder Justitsministeriet om at vurdere, hvordan bestemmelserne i lov om biblioteksvirksomhed, hvorefter bibliotekernes PC'er med Internetadgang skal stå til rådighed for enhver, harmonerer med de foreslåede regler.

Danske Mediers Forum tilslutter sig, at der i kølvandet på de seneste års terrorhandlinger kan være behov for at tage visse forholdsregler med henblik på at fremme efterforskningsmuligheder og forebyggelse. Sammenslutningen finder dog, at bekendtgørelsesudkastet indeholder nogle stærkt problematiske aspekter, som er uforholdsmæssigt vidtgående, og som vil have væsentlig indflydelse på danske mediers vilkår. Logningspligten indebærer ikke blot, at udbydere

skal foretage opbevaring af de trafikdata, som allerede registreres i dag, men pålægger udbyderne at registrere trafikdata i videre omfang. Logningspligten er særligt vidtgående i relation til mobiltelefoni, hvor bekendtgørelsesudkastet forpligter udbyderne til at registrere og opbevare lokaliseringsdata, dvs. oplysninger om brugerens geografiske position under det pågældende opkald. Sammenslutningen tager skarpt afstand fra en så vidtgående logningsforpligtelse, der i yderste konsekvens vil betyde, at politiet kan afdække journalisters færden, herunder eventuel kontakt med anonyme kilder. Af hensyn til kildebeskyttelsen finder sammenslutningen derfor, at registrering og opbevaring af trafikdata til og fra medierne bør undtages fra bekendtgørelsen, der ellers kan få alvorlige konsekvenser for pressefriheden. Sammenslutningen finder det betænkeligt, at hverken udkastet til bekendtgørelse eller vejledning inddrager kildebeskyttelsesreglerne, idet teleoplysninger er egnede til at fastslå identiteten af kilder, som journalisten har været i kontakt med, og som journalisten i medfør af retsplejelovens § 172 som udgangspunkt ikke er forpligtet til at afgive forklaring om. Hvis politiet ønsker oplysninger om kommunikationen mellem et medie og dets kontakter, er det nødvendigt, at det pågældende medie har ret til at udtale sig om spørgsmålet. Der bør på den baggrund - i lighed med reglerne om beslaglæggelse og edition - indføres en direkte henvisning i retsplejelovens kapitel 71 til hensynet til kildebeskyttelsen. Sammenslutningen finder i øvrigt, at kravene i udkastet til bekendtgørelse og vejledning om registrering og opbevaring af trafikdata af retssikkerhedsmæssige grunde i stedet bør fastsættes i retsplejeloven. Sammenslutningen kan herudover tilslutte sig forslaget fra Telekommunikationsindustrien i Danmark om, at der iværksættes et udredningsarbejde vedrørende reglerne, og man deltager meget gerne heri.

#depression.dk# - der er en selvhjælpsgruppe på Internettet for personer, der lider af depression, angst eller andre psykiske lidelser - anfører, at man bliver nødt til at lukke hjemmesiden, hvis udkastet til bekendtgørelse gennemføres. Dette skyldes at bekendtgørelsesudkastet kompromitterer brugerne af hjemmesidens anonymitet, og at der ikke er økonomisk mulighed for at efterleve logningspligten, og at gruppen ikke ønsker at påtage sig rollen som myndighedernes vagthund. Gruppen finder endvidere, at bekendtgørelsesudkastet er udtryk for en krænkelse af privatlivet og en naiv opfattelse af, at forbrydere ikke vil benytte sig af mulighederne for at undgå logning.

B. DEN ANVENDTE TERMINOLOGI OG DEFINITIONER

Advokatrådet gør opmærksom på, at begreberne "telenet" og "teletjenester", som - i overensstemmelse med retsplejelovens § 786 - anvendes i betænkningsudkastet, ikke længere anvendes inden for telelovgivningen. Ved lov nr. 450 af 10. juni 2003 om ændring af lov om

konkurrence- og forbrugerforhold på telemarkedet mv. blev terminologien "telenet" og "teletjenester" således erstattet med henholdsvis "elektroniske kommunikationsnet" og "elektroniske kommunikationstjenester". Denne ændring havde til formål at bringe lovens terminologi i overensstemmelse med den, der anvendes i Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester. Det fremgår imidlertid af lovens forarbejder, at der med indførslen af de nye begreber "elektroniske kommunikationsnet" og "elektroniske kommunikationstjenester" ikke var tilsigtet nogen indholdsmæssig ændring i forhold til den hidtil anvendte terminologi.

For at undgå misforståelser finder Advokatrådet, at ligheder og forskelle mellem den terminologi, der anvendes i henholdsvis retsplejeloven og bekendtgørelsesudkastet, henholdsvis i telelovgivningen, tydeligt bør fremhæves i bekendtgørelsen under henvisning til telelovens § 3, stk. 3.

Endvidere savnes i bekendtgørelsen en definition af begrebet "slutbruger", som i udkastet til vejledningen er defineret i overensstemmelse med definitionen i telelovens § 4, idet der dog anvendes en anden ordlyd. Herudover er "informations- og indholdstjenester" delvis undtaget fra registrerings- og opbevaringspligten, jf. § 1, stk. 2, men begrebet er ikke defineret i bekendtgørelsesudkastet, og det adskiller sig fra definitionen af "informations- og indholdstjenester" i telelovens § 3, stk. 4. Yderligere er begreberne "trafik" og "lokaliseringsdata" i udkastet til vejledning defineret anderledes end i udbudsbekendtgørelsens § 2, stk. 3, selv om der næppe er tilsigtet nogen begrebsmæssig forskel. Begrebet "trafik" er herudover i udbudsbekendtgørelsen betegnet "trafikdata".

Efter Rådets opfattelse bør der i bekendtgørelsen og vejledningen anvendes den samme terminologi som i teleloven, medmindre der er gode grunde til at fravige denne.

Rådet påpeger endvidere, at det centrale begreb "udbydere" af telenet og teletjenester ikke er defineret i bekendtgørelsen. Rådet finder, at dette begreb bør beskrives nærmere i bekendtgørelsen, og at det bør fremgå mere tydeligt af vejledningsudkastets punkt. 6.3., om det f.eks. er relevant for afgrænsningen af denne persongruppe, om den pågældende udbyder offentligt tilgængelige tjenester eller tjenester i lukkede net eller råder over egne lukkede net, der tilvejebringer infrastruktur til eget brug.

Der bør endvidere tages stilling til, hvem der skal anses for "udbyder", når en kommunikation teknisk set kan siges at være leveret af flere forskellige udbydere, f.eks. når en mobilkunde

roamer på en anden operatørs net. Det bør i den forbindelse anføres, om registrerings- og opbevaringspligten kan påhvile flere udbydere.

Institut for Menneskerettigheder foreslår, at det i bekendtgørelsesudkastet anvendte udtryk "trafik" erstattes med det mere præcise begreb "trafiktyper", sådan som begrebet er beskrevet på s. 13 i udkastet til vejledning.

Bolignetforeningen bemærker, at det ikke fremgår klart af bekendtgørelsesudkastet, hvem der hos en juridisk person - herunder bolignetforeninger - er strafferetligt ansvarlig for overholdelsen af logningspligten. Det er således uklart, om det i bolignetforeninger er de medlemmer, der har etableret foreningen, eller boligselskabets hovedbestyrelse, der i givet fald vil blive pålagt et strafferetligt ansvar. Bolignetforeningen rejser endvidere spørgsmål om, hvem det strafferetlige ansvar påhviler, hvis opgaven med at foretage logning hos en bolignetforening varetages af en tredjepart, f.eks. et teleselskab.

Udbyder skal ifølge bekendtgørelsesudkastet (§ 2, stk. 1, nr. 5) registrere "trafik", hvilket i vejledningsudkastet præciseres som den anvendte "trafiktype". Bolignetforeningen påpeger, at begrebet "trafiktype" ikke er veldefineret, og at der ikke i vejledningsudkastet gives eksempler på, hvad der skal forstås ved trafiktype for datakommunikation. Headerinformation fra netværksprotokoller og transportprotokoller er umiddelbart tilgængelig i systemer, der viderebefordrer datakommunikation, mens information om, hvilken applikationsprotokol der anvendes, ikke umiddelbart er tilgængelig. Hvis der med "trafiktype" menes applikationsprotokol, vil det påføre bolignetforeninger betydelige omkostninger til registrering. Endvidere kan applikationsprotokollen være umulig at fastlægge, fordi kommunikationen krypteres, eller fordi der er tale om en ubeskreven applikationsprotokol. Derfor vil pålideligheden af informationen om den anvendte applikationsprotokol være forbundet med betydelig usikkerhed.

TI, ITEK og **Cybercity** anfører, at udkastet til bekendtgørelse og vejledning omtaler en række begreber og definitioner, som dels ikke er klart og udtømmende beskrevet, dels afviger fra de definitioner, som anvendes i telelovgivningen.

Da anti-terror lovforslaget ikke giver holdepunkter for det modsatte, må det efter TI's opfattelse som udgangspunkt forudsættes, at de anvendte begreber skal defineres i overensstemmelse med de tilsvarende begreber anvendt i telelovgivningen. At det har været hensigten at anvende telelovgivningens definitioner underbygges da også af et notat af 17. december 2002 udarbejdet af Videnskabsministeriet forud for et møde med branchen. Det fremgår således heraf, at "det

bør sikres, at de definitioner af teleteknisk karakter, der anvendes i bekendtgørelsen, så vidt muligt er i overensstemmelse med tilsvarende definitioner efter telereguleringen."

TI og **Cybercity** påpeger, at begrebet "teletjeneste" ifølge den almindeligt anerkendte definition ikke omfatter chattjenester. En udbyder af chattjenester er derfor heller ikke nødvendigvis teleudbyder. Det er derfor tvivlsomt, om anti-terror lovforslaget giver hjemmel for en sådan bred forståelse af teletjenestebegrebet.

Som eksempel på afvigelser mellem definitionerne anvendt i bekendtgørelsesudkastet og telelovgivningen nævner TI endvidere anvendelsen af begrebet "lokaliseringsdata" i bekendtgørelsesudkastets § 2, stk. 1, nr. 6. Ved den seneste revision af udbudsbekendtgørelsen indsattes følgende definition af dette begreb i § 2, stk. 4: "*Ved lokaliseringsdata forstås data, som behandles i et elektronisk kommunikationsnet, og som angiver den geografiske placering af det terminaludstyr, som brugeren af en offentlig elektronisk kommunikationstjeneste anvender.*" Det fremgår af det bagvedliggende direktiv (2002/58/EU), at lokaliseringsdata kan være data, som er mere præcise end fremføringen af kommunikation, forudsætter og som (f.eks.) bruges til levering af tillægstjenester, f.eks. persontilpassede trafikoplysninger eller bilistvejledninger (direktivets betragtning 35). Det vil med andre ord sige, at lokaliseringsdata ifølge den i telelovgivningen anvendte definition kan være data, som ikke normalt indgår i produktionen af teleydelser, og som dermed ikke er trafikdata. TI finder det på den baggrund yderst uhensigtsmæssigt, at man i udkastet til bekendtgørelse anvender begrebet "lokaliseringsdata", når man tilsyneladende ikke benytter begrebet i samme betydning som i telelovgivningen.

Som et andet eksempel på et begreb, som efterlader betydelig fortolkningstvivl, fremhæver TI begrebet "trafik", der i bekendtgørelsen er nævnt som én af de oplysninger vedrørende en kommunikation, som skal registreres (§ 2, stk. 1, nr. 5). Uden den tilhørende forklaring i vejledningen må kravet nærmest anses for uforståeligt, hvilket i sig selv er utilfredsstillende. Ifølge vejledningen indebærer kravet om opbevaring af "trafik" dels et krav om opbevaring af oplysning om den anvendte trafiktype, dels et krav om opbevaring af oplysning om, hvorvidt den initierede kommunikation blev gennemført, og hvis ikke, hvad der var årsagen hertil. Især sidstnævnte del af kravet forekommer at være en noget nær absurd brug af begrebet "trafik" og under alle omstændigheder ikke en normal forståelse af begrebet. Eksemplet illustrerer, at bekendtgørelsen ikke indeholder en udtømmende beskrivelse af logningspligtens indhold og dermed ikke lever op til det krav om klarhed og forudsigelighed, der må stilles til regler, der vedrører indgreb i privatlivets fred.

Ligeledes påpeger **TI** og **Cybercity**, at trafikdata ikke er defineret i retsplejelovens § 786, stk. 4, eller i bekendtgørelsesudkastet. Begrebet er i stedet defineret i persondatadirektivet og udbudsbekendtgørelsen. Udbudsbekendtgørelsens § 2, stk. 3, fastsætter, at der ved trafikdata skal forstås "*data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf.*" Det er således en forudsætning, at data behandles i tilknytning til kommunikationen. En del af de registreringer, som er omfattet af bekendtgørelsesudkastet, falder uden for denne definition. Det gælder f.eks. ændring af identitet i forbindelse med telefoniopkald og registrering af brugere af IP-adresser, da de pågældende oplysninger ikke behandles som led i kommunikationen. Der bør på den baggrund skabes en ny lovhjemmel som grundlag for logning af identitetsændringer og opkald til chat-tjenester på Internettet. Samtidig må hjemlen til logning af e-mail tydeliggøres, da dette ikke normalt opfattes som en teletjeneste, men en informationstjeneste, der udnytter teletjenester.

IT-Brancheforeningen er uforstående over for den meget brede kreds af aktiviteter, selskaber, organisationer mv., som Justitsministeriet tilsyneladende anser for omfattet af begrebet "telenet eller teletjenester", henholdsvis begrebet "udbydere af telenet eller teletjenester".

Brancheforeningen antager, at de i retsplejelovens § 786 anvendte begreber "udbydere af telenet eller teletjenester", henholdsvis "telenet" og "teletjenester", har samme betydning som de tilsvarende begreber i telelovgivningen. Det må gælde uanset, at de pågældende begreber efterfølgende i telelovgivningen terminologisk er ændret til "udbydere af elektroniske kommunikationsnet eller -tjenester", henholdsvis "kommunikationsnet eller -tjenester", jf. lovbemærkningerne til den pågældende ændring af telelovgivningen. Med hensyn til begrebet "udbydere" stemmer dette overens med, at lovbemærkningerne til § 786 konsekvent omtaler de pågældende som "teleselskaber og Internetudbydere". Af bemærkningerne til de pågældende bestemmelser i telelovgivningen fremgår, at det afgørende er, om den pågældende på kommercielt grundlag leverer telenet eller teletjenester til flere kunder. Det fremgår samtidig, at ejere af elektroniske kommunikationsnet, der ikke stiller sådanne tjenester til rådighed på kommercielt grundlag, men alene anvender dem til eget brug, ikke kan anses for udbydere af telenet eller teletjenester. Med hensyn til begreberne "telenet eller teletjenester", gengiver bekendtgørelsesudkastet den i telereguleringen anvendte definition heraf, men begrebet teletjenester udvides til også at omfatte chat-tjenester. Det fremgår imidlertid eksplicit af bemærkningerne til § 786, at indholds- og informationstjenester, som f.eks. de omhandlede chat-tjenester, er noget andet end telenet eller teletjenester. Af samme grund nævner bestemmelsen (§ 2 i lov om konkurrence- og forbrugerforhold på telemarkedet), der afgrænser hvilke parter, der er omfattet af telelovgivningen, eksplicit både ejere af elektroniske kommunikationsnet og udbydere af indholds- og informationstjenester, som parter der kan være omfattet af dele at lovens bestemmelser. §

786 omfatter derimod kun "udbydere af telenet eller teletjenester". Det er på den baggrund Brancheforeningens opfattelse, at der ikke er hjemmel til i bekendtgørelsen at fastsætte regler for chat-tjenester. Brancheforeningen gør samtidig opmærksom på, at e-mail ikke internationalt opfattes som en teletjeneste. Der er således ikke knyttet et nettermineringspunkt til en e-mail tjeneste, men alene et nettermineringspunkt til den teletjeneste, der benyttes som adgang til en e-mailtjeneste.

Brancheforeningen fremhæver endvidere, at det er uklart, hvad der forstås ved "identitet". Herudover anvender bekendtgørelsesudkastet begrebet "transmission" i relation til e-mailtrafik, IP-telefoni og andre former for pakkekoblet teletrafik, selv om begrebet er stort set uanvendeligt, idet denne trafiktype er karakteriseret ved, at den i "småbidder" sendes gennem den tilfældigvis tilgængelige infrastruktur og først "genopstår" som en samlet kommunikation, når den når frem til modtageren. Brancheforeningen går ud fra, at hensigten ikke har været at forpligte samtlige udbydere af telenet eller teletjenester til at registrere og opbevare oplysninger om det samlede "trafikflow" gennem deres infrastruktur, men i overensstemmelse med ordlyden i § 2, stk. 1, alene de opkald, som udbyderen er involveret i afviklingen af. Det betyder bl.a., at applikationer på Internet, som alene anvender nettet som underliggende transmissionsressource, ikke skal logges af Internetudbyderen. I modsat fald ville Internetudbyderen være nødsaget til at logge adresser for alle ekspederede pakker til og fra brugeren. Dette ville i givet fald være i strid med afsnit 3.1.3.2 i bemærkningerne til anti-terror lovforslaget, hvor det understreges, at det ikke er hensigten at kortlægge kundernes aktiviteter (det samlede netflow), mens de anvender Internettet. Endelig indeholder bekendtgørelsesudkastet og den tilhørende vejledning ingen præcis beskrivelse af, hvad kravene om døgnbemanding, henholdsvis levering i "læsbart format", i praksis indebærer, og de opstillede eksempler indeholder ikke tilstrækkelig vejledning herom. På den baggrund foreslår Brancheforeningen, at pligten til logning af trafik, der alene "transmitteres" via en udbyders net (jf. § 2, stk. 1), men ikke hverken initieres eller termineres i dette, udgår, idet kravet om logning af transmissionstrafik blot vil føre til dobbelt-logning. Det foreslås endvidere, at der som udgangspunkt kun stilles krav om logning i A-enden (initiering af kommunikationen), og at der - for så vidt angår de få tilfælde, hvor der er behov for logning af transit, henholdsvis terminering, ud fra ønsket om at få registreret oplysninger, der ikke kan registreres af andre net - sker en konkretisering af logningspligten. Yderligere foreslås det, at Justitsministeriet i samarbejde med branchen afklarer, hvordan det kan undgås, at samme trafik logges flere gange hos flere forskellige parter, og at der indtil videre kun skal ske logning af trafikdata, der allerede registreres. Endelig finder Brancheforeningen, at Justitsministeriet i tæt dialog med branchen bør definere de begreber, der anvendes i bekendtgørelsen og vejledningen, og at det bør afklares, hvilke forventninger Justitsministeriet og politiet har i relation til kravet om døgnbemanding og "læsbart format".

C. KREDSEN AF UDBYDERE, DER ER OMFATTET AF LOGNINGSPLIGTEN - BEKENDTGØRELSENS UNDTAGELSER

Advokatrådet anfører, at de væsentlige undtagelser til registrerings og opbevaringspligten, som bekendtgørelsesudkastet indeholder, gør det tvivlsomt, om reglerne reelt er egnede til at nå sit formål, idet det må formodes, at de personer, som måtte ønske at undgå logning, har kendskab til undtagelserne i registrerings- og opbevaringspligten.

Bolignetforeningen har vanskeligt ved at se, hvilke efterforskningsmæssige kriterier der adskiller bolignetforeninger fra f.eks. private virksomheder, universiteter, biblioteker mv., der ifølge bekendtgørelsesudkastet helt er undtaget fra logningspligten. Hensynet til en effektiv efterforskning, samt hensynet til, at der bør gælde lige vilkår for alle udbydere, taler for, at logningspligten i givet fald skal omfatte alle udbydere.

Red Barnet påpeger ligeledes, at udveksling af børnepornografi typisk foregår mellem personer, der er klar over, at distribution af børnepornografisk materiale er ulovligt, og som gør en indsats for at skjule deres spor. Der er derfor efter Red Barnets opfattelse behov for en mere omfattende registrering, hvis bekendtgørelsen skal have en tilfredsstillende effekt for efterforskningen af børnepornografi på Internettet.

Kommunernes Landsforening (KL) anfører, at ordningen i den fremlagte form kun må forventes at ville få begrænset effekt på kommunernes vilkår. KL er opmærksom på, at en ikke uvæsentlig del af såvel telekommunikation som teleydelser vil være friholdt fra ordningen via den reelle friholdelse af den offentlige sektor. Gennemføres ordningen i sin nuværende udformning kan det derfor efter KL's vurdering medføre, at den samfundsmæssige effekt vil være begrænset. I det omfang ordningen ændres for at udvide ordningen med de nu undtagne områder inden for blandt andet den kommunale sektor, vil dette efter KL's opfattelse være omfattet af det udvidede totalbalanceprincip. KL har i høringssvaret taget forbehold for en senere kommunalpolitisk behandling af spørgsmålet.

Rådet for IT-sikkerhed påpeger, at en del virksomheder udbyder services som virtuelle rum til samarbejde mellem medarbejdere, kunder og samarbejdspartnere, som reelt er at betragte som chat-rooms, hvor kredsen af slutbrugere ikke på forhånd er afgrænset. Disse virksomheder står pludselig med en udgift til etablering, drift og sikker håndtering af logning af denne kommunikation. Tilsvarende forhold gør sig gældende i forhold til virksomheders hyppige an-

vendelse af muligheden for på hjemmesider at aktivere en mail med kommentarer, hvilket efter udkastet til bekendtgørelse indebærer, at sådan kommunikation skal logges. Rådet frygter, at udgifterne til logning kan gå ud over investeringerne i IT-sikkerhed. Rådet anbefaler derfor, at det nøje overvejes om undtagelserne i bekendtgørelsens § 3 kan formuleres på en sådan måde, at ikke større dele af danske virksomheder skal investere i og drive logning i et omfang, som det formentlig ikke har været tilsigtet i lovgivningen.

TI og Cybercity påpeger, at det fremgår af bemærkningerne til anti-terror lovforslaget (pkt. 3.1.3.), at hensynet til effektiv regulering og konkurrenceforhold i branchen tilsiger, at logningspligten omfatter alle udbydere. Det er derfor i strid med lovens intention, at bekendtgørelsesudkastet lægger op til at undtage visse udbydere fra logningspligten, mens andre udbydere alene forpligtes til at foretage logning i begrænset omfang.

TI og Cybercity finder desuden, at politiet også kan have efterforskningsmæssig interesse i, at der logges oplysninger om teletrafik hos boligforeninger med mindre end 100 slutbrugere. Der er således intet sagligt grundlag for disse undtagelser fra logningspligten, og det foreslås derfor, at der i stedet indføres en adgang til administrativt at meddele dispensation fra logningspligten, hvis der konkret er grundlag herfor.

Cybercity anfører endvidere, at hensynet til at undgå konkurrenceforvridning samt hensynet til indgrebets effektivitet taler for, at virksomheder og institutioner også skal anses for udbydere, der er omfattet af logningspligten.

TI finder ligeledes, at bekendtgørelsesudkastets undtagelser fra logningspligten for så vidt angår bl.a. institutioners og virksomheders elektroniske post og samtaler via Internettet undergraver logningspligtens effektivitet og skaber en forskelsbehandling og dermed konkurrenceforvridning mellem forskellige kommunikationsformer.

Efter det foreliggende udkast er al elektronisk post, der formidles af virksomheders eller institutioners postservere, undtaget fra logningspligten. Virksomheder skal således ikke logge oplysninger om de ansattes teletrafik, idet denne trafik kun skal logges, hvis en virksomhed benytter udbydere af telenet og teletjenester til den eksterne trafik. For telefonopkald betyder dette, at udgående opkald fra en virksomhed typisk logges med et fælles A-nummer. For elektronisk post er virkningen, at trafikken ikke logges, hvis virksomheden anvender egne postservere. TI og Cybercity finder det uproportionalt og konkurrenceforvridende, hvis outsourcing af en virksomheds kommunikation indebærer, at der skal ske logning af medarbejdernes teletrafik i videre omfang, end hvis virksomhedsinterne net opbygges som et særskilt privat net. Regler-

ne bør i stedet udformes således, at private net i alle tilfælde er undtaget fra registreringspligten, herunder også i tilfælde af outsourcing til et offentligt net. Det bør endvidere præciseres, i hvilket omfang de reducerede krav i henhold til bekendtgørelsesudkastets § 3, stk. 2, nr. 2, kan gøres gældende i forbindelse med outsourcede ydelser.

IT-Brancheforeningen påpeger ligeledes, at undtagelserne fra logningspligten indebærer en problematisk konkurrenceforvridning på det danske telemarked. Endvidere må det må bero på en misforståelse af hjemmelsgrundlaget, at der fastsættes særlige undtagelsesregler for en række parter, der i de fleste tilfælde slet ikke er omfattet af begrebet "udbydere", og som derfor enten slet ikke er omfattet eller alene er omfattet af logningspligten, når og hvis de optræder som udbydere. Som eksempler på parter, der ikke er "udbydere", nævner foreningen for det første arbejdsgivere, der giver deres medarbejdere adgang til Internettet via egen infrastruktur. Foreningen fremhæver i den forbindelse, at Justitsministeriet i sit svar på Retsudvalgets spørgsmål nr. 123 (L 35 - bilag 99) vedrørende anti-terror lovforslaget oplyste, at sådanne arbejdsgivere ikke kan anses for "udbydere" af telenet eller teletjenester, blot fordi de uden vederlag stiller Internetadgang til rådighed for deres medarbejdere, herunder via hjemmearbejdspladser koblet op til virksomhedens øvrige infrastruktur. Ikke desto mindre fremhæves disse i vejledningen som omfattet af undtagelsesbestemmelsen i § 3, stk. 1, nr. 1, om "udbydere, der stiller net eller tjenester til rådighed uden vederlag". Som yderligere eksempel nævner foreningen biblioteker, uddannelsesinstitutioner og andre offentlige institutioner, der på ikke-kommercielt grundlag stiller net eller tjenester til rådighed for eksterne parter i form af lånere, studerende, patienter eller lign., jf. undtagelsen i § 3, stk. 1, nr. 2. Det fremgår af det nævnte svar til Folketinget, at sådanne personer som udgangspunkt heller ikke kan anses for at være udbydere af telenet eller teletjenester. Foreningen finder på den baggrund, at det er telelovgivningens definition af begrebet "udbyder", der bør danne grundlag for afgrænsning heraf. Efter foreningens opfattelse er der behov for en nøje gennemgang af undtagelsesbestemmelserne og den tilhørende vejledningstekst med henblik på dels at få identificeret relevante eksempler på, hvilke udbydere der er omfattet, dels at få fjernet de eksempler, som vedrører parter, der ikke kan anses for at være udbydere.

Brancheforeningen anfører herudover, at en stor og stadigt voksende del af Internet-trafikken består i fuldt ud automatiserede kommunikationer mellem systemer (f.eks. kommunikationer mellem banksystemer og andre lignende løsninger), som ikke kan misbruges til kommunikation i tilknytning til kriminel aktivitet. Sådanne kommunikationer bør derfor generelt undtages fra logningspligten.

For så vidt angår virksomheders outsourcing af IT-drift, anfører Brancheforeningen, at der er en række virksomheder, der som en mindre del af en samlet aftale leverer telekommunikationsydelser, men som først og fremmest leverer intern IT-drift i bred forstand, og herunder leverer intern kobling/infrastruktur, intern trafikafvikling og -dirigering, omstillingsfunktioner og lignende til slutbrugere. Sådanne funktioner ligger på kundens side af nettermineringspunktet og er dermed uden for telenettet. Der er tale om aktiviteter, der falder uden for det område, der er hjemmel til at regulere, nemlig udbud af telenet eller teletjenester. Brancheforeningen finder derfor ikke, at sådanne virksomheder vil have pligt til at logge oplysninger vedrørende trafikken bag deres kunders nettermineringspunkt – internt hos de pågældende – herunder f.eks. oplysninger der sammenkobler det/den enkelte eksterne kald/mailkommunikation med en bestemt medarbejder hos den pågældende kunde, eller oplysninger om rent interne kald eller mailkommunikationer. Det bør udtrykkeligt fremgå af bekendtgørelsen, at logningspligten ikke omfatter denne type oplysninger, heller ikke selv om den pågældende IT-drift er outsourcet. Foreningen påpeger, at disse betragtninger gælder fysiske netydelser i de tilfælde, hvor virksomheden har eget nettermineringspunkt, og de leverede ydelser alene vedrører distribution og indsamling af trafik mellem virksomheden og udbudte teletjenester samt intern kommunikation. Men outsourcing beror i stigende omfang på fællesproduktion af virksomhedsintern og virksomhedsekstern trafik i mobilnet eller Internet uden individuelle grænseflader i form af nettermineringspunkter mellem den enkelte virksomhed og omverdenen. Det vil heller ikke i disse tilfælde være rimeligt, hvis intern trafik skulle logges. Ekstern trafik bør alene kræves logget i samme omfang, som hvis virksomheden selv varetog sit interne net med fælles tilslutning til offentlige net. Tilsvarende gælder med hensyn til virksomheder, der får stillet e-mail server ydelsen til rådighed i stedet for at drive den selv.

Hvis der skal ske logning i tilfælde af outsourcing, vil det betyde en markant konkurrenceforvridning til skade for hele IT-outsourcingmarkedet. Hvis outsourcet drift af virksomhedsintern IT- og teleinfrastruktur mod forventning anses for omfattet af begrebet "udbud af telenet eller teletjenester", bør der indsættes en bestemmelse i bekendtgørelsen, der undtager disse tilfælde fra logningspligten.

Dansk IT finder det problematisk, at bekendtgørelsesudkastet indeholder en række undtagelser fra logningspligten, der gør det muligt for kriminelle at undgå registrering af elektronisk korrespondance mv.

Digital Rights fremhæver, at man ud fra hensynet til beskyttelse af borgernes privatliv naturligvis kan glæde sig over, at der er områder i samfundet, der er undtaget fra den meget indgribende registreringsforpligtelse, så borgerne stadig bevarer muligheden for at kommunikere

elektronisk uden at blive registreret – f.eks. på biblioteket eller via IP-telefoni. Imidlertid vil undtagelserne underminere den efterforskningsmæssige effekt af bekendtgørelsen. Balancen mellem indgrebets efterforskningsmæssige effekt og dets indgriben i borgernes privatliv forrykkes dermed afgørende, og det må overvejes, om et så omfattende indgreb i borgeres privatliv kan berettiges, hvis den efterforskningsmæssige effekt reelt ikke opnås.

Boligselskabernes Landsforening noterer sig med tilfredshed, at boligforeninger med mindre end 100 slutbrugere er undtaget fra registrerings- og opbevaringspligten, og at registrerings- og opbevaringspligten er begrænset for boligforeninger med mindre end 400 slutbrugere. Mange boligforeninger, antenneforeninger mv. overskrider imidlertid disse bagatelgrænser, og for disse vil logningspligten udgøre en stor økonomisk byrde. Samtidig finder Landsforeningen, at de mange undtagelser fra logningspligten efterlader et indtryk af, at der eksisterer så mange muligheder for at undgå logning, at det er stærkt tvivlsomt, om reglerne vil få den tilsigtede effekt. Kriminelle vil således f.eks. blot kunne anvende Internetadgangen på det lokale bibliotek, på en café eller i lufthavnen.

Danske Mediers Forum fremhæver, at reglerne – på grund af bekendtgørelsesudkastets undtagelser fra logningspligten samt mulighederne for på anden måde at unddrage sig logning – må forventes kun at ville få ringe effekt.

D. IT- OG TELEKOMMUNIKATION TIL OG FRA UDLANDET MV.

Rigspolitichefen anfører, at der muligvis er forbundet nogle praktiske vanskeligheder med logning i de tilfælde, hvor teleudbydere kun har etableret servere mv. i lande uden for dansk jurisdiktion. Det fremgår af § 4 i udkastet til bekendtgørelse, at trafikoplysninger skal opbevares i eller overføres til Danmark, men denne forpligtelse gælder efter udkastet ikke for aflytning af telefontrafik.

TI anfører, at logningspligten – i overensstemmelse med principperne i den øvrige telelovgivning – må anses for at omfatte tjenester udbudt i Danmark til en dansk bruger – også selv om brugeren i perioder befinder sig i udlandet. Eksempelvis må en dansk mobilbruger, der er roamet til et udenlandsk net, anses for at være omfattet, mens en udenlandsk mobilbruger, der er roamet til et dansk net, ikke er omfattet. Uden en sådan fortolkning, der helt svarer til principperne i gældende telelovgivning, kan der opstå konflikter mellem landenes nationale udmøntninger af det nugældende teledirektiv (2002/58/EF) og den øvrige telespecifikke regulering. I praksis vil det imidlertid ikke altid være muligt at undtage roamede udenlandske kunder fra registrering, og det vil i mange tilfælde kræve betydelige investeringer at bortsortere eller

anonymisere sådanne registreringer i en efterfølgende proces. Selv en kortvarig lagring af trafikdata vedrørende en udenlandsk kunde, eksempelvis i form af lokaliseringsdata, kan være et brud på et andet lands regler om persondatabeskyttelse. Foreløbige undersøgelser viser samtidig, at udenlandske roamingpartnere ikke i almindelighed agter at udlevere lokaliseringsdata for danske kunder i udlandet, og de vil næppe ændre dette, når de ikke efter nationale regler er forpligtet hertil. Problemstillingen er aktuel for mobilkunder, Internetkunder og calling cards, der udbydes internationalt. Men problemet kan tilsvarende opstå for enhver tjeneste, som udbydes grænseoverskridende. I nogle tilfælde vil det for en internationalt udbudt tjeneste ikke være muligt at fastslå det land, hvortil kundeforholdet skal henføres. Et eksempel herpå er webmail, der udbydes via hotmail, google, icq eller lignende. Logningspligten vil for disse ydelser formentlig være gældende, når kunden er tilmeldt tjenesten fra Danmark – uanset om webmail udbydes fra Danmark eller fra udlandet. Udbyderen af webmail kan imidlertid ikke kontrollere den geografiske adresse, hvorfra en tilmelding er foretaget. Hvis trafikdata registreres for alle brugere af webmail, kan andre landes regler om beskyttelse af persondata herved overtrædes. Efter TI's opfattelse bør hverken danske eller udenlandske udbydere af webmail til danskere dermed i praksis være omfattet af logningspligten, da de pågældende udbydere ikke med sikkerhed kan fastslå, at kundeforholdet er underlagt dansk lovgivning. TI finder det nødvendigt, at der i bekendtgørelsen tages stilling til pligternes omfang i relation til danske og udenlandske kundeforhold, roaming og grænseoverskridende tjenester uden lokaliseringsdata for anvendelsen mv. Det bør fremgå af bekendtgørelsen, om registrering kan foretages i de tilfælde, hvor kundens nationale tilhørsforhold ikke kan fastslås. Hvis dette er tilfældet, vil rækkevidden af logningspligten reelt blive udstrakt til alle udbydere af webmail i hele verden.

TI bemærker vedrørende opkald fra udlandet til Danmark, at det bør afklares, om det vil være i overensstemmelse med teledatadirektivet (2002/58/EF) at registrere A-numre for indkommende kald fra udlandet til Danmark, hvis det eksempelvis ikke i det pågældende land er tilladt at registrere og opbevare trafikdata i henhold til direktivets artikel 6 stk. 1, eller identiteten i sådanne tilfælde må anonymiseres i respekt af et andet lands databeskyttelsesregler. Direktivet giver tilsyneladende ingen vejledning i vurderingen af dette spørgsmål, da det ikke er forudset, at trafikdata kan kræves logget i den kaldte kundes net. Tilsvarende problemstillinger vedrørende registrering af kaldende identitet eksisterer for e-mail, hvor nationaliteten ikke kan udledes af e-mailadressen eller IP-adressen, og hvor registreringen reelt alene vedrører afsenderen, indtil modtageren aktivt har modtaget den fremsendte mail. TI finder derfor, at Justitsministeriet bør vurdere, om der er behov for indførelse af et krav om anonymisering i forbindelse med den foreslåede registrering af kaldende identiteter i udlandet, idet registreringen dermed bliver en registrering af trafikdata for den udenlandske bruger, som har initieret kommunikationen. Spørgsmålet må vurderes både i relation til gennemførte kommunikationer med en dansk

borger og kommunikationer, der alene er forsøgt etableret fra udlandet. Spørgsmålet er ifølge TI, om problemstillingerne ikke reelt betyder, at kravet om logning i kaldte ende under alle omstændigheder må opgives.

IT-Brancheforeningen anfører, at det fremgår af bekendtgørelsesudkastets § 4, at oplysninger, der registreres i udlandet som led i danske udbyderes (f.eks. danske outsourcing virksomheders) virksomhed i Danmark, skal overføres til Danmark med intervaller på maksimalt 72 timer. Foreningen foreslår, at bestemmelsen omformuleres, så den i stedet kommer til at indeholde et krav om, at data, der i en aktuel situation udbedes af myndighederne, skal stilles til rådighed i Danmark inden for 72 timer. Herved undgår de omhandlede selskaber dagligt at skulle overføre og opbevare store mængder af data, som formodentlig aldrig vil skulle anvendes.

TI finder ligeledes, at bestemmelsen i bekendtgørelsesudkastets § 4 savner konkret begrundelse og vil føre til uhensigtsmæssigheder og skævvridninger af konkurrenceforholdene i telesektoren. En række udbydere udnytter allerede i dag de stordriftsfordele, der ligger i at lade visse funktioner udføre centralt for hele Norden eller i Europa i ét af landene for således at nedbringe omkostninger og effektivisere driften. Et krav om, at data som på denne måde opbevares i udlandet, skal overføres og opbevares i Danmark, vil selvsagt påføre udbyderen ekstraomkostninger, og vil dermed blokere udviklingen. Da formålet med reguleringen alene er at sikre, at oplysningerne er tilgængelige for politiet, når disse efterspørges, bør bestemmelsen ændres således, at det geografiske område for opbevaring af oplysningerne udvides til at omfatte hele EU og de nordiske lande. Alternativt bør det geografiske opbevaringskrav helt udgå.

Dansk IT finder det ubegrundet, at bekendtgørelsen (§ 4) fastsætter en pligt for udbyderne til at opbevare registrerede data i Danmark. Det må være tilstrækkeligt enten at kræve, at data skal være umiddelbart tilgængelige fra Danmark, eller at data skal være tilgængelige inden for en bestemt tidsfrist.

Rådet for IT-sikkerhed anfører, at det fremgår af § 2, stk. 4, at registrering og opbevaring af oplysninger efter stk. 1 - 3, efter aftale med udbyderen på dennes vegne kan foretages af en anden udbyder eller af en tredjemand. Rådet anbefaler, at der indsættes en bestemmelse i bekendtgørelsen, der svarer til persondatalovens § 42, således at det følger af bekendtgørelsen, at der skal foreligge en skriftlig aftale mellem parterne, ligesom det af aftalen skal fremgå, at den anden udbyder eller tredjemand (databehandleren) alene handler efter instruks fra udbyderen (den dataansvarlige). Tilsvarende anbefales, at der indsættes en bestemmelse, hvorefter data-

behandlere etableret uden for Danmarks grænser som minimum skal overholde dansk lovgivning om sikkerhedsforanstaltninger.

E. CHAT-TJENESTER MV.

Red Barnet er enig i, at logningspligten bør omfatte chatudbydere, og at man i den forbindelse har noteret sig, at bekendtgørelsesudkastet ikke undtager små chatudbydere.

Datatilsynet anfører, at det fremgår af bekendtgørelsesudkastet, at udbydere af chat-tjenester kun har pligt til at registrere og opbevare oplysninger om ændring af opkaldende og opkaldte identitet, jf. § 2, stk. 1, nr. 2 og 4, samt i givet fald tidspunktet for kommunikationen, jf. § 2, stk. 1, nr. 7, jf. § 3, stk. 2, nr. 3. Det fremgår endvidere af udkastet til vejledning (s. 21), at oplysning om ændring af opkaldte identitet f.eks. vil omfatte oplysning om, hvilket af flere mulige chat-room den opkaldende identitet er tilkoblet. Datatilsynet henleder i den forbindelse opmærksomheden på bemærkningerne til anti-terrorlovforslaget (s. 46, spalte 1), hvoraf fremgår, at: "der ikke med forslaget lægges op til, at Internetudbyderne skal foretage en kortlægning af kundernes aktiviteter, mens de anvender Internettet. Udbyderne vil således ikke løbende skulle foretage registrering af, hvilke hjemmesider, chatrooms mv. kunderne besøger." Det står ikke umiddelbart Datatilsynet klart, hvordan logningskravet for chat-udbyderne harmonerer med disse lovbemærkninger.

Dansk IT anfører, at bekendtgørelsesudkastet går videre, end det er forudsat i retsplejeloven. Det gælder f.eks. pligten til at logge kommunikationen hos virksomheder, der udbyder virtuelle rum til samarbejde mellem medarbejdere, kunder og samarbejdspartnere, som reelt er at betragte som chat-tjenester, uden en på forhånd afgrænset kreds af slutbrugere. Dansk IT frygter, at udgifterne til logning af sådan kommunikation vil gå ud over andre investeringer i bl.a. IT-sikkerhed.

Digital Rights anfører, at registreringspligten indebærer, at det - ud over den enkelte brugers identitet - skal registreres, hvilke chat-rooms brugeren har anvendt, og således også den situation, at to brugere vælger at gå ind i et separat chat-room for at kommunikere privat. Dette svarer til, at indehavere af steder, hvor folk mødes (f.eks. værtshuse, foreninger, forsamlingshuse mv.) fik pligt til at registrere alle besøgende og at holde øje med, hvem der taler med hvem, og om nogen evt. vælger at sætte sig hen til et bord for sig selv. Sådan registrering indebærer efter Digital Rights' opfattelse et omfattende indgreb i borgerens frihed til at mødes i det virtuelle rum. Indgrebet skal ses i lyset af Internettets stigende betydning for borgernes

kontaktmønstre. Brugen af chat er for en stadig stigende del af befolkningen en integreret del af kontakten til omverdenen, og registrering heraf vil således kunne angå væsentlige dele af befolkningens sociale kontakt med omverdenen. Bekendtgørelsen synes endvidere ikke at tage højde for den store spredning i de tjenester, som vil blive omfattet af registreringspligten. Mange personlige hjemmesider og web-dagbøger (Blogs) har chat funktioner, hvor ejeren chatter med sine kontakter på nettet. Det står ikke klart, hvem der i denne situation vil have ansvaret - eller den tekniske mulighed - for at gennemføre en registrering af brugerne. Registrering af chat på personlige hjemmesider føjer desuden en ekstra indgribende karakter til bekendtgørelsen, idet brugere på denne måde vil være tvunget til at registrere sine personlige kontakter på nettet.

Bolignetforeningen forstår bekendtgørelsesudkastet således, at udbydere, der alene viderebefordrer datakommunikation mellem en chat-kunde og en chat-server, ikke skal registrere chat-room identitet, IP-adresse og anvendt chat-room. I modsat fald vil registreringen være forbundet med betydelige omkostninger for disse udbydere. Bolignetforeninger stiller ofte en personlig hjemmeside til rådighed for deres medlemmer, og en af de funktioner, som kan tilbydes, er chat-tjenester. Bolignetforeningen påpeger, at det ikke fremgår klart af bekendtgørelsesudkastet, hvem registreringspligten påhviler i disse tilfælde. Det fremgår ikke af bekendtgørelsen, om det er det enkelte medlem, der, hvis den personlige hjemmeside opbevares på medlemmets egen computer, skal registrere chat-room identiteter og tilhørende IP-adresser. Det fremgår endvidere ikke af bekendtgørelsen, hvem der er registreringspligtig, hvis medlemmets personlige hjemmeside - indeholdende en chat-tjeneste - opbevares på foreningens server.

Danske Mediers Forum finder det problematisk, at bekendtgørelsesudkastet - ud over traditionel televirksomhed - også omfatter chat-tjenester. Bekendtgørelsen vil derfor få virkning for medievirksomhed, der gør brug af chat-teknologien som en del af det redaktionelle koncept. Logningsforpligtelsen vil dermed også få økonomiske konsekvenser for medier, der anvender chat-tjenester på den nævnte måde. Det er endvidere betænkeligt i lyset af, at chat-tjenester - efter almindeligt anerkendte definitioner i telelovgivningen - ikke er teletjenester. Dette rejser endvidere spørgsmål om andre Internetbaserede ydelser også kan omfattes af logningsforpligtelsen uden en lovændring - f.eks. telefoni over Internettet (VoIP), instant messaging, debatfora samt publicering af indhold på hjemmesider. I givet fald vil det indebære en endnu større påvirkning af vilkårene for produktion og tilvejebringelse af indhold på Internettet.

ITEK mener, at det bør overvejes nøje, om en afgrænsning, der vil omfatte alle former for chat-tjenester, er hensigtsmæssig. ITEK peger i den forbindelse på, at stort set alle Internetsider i dag giver mulighed for online og samtidig udveksling af meddelelser.

IT-Brancheforeningen mener ikke, at § 786 giver hjemmel til at fastsætte regler om registrering og opbevaring med hensyn til chat-tjenester. Herudover ville en sådan regulering have særdeles vidtgående og ikke-gennemtænkte konsekvenser for en række chat-tjenester, der drives af foreninger, frivillige organisationer mv., ligesom det ville umuliggøre ad hoc anvendelse af en række professionelt anvendte netværks- og videndelings-værktøjer (f.eks. Groupcare).

F. SPØRGSMÅL VEDRØRENDE DE TEKNISKE MULIGHEDER FOR REGISTRERING OG OPBEVARING AF TRAFIKDATA MV.

Datatilsynet understreger, at det indgik som et centralt element i forhandlingerne i Folketinget om indsættelse af den nye bestemmelse i retsplejelovens § 786, stk. 4, at registrerings- og opbevaringspligten alene omfatter teletrafikdata og ikke indholdet af kommunikationen. Datatilsynet lægger derfor til grund, at udbydernes logningsforpligtelse er begrænset til alene at omfatte trafikdata, og at der kun indføres logningspligt i det omfang, det rent teknisk er muligt at adskille trafikdata fra indholdsdata. Datatilsynet bemærker i den forbindelse, at der ikke ses at være foretaget undersøgelse af, om den registrerings- og opbevaringspligt, som udbyderne pålægges, kan opfyldes i teknisk henseende, uden at der samtidig sker registrering og opbevaring af indholdet i den elektroniske kommunikation. Datatilsynet henviser i den forbindelse til Telekommunikationsindustrien i Danmarks (TI) høringssvar vedrørende lovforslaget, hvori TI bemærkede, at oplysningen om modtageren af en SMS-besked rent teknisk er en del af indholdet af beskeden, og at opfyldelse af registreringspligten dermed vil indebære, at hele indholdet registreres. Datatilsynet fremhæver, at registrering og opbevaring af indholdsdata af en elektronisk kommunikation hos udbyderen kan indebære en overtrædelse af persondatalovens regler.

Dansk IT påpeger, at den teknologiske udvikling konstant vil udfordre bekendtgørelsens krav og afgrænsninger. Som eksempel nævnes, at internetbaseret kommunikation som IP-telefoni og instant meassaging næppe lader sig registrere efter de normer, bekendtgørelsen forudsætter.

Bolignetforeningen fremhæver, at bekendtgørelsen pålægger bolignetforeningerne at registrere og opbevare oplysninger, der ikke normalt registreres, og at det ikke er muligt at fastslå, hvilke oplysninger der skal registreres. Bolignetforeningen finder, at en bekendtgørelse, der specifikt definerer, hvad der skal registreres, vil medføre meget store omkostninger til at opgradere deres systemer, så det bliver muligt at registrere disse data.

Boligneforeningen mener ikke, at bekendtgørelsen bør kræve specifikation af trafik ud over transportprotokol og eventuelt dertil knyttet portnummer. Dette skyldes, at identifikation af anvendt applikationsprotokol i visse tilfælde vil være umulig (f.eks. pga. kryptering), og hvor den er umulig, vil det være forbundet med betydelige meromkostninger for udbyder, idet disse informationer ikke er umiddelbart tilgængelige i dennes systemer og derfor vil kræve intensiv pakkeanalyse at fremskaffe.

Boligneforeningen påpeger endvidere, at det – for så vidt angår datakommunikation – i en lang række tilfælde vil være umuligt at indsamle de oplysninger, som bekendtgørelsesudkastet kræver. Det gælder således oplysning om, hvorvidt kommunikationen blev gennemført, om der blev etableret forbindelse til den opkaldte identitet, og i givet fald oplysning om, hvorfor forbindelse ikke blev etableret. Eksempelvis har visse almindeligt anvendte transportprotokoller ikke nogen defineret sekvens eller forløb og dermed ingen afslutning. Det giver i så fald ikke mening at tale om kommunikationens afslutning. Det vil oftest også være umuligt at afgøre, hvorfor en given netværkspakke ikke nåede den opkaldte identitet (serveren var slukket, forbindelsen afbrudt mv.). Boligneforeningen mener på den baggrund ikke, at en registrering af, om kommunikationen blev gennemført, giver mening for datakommunikation, og kravet herom bør således udgå af bekendtgørelsen.

Vedrørende registrering af opkaldende og opkaldte identitet bemærker Boligneforeningen endvidere, at det i relation til datakommunikation ikke står foreningen klart, hvordan en IP-adresse kan anvendes i efterforskningsøjemed, hvis den pågældende IP-adresse ikke identificerer en specifik slutbruger (f.eks. et medlem af en boligneforening) eller en præcis geografisk lokalitet (f.eks. en bestemt lejlighed i boligforeningen). På trods heraf er slutbrugeridentitet (f.eks. navn og CPR-nummer) ikke nævnt i udkastet til bekendtgørelse og vejledning, ligesom lokaliseringsdata ikke er nævnt blandt eksemplerne på de oplysninger, som udbydere skal udlevere til politiet (vejledningsudkastets s. 17). Boligneforeningen finder det meget væsentligt, at det fremgår klart af bekendtgørelsen, hvad der skal forstås ved "opkaldende identitet" og "opkaldte identitet" i forbindelse med datakommunikation. Hvis der med opkaldende identitet menes identiteten på en slutbruger, indebærer det en belastning for boligneforeningerne, som er langt tungere, end det er tilfældet for fastnettelefoni, hvor lokaliseringsdata for kommunikationsudstyret synes tilstrækkelig. Såfremt boligneforeningerne skal identificere slutbrugere, bør det endvidere fremgå af bekendtgørelsen, hvilke identifikationskrav boligneforeninger pålægges i forbindelse med identifikation af medlemmer (f.eks. billedlegitimation i form af pas eller kørekort). Hvis den opkaldende identitet fastlægges ud fra en sammenkobling af IP-adresse med lokaliseringsdata (den fysiske adresse, hvor slutbrugerens kommunikationsudstyr er koblet på udbyderens netværk), bør disse oplysninger anføres blandt de informationer, som udbydere af

datakommunikation ifølge udkastet til vejledning (s. 17) typisk skal udlevere til myndighederne. Anvendelse af trådløse netværk umuliggør i øvrigt en præcis fastlæggelse af geografisk placering.

Boligneтforeningen finder det desuden uklart, hvilke oplysninger der kræves registreret, når en opkaldt IP-adresse uden for foreningen dækker over flere forskellige identiteter. Et ofte forekommende eksempel på dette er såkaldte hosting-firmaer, som giver adgang til hjemmesider, der tilhører flere forskellige domæner. Fastlæggelse af, hvilket domæne der i en sådan situation kaldes op til, forudsætter analyse af kommunikationens indhold og vil påføre boligneтforeninger væsentlige omkostninger til analyseudstyr.

For så vidt angår registrering af elektronisk post anfører Boligneтforeningen, at begreberne afsenders og modtagers e-postadresse er uklart beskrevet i bekendtgørelsesudkastet. Det er eksempelvis muligt at anføre hvad som helst i e-mailens "To"-felt, da det er "RCPT to"-kommandoen i (SMTP-)kommunikationen med e-postserveren, som har betydning for, hvem e-mailen afleveres til. Oplysninger om e-mailadresser er ikke umiddelbart tilgængelige i systemer, der overfører datakommunikation mellem bruger og e-postserver. Det er heller ikke muligt umiddelbart at afgøre, om en given datakommunikation er en e-post. Det er derfor forbundet med betydelige ressourcer at fremskaffe disse oplysninger, idet samtlige IP-pakker, der transporteres i netværket, skal analyseres for tilstedeværelsen af e-postadresser. Elektronisk post bør efter Boligneтforeningens opfattelse alene være omfattet af samme registreringspligt, som gælder for anden datakommunikation (dvs. registrering af IP-adresser mv.). Det forhold, at udbydere af WEB-posttjenester ikke pålægges at registrere e-mailadresser på afsender og modtager, taler også for at opgive dette krav i relation til andre udbydere.

Efter Boligneтforeningens opfattelse er det for al datakommunikation således kun meningsfyldt at registrere opkaldende og opkaldte IP-adresse, tidspunkt, eventuelt TCP-portnummer og geografisk lokalitet forstået som den lejlighed i foreningen, som kommunikationen vedrører.

Boligneтforeningen forstår i øvrigt bekendtgørelsesudkastet således, at datakommunikation mellem to nettermineringspunkter inden for en boligneтforening (det lokale netværk) er omfattet af registreringspligten. Dette indebærer i givet fald, at registreringen både skal foretages på det centrale udstyr, der viderebefordrer kommunikation til og fra Internettet og i de enkelte underkrydsfelter, som forbinder foreningens nettermineringspunkter i et netværk. Udstyret i disse underkrydsfelter (hubs, switche og routere) har i dag ingen eller begrænsede logningsfunktioner, og indkøb af det nødvendige udstyr hertil vil være forbundet med meget betydelige omkostninger. Hvis registreringspligten omfatter informationer, der kun kan fremskaffes ved pak-

keanalyse (f.eks. e-mail adresser eller applikationsprotokoltyper), er det endvidere tvivlsomt, om det rent teknisk er muligt at opfylde registreringspligten ved kommunikation mellem nettermineringspunkter inden for foreningen. Bolignetforeningen mener på den baggrund, at registreringspligten bør begrænses til at omfatte datakommunikation mellem et nettermineringspunkt inden for foreningen og et nettermineringspunkt uden for foreningen.

Digital Rights anfører, at de seneste års udvikling på Internettet, viser en tendens til, at tjenester stilles til rådighed som såkaldte "peer-to-peer" (P2P) snarere end via en central serviceudbyder. P2P forretningsmodellen indebærer, at funktioner stilles til rådighed via software, der installeres på slutbrugerens egen computer, og som kommunikerer direkte med tilsvarende software installeret på andre brugeres computere uden brug af en central server. Eksempler på populære P2P tjenester er fildelingstjenester som KaZaA og IP-telefoni tjenesten Skype. Brugen af P2P tjenester har bredt sig eksplosivt på Internettet. Dette skyldes bl.a., at de kan stilles til rådighed gratis, idet forretningsmodellen indebærer meget små marginalomkostninger, da der ikke skal bruges ressourcer på at drive centrale servere. Som eksempel er softwaren til IP-telefoni tjenesten Skype siden lanceringen i august 2003 blevet hentet af mere en 11 mio. brugere. Da leverandøren af en P2P tjeneste har karakter af en software leverandør, vil de ikke være omfattet af bekendtgørelsen. Rent teknisk vil leverandøren heller ikke have mulighed for at registrere de data, bekendtgørelsen kræver, da det er en integreret del af forretningsmodellen, at der ikke etableres centrale servere. Dette forhold vil underminere bekendtgørelsens effekt for kriminalitetsbekæmpelsen, da store dele af kommunikationen på Internet fremover må forventes at ske via P2P tjenester. Samtidig vil bekendtgørelsen give anledning til teknologisk skævvridning, idet tjenester opbygget omkring centrale servere vil være opfattet af omkostningstunge registreringskrav, mens P2P tjenester ikke vil være det. Man kan således forestille sig, at lavpristelefonselskaber fremover vil vælge en P2P model snarere end tjenester baseret på centrale servere, alene for at undgå registreringsforpligtelsen. Dette vil i givet fald også medvirke til at underminere bekendtgørelsens efterforskningsmæssige effekt.

Rådet for IT-sikkerhed anbefaler, at det afklares, om registrerings- og opbevaringspligten i alle tilfælde kan opfyldes i teknisk henseende, uden at der sker samtidig registrering og opbevaring af indholdsdata. Det vil i øvrigt være i strid med persondataloven, hvis der sker opbevaring af andre oplysninger end de i bekendtgørelsesudkastet nævnte, herunder kommunikationsindholdet i længere tid end udbyderen har behov for af hensyn til egne formål og/eller i henhold til den aftale, som udbyderen har med kunden.

Netudvalget, Kollegiet Studentergården, bemærker, at det er tydeligt, at bekendtgørelsen er udarbejdet ud fra et tankesæt, der muligvis er anvendelig på kredsløbskoblede net, men kun

meget vanskeligt finder anvendelse på moderne pakkekoblede netværk. Det bemærkes videre, at det ikke lader sig gøre på forhånd at skelne informations- og indholdstjenester fra tjenester, der tillige tilbyder mulighed for kommunikation, der kræves registreret. Det altovervejende flertal af datanetværk benytter i dag IP-protokollen, der udgøres af to protokoller: TCP/IP og UDP/IP. UDP-protokollen er forbindelsesløs, idet hver pakke i sig selv både er start og slut på en kommunikation. For at være sikker på at opfylde logningsforpligtelsen vil det således være nødvendigt at registrere hver eneste UDP-pakke, der krydser et datanetværk.

TCP-protokollen er forbindelsesorienteret og har konceptet start og slut på en forbindelse. Det er dog langt fra sikkert, at alle forbindelser, der oprettes med TCP/IP, vil blive afsluttet korrekt med en "slut"-pakke. For at være sikker på at opfylde kravet om at kunne fastslå slutningen på en forbindelse, vil det således være nødvendigt at registrere hver eneste TCP-pakke, der krydser et datanetværk.

Netudvalget påpeger, at hovedparten af data på de fleste netværk udgøres af informations- og indholdstjenester. Da det ikke er muligt maskinelt at skelne mellem på den ene side informations- og indholdstjenester, der tillige giver mulighed for kommunikation, og på den anden side informations- og indholdstjenester, der ikke giver mulighed for kommunikation, indebærer bekendtgørelsesudkastet, at det vil være nødvendigt at registrere al datakommunikation. Hertil kommer, at det ikke er teknisk muligt at overvåge datatrafik, der alene passerer igennem lag 2 netværksudstyr, og som ikke passerer mere "intelligent" lag 3 netværksudstyr, såsom router, firewall eller gateway. Meget ældre udstyr – f.eks. telefonomstillinger – vil endvidere ikke være i stand til at registrere visse former for data – f.eks. gratis interne opkald – og må følgelig udskiftes med store omkostninger til følge for især mindre beboernetværk.

Netudvalget foreslår på den nævnte baggrund, at bagatelgrænsen sættes op til mindst henholdsvis 250 og 600 brugere, og at opbevaringstiden nedsættes til 3 eller 6 måneder. Endvidere foreslås det, at omfanget af data, der skal registreres, indsnævres således, at der ikke er krav om registrering af datatrafik inden for et lokalt netværk og af interne opkald.

Red Barnet anfører, at bekendtgørelsesudkastet ikke forholder sig til nye Internet-teknologier såsom fildeling og messenger-tjenester.

TI og **Cybercity** anfører, at man – med udgangspunkt i anti-terror lovforslaget samt Rådets direktiv 97/66/EF af 15. december 1997 om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren – havde fået den opfattelse, at registrerings- og opbevaringspligten alene skulle omfatte de data, der lagres eller umiddelbart kan lagres af udbyderen

efter en kommunikations ophør, og at den udvidede logningspligt dermed alene indebar, at teleudbyderne skulle undlade at slette allerede registrerede trafikdata i 1 år. Denne forståelse af logningspligten har efter TI's og Cybercitys opfattelse støtte i bemærkningerne til anti-terror lovforslaget, hvor der bl.a. peges på problemstillingen i forbindelse med udbud af "flat rate" abonnementer, herunder ADSL-abonnementer, hvor afregningsformen gør opbevaring af registrerede trafikdata unødvendig. TI og Cybercity finder det på den baggrund både overraskende og vidtgående, at det foreliggende udkast til bekendtgørelse indebærer en pligt for udbyderne til at overvåge, opsamle, registrere og opbevare oplysninger af helt midlertidig karakter, selv om disse trafikdata slet ikke efter de gældende produktionsmetoder registreres og opbevares af teleudbyderne. Bekendtgørelsesudkastet går således videre, end det vedtagne lovforslag forudsatte.

TI og Cybercity anfører i forlængelse heraf, at det er helt uden støtte i anti-terror lovforslaget med tilhørende bemærkninger, når det i udkastet til vejledning (s. 16) fremgår, at politiet i forbindelse med indhentelse af oplysninger om indgående e-mail trafik skal have oplyst dato, tid og unik identitet involveret i alle adgange til e-mailadressen knyttede e-mail. Da der endvidere ikke er tale om oplysninger om tele- eller Internettrafik, finder TI og Cybercity, at vejledningens krav om registrering og opbevaring af disse oplysninger bør opgives. Det er endvidere uacceptabelt, at et så vidtgående krav alene fremgår af vejledningen til bekendtgørelsen.

Endvidere finder TI og Cybercity, at kravet i vejledningen (s. 16) om at registrere IP-adressen for hver enkelt Internetkommunikation, som initieres og termineres hos den enkelte kunde, går ud over hensigten med retsplejelovens § 786, stk. 4. Internettrafik er en såkaldt forbindelsesfri nettjeneste, hvilket indebærer, at selve trafikken på Internettet ikke kan logges. Registrering af data for hver enkelt kommunikation, herunder de IP-adresser, som hver enkelt borger har været i kontakt med, kan kun foretages af udbydere, der for bestemte anvendelser benytter Internettet som adgang til udbud af Internetbaserede tjenester. Det er således udbydere af sådanne tjenester - og ikke Internetudbyderen - som logningspligten i denne sammenhæng kan påhvile.

TI anfører, at den i vejledningen anvendte formulering - i relation til den leverede transmissionsydelse via pakker - kan give det indtryk, at Internetudbyderen skal logge alle adresser i de for brugeren transporterede IP-datagrammer. Det er en ekstremt vanskelig opgave, som både er i strid med Brydensholt udvalgets betænkning og bemærkningerne til anti-terror lovforslaget. TI henviser i den forbindelse til afsnit 3.1.3.2 i lovforslagets omtale af krav til Internetudbydere, hvor det direkte understreges, at der ikke skal foretages en kortlægning af kundernes aktiviteter, mens de anvender Internettet. TI finder på den baggrund også, at forarbejderne til loven udelukker, at http-anvendelsen skal logges. Under henvisning til lovforarbejderne anfø-

rer TI endvidere, at man hverken finder, at der er behov for eller mulighed for at logge sessionstype. Selv om det ikke fremgår klart af udkastet til vejledning, finder TI på den nævnte baggrund ikke, at der findes kommunikationer, som en Internetudbyder skal logge, og logningspligten vedrører dermed alene omsætning mellem bruger og anvendt IP-adresse (ændring af identitet), som slet ikke nævnes i eksemplet. Dette er i overensstemmelse med konklusionen i IT- og Telestyrelsens redegørelse til Forskningsministeriet "Vurdering af de tekniske muligheder og de forbundne omkostninger for Internetudbyderne i Danmark for at kunne foretage en løbende registrering af deres brugeres adfærd på Internettet - oktober 2000". Det bør på den baggrund præciseres, at forslaget ikke indebærer en forpligtelse for udbydere af Internet til at foretage en løbende registrering af kundernes adfærd ved anvendelse af Internettet. Herudover efterlader eksemplet med dial-up adgang til Internet en del tvivl om de foreslåede krav. Som også belyst i den nævnte redegørelse fra IT- og Telestyrelsen, er det yderst vanskeligt at skabe samstemmende oplysninger mellem en Internetudbyder og udbyderen af adgang hertil via det almindelige telefoninet. Eksempelvis logger Internetudbyderen sjældent A-nummer fra telefoninettet, og dette nummer må ikke udleveres til udbyderen, hvis brugeren har hemmeligt nummer. Omvendt har telefoniudbyderen ingen viden om det IP-nummer, som Internetudbyderen tildeler kunden efter dennes opkobling via et fællesnummer i telefoninettet. Realiteten er derfor i de fleste tilfælde, at hverken telefoniudbydere eller Internetudbydere kan levere de sammenkædede data, som udkastet til vejledning (s. 16) kræver.

Efter Cybercitys opfattelse er kravet om logning af hver Internetkommunikation, som kun fremgår af vejledningen, det mest vidtgående og urimelige element i logningsforpligtelsen, og kravet vil nærmest være uoverkommeligt for danske Internetudbydere. Cybercity påpeger i den forbindelse, at en Internetbruger, der anvender såkaldte peer-to-peer tjenester mv. nemt vil kunne generere kommunikation med 200-500 IP-adresser i sekundet. Det vil på grund af omfanget af oplysningerne være næsten umuligt at foretage en brugbar registrering af oplysningerne og efterfølgende bearbejde dem, så de udgør et brugbart datamateriale. Cybercity anslår, at der med det nuværende antal Internetbrugere vil skulle logges mere end én billiard IP-kommunikationer om året.

Cybercity anfører endvidere, at bekendtgørelsesudkastet indebærer, at der skal foretages logning af elektronisk post både hos afsenderen og hos modtageren. Cybercity antager, at der i Danmark dagligt sendes ca. 30 millioner e-mails, hvorfor logningspligten vil indebære, at der skal registreres helt op til 20 milliarder e-mails årligt. Cybercity gør i den forbindelse opmærksom på, at elektronisk post navnlig sendes til og fra postservere i virksomheder, institutioner mv., der efter bekendtgørelsesudkastet ikke er omfattet af logningspligten. Hertil kommer, at elektronisk post afviklet via instant messaging og webmail ikke i praksis vil blive log-

get. I praksis vil der således formentlig kun blive tale om logning af ca. 10 milliarder e-mails pr. år, og den efterforskningsmæssige værdi af logningspligten vil på den baggrund være begrænset.

TI anfører, at IDC har forudsagt, at der på verdensplan vil blive sendt 60 mia. e-mails pr. dag i 2006. Ud fra dette vil et forsigtigt skøn være, at der vil blive sendt ca. 100 mio. e-mails pr. dag i Danmark inklusive SMS, instant messaging beskeder mv. Ønsket om registrering kan således principielt omfatte op mod 30 mia. udvekslinger og dermed 60 mia. registreringer, eller 12.000 pr. indbygger. Imidlertid afvikles e-mail overvejende via postservere i virksomheder, institutioner, kollegier, læreranstalter mv. Post besørget af disse postservere skal efter forslaget ikke registreres. Hertil kommer, at mails afviklet via instant messaging og webmail som tidligere omtalt ikke i praksis kan underkastes en registreringspligt. Det er dermed en ganske begrænset mængde e-mails, der vil blive registreret. Formentlig er der tale om langt mindre end 5 mia. registreringer pr. år og dermed mindre end 10 % af det tidligere nævnte totale antal. Via webmail og forskellige former for instant messaging er det muligt for enhver Internetbruger at skabe en mail-funktion, der ikke er underkastet registrering. Den efterforskningsmæssige værdi af registreringerne må derved med omtalte "huller" og omgåelsesmuligheder være stærkt begrænset. Hertil kommer, at det vil være vanskeligt at opbevare de ønskede oplysninger i en anvendelig form, jf. tidligere bemærkninger herom. Forslaget om logning af e-mails er dermed yderst problematisk. Det bør på den baggrund meget nøje overvejes, om de økonomiske omkostninger ved gennemførelsen af forslaget i sin nuværende form står mål med det forventede udbytte for politiet, henset til de mange nævnte muligheder for at unddrage sig logning.

For så vidt angår telefoni i fastnet, anfører TI og Cybercity, at en stor del af de registrerede telefonopkald ikke vil indeholde et A-nummer, idet f.eks. virksomheder, kommuner og institutioner oftest angiver et fællesnummer som A-nummer. Opkald af denne art fra virksomheder mv. vil således isoleret set ikke have nogen større efterforskningsmæssig værdi, medmindre politiet samtidig har adgang til virksomhedsinterne registreringer. Endvidere skulle registreringer ifølge Brydensholt-udvalgets betænkning især benyttes i forbindelse med elektroniske spor for brug af Internettet, hvor kunder på daværende tidspunkt overvejende brugte modem og telefonforbindelse til adgangen. Imidlertid vil det med de i dag kendte produktionsmetoder være særdeles vanskeligt at spore disse adgange med blot nogenlunde effektivitet gennem registreringer i telefonnettet. A-nummeret logges ikke – som forudsat i Brydensholt udvalgets betænkning – af Internetudbydere ved direkte indvalg, og det vil derfor være vanskeligt i alle tilfælde at benytte logningerne til at udpege tilslutningen til et offentligt telefonnet, som blev benyttet i forbindelse med et efterladt elektronisk spor på Internettet. Oftest vil det således ale-

ne være kundens kundenummer og password, der logges af udbyderen i forbindelse med en dial-in Internet session. I praksis vil udpegningen dermed langt mere effektivt kunne ske gennem kundeidentiteten i Internet og en screening af de sandsynlige forbrugssteder for den pågældende borger. Hvis borgeren med hensigt har sløret sin identitet, er det dog nærliggende at antage, at borgeren også vil benytte en adgangsvej, som alligevel ikke kan spores. Hertil kommer, at adgangen til Internettet via telefonitjenesten er aftagende i takt med udbredelsen af forskellige former for bredbåndsadgang. Det er derfor svært at underbygge det omfattende krav om logning ud fra den oprindelige begrundelse. Almindelige telefonsamtaler kan ligeledes nemt sikres mod logning f.eks. ved anvendelse af instant messaging eller en ren VoIP-tjeneste, hvor der ikke er involveret en udbyder i forbindelse med samtalen. Da udbredelsen af disse kommunikationsformer er stærkt stigende, vil registreringer af taletelefoni (PSTN-telefoni) sandsynligvis være ganske værdiløse i forbindelse med professionelt tilrettelagte forbrydelser.

TI påpeger, at der er ca. 2 mia. opkald og opkaldsforsøg fra mobiltelefoner i Danmark om året. Bekendtgørelsens krav afføder dermed et behov for mindst 4 mia. registreringer af opkaldsforsøg – eller ca. 800 registreringer pr. indbygger. Det er vanskeligt at se den efterforskningsmæssige værdi af registreringer ud over de i dag registrerede trafikdata for afgående opkald, som evt. kan udbygges gennem en sikring af, at lokaliseringsdata opbevares i minimum 1 år. Hertil kommer, at registreringspligten efter TI's opfattelse ikke vil omfatte udenlandske telefoner, der er roamet til Danmark. I praksis vil samtaler ført i udlandet heller ikke kunne registreres ud over de gældende registreringer, der oftest ikke indeholder lokaliseringsdata. Det er dermed let at anvende mobiltelefoner mellem hvilke, opkald ikke kan kræves registreret. Samtidigt vil den stigende brug af adgangen til almene datatjenester i mobilnet, herunder GPRS og 3G-tjenester, øge mulighederne for, at kunderne i både mobilnet og fastnet kan kommunikere indbyrdes via tale og data, uden at der i mobilnettet eller i fastnettet sker en registrering af trafikdata for kommunikationen. TI finder det derfor vanskeligt at se den efterforskningsmæssige værdi af de øgede registreringer af mobilopkald i relation til planlægning og udførelse af alvorlige forbrydelser.

For så vidt angår SMS anfører TI, at antallet af SMS afsendt fra mobiltelefoner i Danmark formentlig snart vil udgøre 6 mia. om året. Det giver efter forslaget anledning til 12 mia. registreringer eller ca. 2.400 pr. indbygger. Efter forslaget skal også SMS afsendt fra fastnettet registreres. Det kan ske ved den ligeledes foreslåede registrering af afsendte e-mails. TI henleder i den forbindelse opmærksomheden på, at afsendende identitet ikke i almindelighed vil fremgå af trafikdata tilgængelige i modtagende mobilnet. Det gælder både e-mail adresse fra fastnettet og afsendernummer fra afsendende mobiltelefon. Dette skyldes, at denne information er en del af indholdsdata for den terminerende SMS. Principielt kan funktionerne i et mobilnet

og SMS-C adskilles og varetages af forskellige organisationer. Dette er f.eks. ofte tilfældet for gensælgere. I sådanne tilfælde vil originerende mobilnet ikke kunne logge det nummer, som en SMS sendes til, da denne information er en del af indholdsdata, og den endelige modtager af SMS er alene kendt af SMS-C. Med udbredelsen af datatjenester i mobilnet er det eksempelvis via GPRS muligt at sende besked til en anden mobilbruger, uden at dette kan registreres i de involverede mobil- og fastnet. Disse muligheder for at omgå registrering af beskedudveksling vil øges med den forudsete tjenesteudvikling.

TI påpeger endvidere, at reglerne bør udformes, så det også er muligt at gennemskue, hvilke krav udbydere skal opfylde i relation til nye ydelser. Det er f.eks. ikke klart, i hvilket omfang lokaliseringsdata skal foreligge for VoIP-tjenester udbudt via Internettet eller Internetadgang udbudt via hot spots.

TI anfører, at bekendtgørelsesudkastets § 2, hvorefter registreringspligten bl.a. omfatter oplysninger om en kommunikation, som initieres, transmitteres eller termineres som led i udbuddet af telenet eller teletjenester, indebærer, at hver enkelt kommunikation som minimum skal registreres i såvel a- som b-nettet (dvs. både det originerende og det terminerende net) samt i eventuelle transiterende net. Dette betyder, at langt de fleste kommunikationsoplysninger i praksis vil blive registreret dobbelt eller tredobbelt. Da dette meget væsentlige aspekt af logningsforpligtelsen slet ikke er omtalt i bemærkningerne til anti-terror lovforslaget eller i justitsministerens besvarelser af Retsudvalgets spørgsmål i forbindelse med lovforslagets behandling, må det antages, at man ved lovens tilblivelse alene har forudsat, at registreringerne skal foretages i a-nettet. Derimod fremgår det af bemærkningerne, at lovforslaget for så vidt angår logning af trafikdata bl.a. blev fremsat ud fra en formodning om, at trafikdata i visse tilfælde slettes umiddelbart efter kommunikationen er gennemført og derfor ikke er tilgængelige for politiet i forbindelse med efterforskning. I de specielle bemærkninger vedrørende logning af teletrafikdata nævnes det, at det er vigtigt at sikre, at der sker registrering af teleoplysninger i traditionel forstand, dvs. oplysninger om a- og b-nummer, opkaldstidspunkter og varigheden af samtaler (pkt. 3.1.3.1). Med hensyn til Internettrafikdata anføres det, at formålet med den foreslåede regulering er at sikre, at de elektroniske spor, der findes på Internettet i tilknytning til en kriminel aktivitet, ikke ender blindt hos Internetudbyderen. Dette forudsætter ifølge bemærkningerne, at Internetudbyderen er i besiddelse af præcise oplysninger om, hvilken kunde der på et givet tidspunkt har anvendt en tildelt IP-adresse. Videre fremgår det, at registrering af det kaldende nummer (a-nummeret) vil være relevant, hvor forbindelsen til Internetudbyderens server er etableret via telefonnettet. Registrering af b-nummeret anføres at være relevant, hvor udbyderen stiller flere forskellige forbindelser til rådighed for deres kunder med henblik på at etablere forbindelse til Internettet. Logning af oplysninger vedrørende brug af elektronisk post

forudsættes tilsvarende at skulle omfatte oplysninger om afsender, modtager og tidsangivelse vedrørende kommunikationen (pkt. 3.1.3.2). TI fremhæver i den forbindelse, at der ikke i forbindelse med behandlingen i Retsudvalget er fremkommet oplysning om, at logningspligten generelt kunne rettes mod b-nettet. Tværtimod synes det også her forudsat, at kravet alene skulle rettes mod a-nettet. TI henviser i den forbindelse til Justitsministeriets besvarelse af spørgsmål nr. 123 (L 35 - bilag 123) angående omkostningerne i forbindelse med den foreslåede registreringspligt samt til et notat af 17. december 2002 udarbejdet af Ministeriet for Videnskab, Teknologi og Udvikling til brug for et møde den 19. december 2002 mellem telebranchen, Justitsministeriet og Videnskabsministeriet. Af notatet fremgår bl.a., at der kan fastsættes regler om registrering af det kaldende og kaldte nummer (i den nævnte rækkefølge). TI har på den nævnte baggrund været overbevist om, at kravet om registrering kun ville omfatte b-nettet i de meget specielle tilfælde, hvor der er dial-up adgang til Internet.

I forlængelse heraf bemærker TI, at det forekommer uklart, hvad der nærmere ligger i udkastets § 2, stk. 3, herunder om bestemmelsen netop vedrører denne dobbelte registrering af hver enkelt kommunikation. I givet fald (og forudsat, at kravet fastholdes) bør dette præciseres, herunder således, at registreringspligten består, medmindre den enkelte udbyder træffer eksplicit aftale med en anden udbyder om, at denne sørger for opfyldelse af forpligtelsen. I modsat fald efterlader bestemmelsen et juridisk tomrum, hvor visse (formentlig især mindre) udbydere – måske med rette – forlader sig på, at registreringen foretages i andre net, og at de dermed ikke overtræder bekendtgørelsen ved at undlade at gemme trafikdata.

For så vidt angår spørgsmålet om, hvilke trafikdata der skal registreres i medfør af bekendtgørelsesudkastet, anfører TI, at det efter ordlyden af § 2 er alle de i stk. 1 nr. 1-8 nævnte oplysninger, der skal registreres i forbindelse med enhver kommunikation. TI forudsætter, at denne registreringspligt i praksis reduceres til praktisk forekommende trafikdata blandt de oplistede for den enkelte tjenestetype. Dette underbygges af de i vejledningen angivne eksempler på anmodninger om udlevering af data, hvor der eksempelvis ikke ønskes lokaliseringsdata i tilknytning til opkald i det faste telenet. Det er åbenbart, at lokaliseringsdata ikke er relevante i nævnte tilfælde.

I mange andre tilfælde skaber bekendtgørelsesudkastets krav imidlertid stor tvivl om den praktiske rækkevidde af kravene for en konkret tjeneste. Eksempelvis giver vejledningen indtryk af, at lokaliseringsdata (bekendtgørelsens § 2, stk. 1, nr. 6) skal registreres i forbindelse med kommunikation via GPRS og i forbindelse med udveksling af MMS. Imidlertid registreres lokaliseringsdata ikke i forbindelse med nævnte kommunikationer i de fleste mobilnet. Dette skyldes, at de pågældende tjenester er baseret på åbne logiske kanaler, der typisk er aktiveret

så længe terminalen er tændt. Transportnettet opdateres løbende i takt med kundens skift mellem celler, men denne oplysning benyttes alene til en dynamisk opdatering af rutningsdata. Der er derfor hverken anledning til eller behov for logning af lokaliseringsoplysninger for den enkelte kommunikation. I de tilfælde, hvor GPRS benyttes til eksempelvis meddelelser på højere niveau i forhold til mobiltjenesten - evt. via en af mobiludbyderen uafhængig e-mail udbyder - vil der ikke foreligge en registrering af kommunikationen i mobilnettet bortset fra de kvantiseringer af volumenforbruget, som benyttes til volumentaksering. Hvis der skal registreres lokaliseringsdata i forbindelse med MMS og kommunikation via GPRS generelt, kan dette alene ske ved en logning af al celleinformation i tilknytning til den logiske kanal, der benyttes som bærer, og en efterfølgende tidsmæssig matchning af disse poster med genererede poster for kommunikation. Dette vil være en ekstremt omfattende opgave, og det vil indebære, at der sker en logning af kundens adfærd uafhængigt af kommunikationer til og fra den pågældende. Derved er de opsamlede informationer om celler ikke trafikdata, og kravet fører således til en utilsigtet og ganske omfattende registrering af brugerens adfærd. En sådan registrering er helt åbenbart ikke omfattet af logningsforpligtelsen, jf. f.eks. Justitsministeriets besvarelse af Retsudvalgets spørgsmål nr. 147 (L 35 - bilag 127). Det præciseres i svaret, at logning af oplysninger om, hvilken sendemast en tændt mobiltelefon har forbindelse til, når den ikke anvendes til kommunikation, efter Justitsministeriets opfattelse ikke er en oplysning om teletrafik i relation til § 786, stk. 4. Heraf følger, at det vil være direkte retsstridigt at registrere sådanne oplysninger, idet det i givet fald vil være en overtrædelse af udbudsbekendtgørelsens § 29, da henvisningen til retsplejeloven alene findes i § 28 om registrering af trafikdata, men derimod ikke i § 29 om registrering af lokaliseringsdata, der ikke samtidig er trafikdata.

Et andet eksempel findes i bekendtgørelsesudkastets § 2, stk. 1, nr. 8, som bestemmer, at logningspligten også omfatter en pligt til registrering af oplysninger om identiteten på det benyttede kommunikationsudstyr.

Vejledningen til bekendtgørelsen nævner specifikt, at dette omfatter IMEI-numre for mobilterminaler og MAC-adresser for computere i forbindelse med opkobling til Internettet. Disse unikke identiteter tildeles under produktionen af udstyret, men da identiteten kan ændres af senere brugere, er det vanskeligt at se formålet med denne del af logningskravet. Eksempelvis kan MAC-adresser på langt det meste udstyr forholdsvist enkelt ændres ved brug af en funktionalitet i operativsystemet. Visse typer systemer anvender endda dette aktivt i forbindelse med fordeling af forespørgsler mod enkelte enheder. IMEI-numre på mobilterminaler kan endvidere på visse typer mobilterminaler ændres ved brug af specialudstyr og software, som er frit tilgængeligt på Internettet. Det nævnte eksempler viser, at de generisk beskrevne krav i bekendtgørelsen ikke i praksis er anvendelige inden for de i lovforslagets bemærkninger angivne præ-

misser. Trafikdata, som for nogle tjenester umiddelbart foreligger i en registrerbar form, vil for andre tjenester medføre ganske omfattende nye registreringer, der som illustreret ved førstnævnte eksempel tilmed i sig selv kan repræsentere et brud på de angivne præmisser. Eksemplet illustrerer også, at begrebet trafikdata må vurderes i forhold til den stadig mere udbredte lagdelte produktion af teleydelser, hvor alle informationer ikke er tilgængelige i et fælles system.

TI finder endvidere, at der på tilsvarende vis knytter sig en betydelig usikkerhed til betydningen af flere af de ønskede data i forbindelse med mange andre konkrete tjenester. Eksempelvis er ændring af opkaldende og opkaldte identitet vanskelig at omsætte til praktiske begreber. I vejledningen anføres telekort som et eksempel, og der sker omtale (afsnit 6.3.2) af muligheden for, at en lokalt udbudt tjeneste registrerer den egentlige slutbruger, hvis et opkald ud i andre net ikke afspejler denne via et individuelt A-nummer. Tilsyneladende er formålet hermed, at registreringer i det offentlige net efterfølgende kan parres med registreringer af ændringer i identiteten. Bag fremgangsmåden anes imidlertid en opfattelse af, at A- og B-numre mellem net forvaltes på en konsekvent og entydig måde. Dette er ikke nødvendigvis tilfældet. Mange kald mellem net indeholder ikke et A-nummer eller det angivne A-nummer afspejler ikke den kaldende slutbruger. Det bliver også mere og mere almindeligt, at kaldenummeret er et personligt nummer eller et servicenummer, som på dynamisk vis benyttes til valg af det endelige svarsted. Hvis servicenummeret forvaltes af et andet net end originerende eller terminerende net, vil mapningen for et aktuelt kald slet ikke blive registreret. Der er således flere eksempler på, at kaldende net ikke kan registrere opkaldte identitet og/eller ændringer heri. Tilsvarende kan opkaldte net ikke registrere kaldende identitet eller ændringer heri.

Specielt for ændring af identitet er der behov for en præcisering af omfanget i forhold til geografisk begrænsede tjenester, der skal foretage registrering fra 1. juli 2006. Efter ordlyden i vejledningen indebærer kravet, at eksempelvis hoteller, Internetcaféer, hot spot tjenester og private hospitaler mv. skal logge data for såvel afgående som ankommende trafik med ændringer af identiteter. I visse tilfælde vil brugen af enkeltstående betalingstelefoner ved hjælp af et identificerbart kort muligvis også skulle logges. Omfanget af disse pligter må nødvendigvis tydeliggøres, da fortolkningen af identitet ikke forekommer åbenbar ved disse anvendelser. Det er f.eks. ikke klart, om registrering af identitet indebærer registrering af f.eks. værelsesnummer, apparatnummer eller navn på den pågældende hotelgæst.

IT-Brancheforeningen anfører, at der er usikkerhed om, hvilke oplysninger der skal registreres i henhold til bekendtgørelsesudkastets § 1. Det giver for det første stor usikkerhed om rækkevidden af kravene i forbindelse med tjenester, der ikke er omtalt. Skal en udbyder af VoIP

eksempelvis registrere lokaliseringsdata, hvis kunden har mulighed for at anvende tjenesten fra flere lokationer. For det andet er der - for de i vejledningen angivne eksempler - stor usikkerhed om kravenes praktiske rækkevidde, og flere af de ønskede oplysninger kan ikke registreres uden meget omfattende nye overvågnings- og registreringsfunktioner, som i sig selv er i strid med lovgrundlaget for bestemmelserne. Eksempler herpå er lokaliseringsdata i forbindelse med GPRS, hot spot og andre mobile datatjenester. Registreringspligtens rækkevidde er endvidere uklar i relation til bl.a. roamede kunder i Danmark, danske roamede kunder i udlandet, opbevaring af data, kontokald, tjenester udbudt internationalt. Omfang af kravene og de mange uklarheder indebærer i praksis, at udbydere ikke har mulighed for at efterleve de foreslåede regler pr. 1. juli 2005.

Catpipe Systems påpeger, at mange tjenester i dag fungerer som en kombination af forskellige protokoller f.eks. Webmail, hvor afsender arbejder med http (normalt port 80), mens modtager arbejder på andre porte (f.eks. port 25 (SMTP) eller 110 (POP3)). Således er det ikke muligt uden et indgående kendskab til applikation-sammensætningen at udelukke specifikke protokoller eller porte. For chat-tjenester er tilsvarende forhold gældende, og det er for disse desuden almindeligt, at deres port-allokering er dynamisk og derfor umulig at forudbestemme. De nævnte forhold indebærer, at udbydere i praksis vil skulle registrere og opbevare alle connection, hvilket for mange virksomheder inden for branchen vil være en uoverkommelig opgave. Når man tillægger kravet om et døgnbetjent kontaktpunkt, vil udbyderne samlet blive pålagt store driftsudgifter. Catpipe Systems vil sikre seriøse løsningsmuligheder, men udgiften vil skulle bæres af udbyderne, hvilket bl.a. vil vanskeliggøre påbegyndelse af ny virksomhed inden for branchen. Catpipe Systems mener i øvrigt, at de registrerede kontakt-profil data ikke vil have nogen værdi som bevis. En IP-adresse eller et A-nummer vil således kun kunne antyde en kommunikation mellem bestemte personer, da der er flere muligheder for at sløre eller forfalske sådan kommunikation. Dette indebærer samtidig, at der er stor risiko for, at uskyldige inddrages i efterforskningen. Selv om Catpipe Systems havde været enig i indholdet af udkastet til bekendtgørelse og vejledning, ville man alligevel være betænkelig ved, at der overlades politiet et sådant redskab, idet politiet ikke besidder den tilstrækkelige indsigt i Internettets protokoller og mulighederne for at lave falske mails og for at udgive sig for at være en anden, end den man er.

Damm Cellular Systems A/S gør opmærksom på, at det i et Tetra telenet ikke er muligt at registrere opkaldte identitet ved almindelige gruppekald, og at lokaliseringsdata registreres på opkaldstidspunktet.

G. SPØRGSMÅL VEDR. TIDSANGIVELSE

TI anfører vedrørende vejledningens krav om en nøjagtighed på 1 sekund for tidsregistreringer, at denne nøjagtighed hverken er omtalt i Brydensholtudvalgets betænkning, lovforslagets bemærkninger eller den foreslåede bekendtgørelse. I telenet er der sjældent behov for en sådan præcision af den absolutte tid, da taksering beror på samtalers varighed, der måles meget nøjagtigt, eller volumen af overført datamængde. Derfor kan den absolutte tid i registrerende enheder ofte variere betydeligt fra sand tid. Ofte er tidsstemplet for en registrering i nettet slet ikke relateret til sand tid. Tidsangivelsen kan f. eks. angive tidsperiode siden sidste opstart eller en anden hændelse i systemet. Associering til sand tid vil i sådanne tilfælde først ske i forbindelse med indsamling og central logning af de poster, der er dannet i nettet. Eksemplet viser, at kravet om nøjagtighed af tidsstempler er i modstrid med produktionsforudsætningerne, og det vil derfor ikke kunne opfyldes på kortere sigt. Det vil samtidigt sætte betydelige begrænsninger for udformningen af effektive telenet i fremtiden. TI finder derfor, at kravet om et sekunds nøjagtighed, der bør fremgå af bekendtgørelsen, alene skal gælde tidsstempling af de i nettet opsamlede dataposter med trafikdata.

H. DØGNBETJENT KONTAKTPUNKT

Advokatrådet anfører, at bestemmelsen i bekendtgørelsesudkastets § 7 om pligt til at etablere et døgnbetjent kontaktpunkt, vil kunne risikere at skade navnlig de mindre teleudbyderes konkurrenceevne og muligvis forhindre nye aktørers adgang til telemarkedet. På den baggrund finder Rådet, at kravet om etablering af et døgnbetjent kontaktpunkt bør lempes.

Bolignetforeningen finder det vanskeligt at se den efterforskningsmæssige logik bag kravet om et døgnbetjent kontaktpunkt, idet formålet hermed synes at være hensynet til hurtig bevissikring. Da bekendtgørelsesudkastet netop indebærer, at trafikdata automatisk skal registreres og opbevares i et år, er beviset sikret uden politiets indgriben. Kravet om etablering af et døgnbetjent kontaktpunkt er endvidere besynderligt, idet bekendtgørelsen ikke indeholder nogen frist for udbydernes udlevering af oplysningerne til politiet. Omkostningerne til et døgnbetjent kontaktpunkt vil ifølge Bolignetforeningen årligt udgøre ca. 3 mio. kr. Bolignetforeningen foreslår ud fra de nævnte betragtninger, at kravet om et døgnbetjent kontaktpunkt erstattes af frister for udbydernes udlevering af oplysningerne til politiet.

I. OPBEVARING OG VIDEREGIVELSE AF OPLYSNINGER TIL POLITIET

Rigspolitichefen og Politiets Efterretningstjeneste (PET) påpeger, at det bør fremgå udtrykkeligt af bekendtgørelsesudkastets § 8, at oplysninger om teletrafik skal videregives til politiet i *elektronisk* form, da der vil kunne være tale om betydelige datamængder. PET bemærker i øvrigt, at bekendtgørelsesudkastet er i overensstemmelse med hovedtrækkene i det forslag til rammeafgørelse om registrering og opbevaring af oplysninger om teletrafik (CRIMORG 36 8958/04), som den 28. april 2004 er fremsat af Frankrig, Irland, Sverige og Storbritannien.

TI og **Cybercity** anfører, at det er uklart, hvad der i bekendtgørelsesudkastets § 8 menes med, at oplysningerne skal videregives i læsbart format. Det påpeges i den forbindelse, at det vil være forbundet med endog meget store omkostninger, hvis trafikdata skal organiseres på en sådan måde, at politiet kan få udleveret teletrafikdata vedrørende én bestemt bruger. F.eks. vil det være en ekstremt omfattende opgave at bearbejde registreringer i e-mailsystemer, kopiere dem og organisere dem efter den enkelte kundes kommunikationer og adgang til e-mailkontoen. I øvrigt vil alene eksistensen af et sådant samlet arkiv over borgernes adfærd være betænkelig. TI og Cybercity finder på den baggrund ikke, at bekendtgørelsesudkastets krav om læsbarhed bør kunne udstrækkes til at omfatte en pligt for den enkelte udbyder til at sammenkøre registrerede trafikdata. En sådan sammenkøring må i stedet skulle foretages af politiet. Justitsministeriet anmodes i den forbindelse om at bekræfte, at den enkelte udbyder udelukkende vil være forpligtet til at opbevare trafikdata i et format, som er tilpasset produktionsformen og mulighederne for at registrere trafikdata.

Boligneforeningen bemærker, at der reelt er tale om, at boligneforeninger nu skal udføre politimæssige overvågnings- og efterforskningsopgaver. Boligneforeningerne kan ikke forventes at ligge inde med den tekniske, økonomiske og administrative kompetence til at løfte den politimæssige opgave på forsvarlig vis. Logningen bør derfor i givet fald – for boligneforeningernes vedkommende – gennemføres af en uafhængig ekstern partner (f.eks. Datatilsynet), og omkostningerne hertil bør afholdes af politiet. Denne dataopbevarende myndighed bør desuden kunne bistå udbyderne med gratis konsulentbistand med henblik på at sikre, at registreringen af data foregår på en korrekt måde. Det er endvidere problematisk, at boligneforeninger i medfør af bekendtgørelsesudkastet vil skulle opbevare personfølsomme oplysninger om medbeboere. Boligneforeningen finder endvidere ikke, at bekendtgørelsen er tilstrækkelig klart afgrænset i forhold til reglerne i bl.a. persondataloven. Som bekendtgørelsesudkastet er udformet, vil det reelt være umuligt for boligneforeninger at administrere deres netværk på en måde, der hverken strider mod logningspligten eller persondataloven.

TI anfører, at reglerne for udbydere af offentlige tjenesters opbevaring af trafikdata er sort/hvide, idet pligten til i medfør af bekendtgørelsesudkastet at opbevare trafikdata i princippet erstattes af en pligt til at slette eller anonymisere data i samme øjeblik, der er gået mere end ét år siden registreringen. Det vil i mange tilfælde være umuligt at forvalte loggede data med den krævede præcision, uden at der sker omlægning til nye og ganske kostbare opbevaringssystemer. På tilsvarende måde vil det være ganske vanskeligt at ændre procedurerne, hver gang grænserne for undtagelserne (100 hhv. 400) passeres. Hvis det er vurderingen, at de undtagne områder efter § 3 stk. 1, nr. 1, og nr. 3, § 3 stk. 2, nr. 1, og nr. 2, ikke kan være udbydere af offentlige telefonitjenester omfattet af § 28 i udbudsbekendtgørelsen, vil den deraf følgende fjernelse af brugernes beskyttelse mod opbevaring af og brug af trafikdata efter TI's opfattelse være urimelig og muligvis i strid med databeskyttelsesdirektivet (2002/58/EF). TI finder derfor, at samspillet mellem de foreslåede regler og udbudsbekendtgørelsen/generelle persondataretlige regler må gøres mere smidigt, så det bliver muligt i praksis at efterleve begge regelsæt. TI finder det desuden uheldigt, at bekendtgørelsesudkastets § 6, stk. 4, fastsætter, at bistand til politiet og efterkommelse af pålæg, skal ske "snarest muligt" og "i overensstemmelse med politiets anvisninger." TI gør i den forbindelse opmærksom på, at der er tale om forpligtelser for udbyderne.

J. SIKKERHEDSMÆSSIGE KRAV I FORBINDELSE MED REGISTRERING OG OPBEVARING AF OPLYSNINGER OM TELETRAFIK MV.

Datatilsynet anfører, at det giver anledning til tvivl, i hvilket omfang det er reglerne i persondatalovens § 41, stk. 3, eller reglerne i udbudsbekendtgørelsens § 31, stk. 1, der fastsætter de sikkerhedsmæssige krav til udbydernes behandling af oplysningerne om teletrafik. Dette rejser samtidig spørgsmål om, hvorvidt det er Datatilsynet eller IT- og Telestyrelsen, der har kompetence til at føre tilsyn med datasikkerheden. Datatilsynet vil søge kompetencespørgsmålet afklaret ved henvendelse til IT- og Telestyrelsen.

Institut for Menneskerettigheder påpeger, at det er af afgørende betydning, at behandlingen af de teletrafikdata, som skal opbevares i medfør af udkastet til bekendtgørelsen, lever op til de standarder, som persondataloven og Den Europæiske Menneskerettighedskonvention foreskriver. Da bekendtgørelsesudkastet bl.a. retter sig mod private aktører, finder Instituttet imidlertid, at der er behov for at fastsætte nogle sikkerhedsforskrifter vedrørende opbevaring og tilgang til loggede teletrafikdata, der er mere præcise end de regler, der gælder efter persondataloven. Et eksempel kunne være krav om logning af tilgang til datamaterialet kombineret med krav om godkendelse for at kunne tilgå datamaterialet.

IT-Brancheforeningen fremhæver, at foreningen for tiden er i dialog med Datatilsynet og Internet-udbyderne om opbevaring af kunderelaterede data. Foreningen har på møderne med Datatilsynet efterspurgt en afklaring af samspillet mellem reglerne om databeskyttelse og reglerne om logning af trafikdata, og dermed en sikkerhed for, at branchen ikke ville komme i klemme mellem to myndigheder med hver sin fortolkning af de respektive regelsæt. Behovet for afklaring omhandler både de to regelsæts forskellige krav til opbevaringsperiodens længde og spørgsmålet om, hvilke typer data de to regelsæt hver især angår. Foreningen går ud fra, at Justitsministeriet sørger for en sådan afklaring, inden bekendtgørelsen sættes i kraft. Dette kunne eksempelvis ske ved, at samspillet beskrives nærmere i den tilhørende vejledning.

Digital Rights anfører, at den omfattende registrering af bl.a. afsender- og modtageradresse på e-mail uvægerligt vil forøge risikoen for, at oplysninger om borgerens private forhold misbruges eller kommer i forkerte hænder. Hertil kommer, at bekendtgørelsen indebærer, at private aktører, som f.eks. boligforeninger eller mindre foreninger, som tilbyder chat-tjenester, involveres i en omfattende registrering af deres brugere. I forhold til traditionelle teleudbydere vil disse aktører ikke have nogen erfaring med den tekniske håndtering af en sådan registrering. Samtidig vil de typisk ikke have sikre IT-systemer til rådighed eller ressourcer til at etablere disse. Konsekvensen af dette kan være, at der opstår alvorlige sikkerhedsproblemer omkring de registrerede data. Dette forværres af, at udbyderne i mange tilfælde vil være i tæt kontakt til eller måske ligefrem været kontrolleret af mennesker, som har personlige interesser i de data, som registreres. Dette vil f.eks. gælde udbydere i boligforeninger, som typisk vil være i tæt kontakt til beboerne og i mange tilfælde ejet eller kontrolleret af disse. I modsætning til en professionel og uafhængig teleudbyder, kan man frygte, at det for de teknisk ansvarlige i en sådan brugerstyret organisation kan være vanskeligt at modstå et eventuelt pres for at give uautoriseret adgang til data.

Rådet for IT-sikkerhed finder, at det kan give anledning til tvivl, i hvilket omfang det er reglerne i persondatalovens § 41, stk. 3, eller reglerne i udbudsbekendtgørelsens § 31, stk. 1, der fastsætter de sikkerhedsmæssige krav til udbyderes behandling af oplysninger om teletrafik. I konsekvens heraf opstår der samtidig tvivl om, hvorvidt det er IT- og Telestyrelsen eller Datatilsynet som har tilsynskompetencen. Der henvises blandt andet til persondatalovens § 2, stk. 1. Det anbefales, at dette kompetencespørgsmål afklares. Endvidere anbefaler rådet, at der i bekendtgørelsen indsættes en bestemmelse om tekniske og organisatoriske sikkerhedsforanstaltninger, herunder af IT-sikkerhedsmæssig karakter med henvisning til de relevante love på området, samt at det i vejledningen nærmere uddybes, hvem der har tilsynskompetencen.

Karina Pedersen

Fra: Justitsministeriet
Sendt: 14. maj 2004 11:37
Til: JOURPolitikontoret
Emne: VS: Justitsministeriets sagsnr. 2002-945-0922

-----Oprindelig meddelelse-----
Fra: Martin Broms [mailto:MBR@domstolsstyrelsen.dk]
Sendt: 14. maj 2004 11:35
Til: Justitsministeriet
Emne: Justitsministeriets sagsnr. 2002-945-0922

Vedhæftet sendes Domstolsstyrelsens høringssvar.

Med venlig hilsen
Martin Broms
Fuldmægtig
Direkte + 45 33 92 95 95
mbr@domstolsstyrelsen.dk

Domstolsstyrelsen
Administrationskontoret
St. Kongensgade 1-3
1264 København K.
Tlf. + 45 70 10 33 22
Fax + 45 70 10 44 55
www.domstolsstyrelsen.dk

Domstolsstyrelsen

Justitsministeriet
Civil- og Politiafdelingen
Slotsholmsgade 10
1216 København K

Administrationskontoret
St. Kongensgade 1-3
1264 København K
Tlf. 70 10 33 22
Fax 70 10 44 55
post@domstolsstyrelsen.dk
CVR nr. 21-65-95-09
Jeres j.nr. 2002-945-0922.
MBR10693/Sagsbeh. MBR
J.nr. 02.01.01.2004-19.2

14. maj 2004

Udkast til bekendtgørelse og vejledning

Justitsministeriet har ved brev af 24. marts 2004 anmodet Domstolsstyrelsen om en udtalelse om udkast til bekendtgørelse og vejledning om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

Vi har ikke bemærkninger til forslaget.

Med venlig hilsen

Martin Broms

Karina Pedersen

Fra: Justitsministeriet
Sendt: 17. maj 2004 07:55
Til: JOURPolitikontoret
Emne: VS: Høringssvar vedr. logningsbekendtgørelse

Høringssvar vedr. logning fra ...

-----Oprindelig meddelelse-----
Fra: Niels Vestergaard Jensen [mailto:niels@digitalforbruger.dk]
Sendt: 15. maj 2004 12:21
Til: Justitsministeriet
Cc: DFD's bestyrelse
Emne: Høringssvar vedr. logningsbekendtgørelse

Att: Lennart Lindblom

Høringssvar vedr. "Høring vedr. udkast til bekendtgørelse og vejledning om telenet og teletjenesteudbyderes registrering og opbevaring af oplysning om teletrafik samt praktisk bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden"

Se venligst Digital Forbruger Danmarks høringssvar i vedlagte fil.

med venlig hilsen

Niels Vestergaard Jensen

Digital Forbruger Danmark

Akt.nr. 84.
Justitsministeriet 2002 NR. 945-0922
Politikontoret

Ryparken d. 15. maj 2004

Justitsministeriet
att: Lennart Lindholm
Slotsholmsgade 10
1216 København K

Vedr. "Høring vedr. udkast til bekendtgørelse og vejledning om telenet og teletjenesteudbyderes registrering og opbevaring af oplysning om teletrafik samt praktisk bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden"

Digital Forbruger Danmark (DFD) er en forening, som arbejder for at bevare forbrugernes og borgernes rettigheder i overgangen til det digitale rum. Nærværende udkast til bekendtgørelse er en alvorlig indgriben i vores interessesfære, hvorfor vi sender dette høringssvar.

Generelle bemærkninger

DFD ser nærværende udkast som en uhørt krænkelse af borgernes privatliv og det mest alvorlige brud på traditionelle borgerrettighedsprincipper i nyere tid. Bekendtgørelsens indhold bygger på en idé om total systemkontrol man i den fysiske verden ville betragte som udemokratisk og usmagelig. Dette er specielt alvorligt da telekommunikation dagligt bliver en vigtigere del af forbrugernes hverdag.

DFD anbefaler derfor at bekendtgørelsen trækkes tilbage.

Mere konkret ser vi i DFD 4 væsentlige problemstillinger, som bekendtgørelsen skaber for det danske samfund: (1) den betragter internettets brugere som passive, (2) den giver grobund for utryghed og mistro, (3) den er en økonomisk byrde og vil lægge en dæmper på mange positive aktiviteter og (4) den er uigennemtænkt og virkningsløs.

(1) Bekendtgørelsen betragter internettets brugere som passive

Bekendtgørelse antager at internettet består af få aktive udbydere af services (teletjenester) og mange passive forbrugere. Men sådan fungerer internettet langt fra. En stor del af af de services (teletjenester) som udbydes på internettet, udbydes af forbrugerne selv. Enten ved brug af den megen software (fx online spil) som sætter forbrugeren i rollen af aktiv udbyder af services (teletjenester). Eller ved de utallige aktive og privatehjemmesider som brugerne og communities (uformelle fællesskaber) hoster enten på et webhotel eller egen PC. I onlinespil er det ofte sådan at en enkelt spiller "hoster" et spil på sin PC, som andre spillere kan logge sig på. Når man "hoster" et spil, bliver man udbyder af services (teletjeneste), da PC'en står for at udveksle data (bla. kommunikation) imellem spillerne. Lignende situation kommer brugerne af de populære p2p/fildelingstjenester ud for. Mange bruger også deres PC'er som en server, hvor de så tilbyder en række teletjenester. Det kan fx være deres egen hjemmeside med chatrum, blog, gæstebog og debatfora. Eller "Wikiboards", som er en populær måde for store og små fællesskaber at skabe vidensdatabaser. Alle services (teletjenester) som bekendtgørelsen pålægger at forbrugerne skal gennemføre en overvågning og registrering af aktiviteter. Vi kan ikke give en udtømmelig liste over eksempler, hvor den almindelig internetbruger bliver udbyder af services (teletjenester), da den er meget lang og der dagligt opstår nye muligheder. Men det er vores overbevisning at en overvejende del af internettets aktiviteter og services (teletjenester) udspringer fra internettets communities og brugerne selv.

(2) Bekendtgørelsen giver grobund for utryghed og mistro

Jvf. (1) vil majoriteten af aktive danske internetbrugere opleve at de skal efterleve bekendtgørelsens krav om overvågning og registrering af danskernes aktivitet på internettet, hvilket sætter dem i rollen som myndighedernes repræsentant. En rolle, som både er ubehagelig for den der har rollen som myndighedernes "vagthund", men også for dem der bliver overvåget. F.eks. vil det for

boligforeninger med eget netværk øge mistroen mellem de beboere, som forestå driften af netværket, og resten af beboerne. Alt andet lige vil der jo være større risiko for misbrug jo mere data der gemmes, og misbrugeren vil kunne dække sin snagen bag lovens krav - en meget utryg situation for den enkelte beboer. De samme etiske problemer gør sig gældende for internettets utallige communities. Mao. vil bekendtgørelsen skabe etiske problemer og latente konflikter for majoriteten af internettes aktiviteter.

(3) Bekendtgørelsen er en økonomisk byrde og vil lægge en dæmper på mange positive aktiviteter.

Mange af internettets aktiviteter og services (teletjenester), er nonprofit aktiviteter, som er forankret i communities og enkeltindivider. Arbejdet, som ligger i at udbyde aktiviteterne, sker på frivillig basis, og lader sig kun realisere takket være internettets åbne natur og den nemme adgang til fri og gratis software. For de fleste communities er der ingen økonomi involveret. Men skal disse communities og enkeltindivider til at efterleve bekendtgørelsens krav om overvågning og logning, pålægges de økonomiske udgifter og administrativt ansvar. Det er en byrde mange communities og enkeltindivider ikke vil kunne leve op til og aktiviteterne må lukke. Samme problemstilling står de større aktører også over for. De har også store udgifter ifb. med logning og administration af overvågningen af danskerne. Det er selvfølgelig en regning, som vil blive lagt over på kunderne og hæmme udbredelsen af bredbånd. Alt i alt vil bekendtgørelsen hæmme legitime danske aktiviteter på internettet.

(4) Bekendtgørelsen er uigenemtænkt og virkningsløs

Bekendtgørelsen forudsætter at potentielle terrorister ikke er IT-kyndige for at den skal have nogen form for præventiv eller efterforskningsmæssig effekt. Da det næppe er tilfældet vil bekendtgørelsen ikke være til hjælp iterrorbekæmpelsen. Ifb. med registrering af borgernes breve (epost) har potentielle terrorister 3 muligheder for at undgå modtager og afsender ender i befolkningens overvågningsregister: i) være tilknyttet en uddannelsesinstitution, virksomhed eller blot besøge folkebibliotekerne, ii) benytte populære udenlandske eposttjenester. iii) "hoste" sin egen SMTP server.

For chat gælder det samme, her har potentielle terrorister også flere muligheder for ikke at ende i befolkningens overvågningsregister: i) Bruge en af mange udenlandske IMtjenester (Instant Messages) som MSN Messenger, AIM, ICQ, Jabber mm., ii) benytte udenlandske chatrum, iii) logge på udenlandske IRCnetværk eller iv) "hoste" sin egen IRCserver og lade være med at fortælle det til nogen. Og sådan gælder det for alle de services (teletjenester) som bekendtgørelsen forsøger at tæmme og overvåge. Vi kan nævne en håndfuld smuthuller til dem alle. Det eneste bekendtgørelsen kan bruges til er at overvåge ganske almindelige danskers aktiviteter på internettet. Potentielle terrorister og andre kriminelle elementer er kyndige nok til at undgå uønsket overvågning og registrering.

Konklusionen i Digital Forbruger Danmark er på den baggrund at nærværende forslag til bekendtgørelse er stærkt samfundsskadelig med ingen eller ringe effekt ved terrorbekæmpelse. DFD anbefaler at det trækkes tilbage.

Med venlig hilsen

Digital Forbruger Danmark
v/ Niels Vestergaard Jensen
Ryparken 26, 2. th.
2100 København Ø
niels@digitalforbruger.dk

Karina Pedersen

Fra: Justitsministeriet
Sendt: 17. maj 2004 08:14
Til: JOURPolitikontoret
Emne: VS: Høringssvar - logningsbekendtgørelse

Scan001.PDF

-----Oprindelig meddelelse-----
Fra: Nicholai Kramer Pfeiffer [mailto:NKP@CyberCity.dk]
Sendt: 14. maj 2004 13:39
Til: Justitsministeriet
Cc: Nicholai Kramer Pfeiffer
Emne: Høringssvar - logningsbekendtgørelse

Att: Civil- og Politiafdelingen

Hermed fremsendes Cybercitys høringssvar på Justitsministeriet udkast til bekendtgørelse om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet I forbindelse med indgreb I meddelelseshemmeligheden.

Høringssvaret er tillige fremsendt med almindelig post.

Vh.

Nicholai K. Pfeiffer
Regulatorisk Chef
Cybercity A/S
Tel: + 45 33 98 31 31
Fax: + 45 33 98 31 20
Mob: + 45 29 49 31 31

Akt.nr. 82
Justitsministeriet 2002 NR. 945-0922
Politikontoret

cybercity

Justitsministeriet
Civil- og Politiafdelingen
Slotholmsgade 10
1216 København K

København, d. 14. maj 2004

J.nr: nkp/558

Høring over Justitsministeriets udkast til bekendtgørelse om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om teletrafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden

Cybercity skal hermed fremsende sine bemærkninger til ovennævnte udkast til bekendtgørelse med tilhørende udkast til vejledning, som Justitsministeriet har sendt i høring ved brev af 24. marts 2004.

Som bekendt sker de teknologiske landvindinger inden for telesektoren ofte i et halsbrækkende tempo, og mulighederne for misbrug og kommunikation til understøtning af strafbare handlinger ændres dermed hastigt. Det virker derfor ikke på alle områder helt gennemtænkt, at et meget omfattende logningskrav baseres på Brydensholt-rapporten, der er udarbejdet godt 7 år før udmøntningen af de foreslåede krav. Dette har da også haft det resultat, at en del af de i udkastet indeholdte forslag afspejler det noget utidssvarende grundlag, som bekendtgørelsen tager udgangspunkt i.

Cybercity støtter naturligvis det principielle sigte med de foreslåede regler i overensstemmelse med den politiske intention, men vi må imidlertid alligevel under omstændighederne forholde os kritisk til det fremsendte forslag. I det følgende er elementerne af denne kritik belyst.

Logningspligtens grundlag
De gældende bestemmelser i bekendtgørelse nr. 666 af 10. juli 2003 (Udbudsbekendtgørelsen) tillader som bekendt opbevaring af trafikdata til visse nærmere bestemte formål, men forpligter ikke til en sådan opbevaring.

Cybercity har med dette udgangspunkt hidtil arbejdet ud fra, at registrerings- og opbevaringspligten alene vedrører de data, der lagres eller umiddelbart kan

lagres af udbyderen efter en kommunikations ophør og at den udvidede logningspligt dermed skulle indebære, at teleudbyderne skulle undlade at slette allerede registrerede trafikdata i 1 år.

Denne formodning synes at have støtte i bemærkningerne til lovforslaget. Der peges således i bemærkningerne på problemstillingen i forbindelse med udbud af flat-rate, herunder ADSL-abonnementer, hvor afregningsformen gør opbevaring af registrerede trafikdata unødvendig og dermed i princippet efter gældende regler direkte ulovlig.

Derfor er det særdeles vidtgående og højst overraskende, at det foreliggende forslag er baseret på en pligt for teleselskaberne til at overvåge, opsamle, registrere og gemme oplysninger af hel midlertidig karakter, selv om disse trafikdata slet ikke efter de gældende produktionsmetoder registreres og opbevares af teleudbyderne. Kravet om opbevaring er således ikke som oprindeligt tiltænkt en fravigelse af sletningskravet, men i realiteten et nyt krav om at registrere borgeres adfærd i det omfang denne efterlader sig spor i teleudbydernes net i form af data, som kan registreres.

Efter Cybercity's opfattelse forpligtes teleudbyderne hermed til egentlige overvågnings- og registreringsopgaver for politiet uden at dette har været beskrevet eller behandlet i lovens forarbejder. Forslaget til udmøntning repræsenterer dermed en funktionel, økonomisk og retssikkerhedsmæssig radikal udvidelse i forhold til den oprindeligt foreslåede og af Folketinget vedtagne pligt til opbevaring af trafikdata.

Som illustreret i det følgende vil det herudover af praktiske årsager ikke være muligt at gennemføre forslaget i foreliggende form på en hensigtsmæssig måde til den 1. juli 2005 og dele af forslaget vil samtidig få vidtrækkende økonomiske konsekvenser for de omfattede udbydere. Forslaget er endvidere efter Cybercity's opfattelse ganske ineffektivt på grund af store "huller" i registreringerne og umiddelbare omgåelsesmuligheder. Endelig finder Cybercity, at udkastet i sin nuværende form rejser en række principielle juridiske problemstillinger som bør overvejes nøje inden bekendtgørelsen udstedes.

Hjemmel
For så vidt angår hjemmel, fremgår det af bemærkningerne til lovforslaget, at hensynet til effektiv regulering og konkurrenceforholdene i branchen tilsiger, at logningpligten omfatter alle udbydere.

Det overrasker derfor, når en række udbydere imidlertid ifølge udkastets § 3 helt er undtaget fra logningsforpligtelsen, mens andre alene er underlagt en begrænset logningspligt.

Det er i bemærkningerne til loven intetsteds beskrevet, at udmøntningen af hjemlen til logning kan undtage en del af målgruppen fra logningspligten.

Indførelsen af en *begrænset logningspligt* for visse udbydere har således ikke været genstand for drøftelse i folketinget, hvorfor indførelsen af en begrænset logningspligt dermed efter Cybercitys bedste vurdering dermed ligger udenfor de forudsætninger som folketinget var bekendt med, da man vedtog loven.

Registrering af oplysninger om kundens adgang til sin e-mail konto
Det fremgår af side 16 i vejledningen til bekendtgørelsen, at den efterforskende myndighed i forbindelse med indhentelse af oplysninger om indgående e-mail trafik forventer at få oplyst dato, tid og unik identitet involveret i alle adgange til e-mail adressen knyttede e-mails. Dette indebærer med andre ord, at udbydere af e-mail tjenester skal føre en separat log over alle tidspunkter, hvor borgeren har haft adgang til sin e-mail konto.

Udover at være et særligt godt eksempel på et krav, der går langt ud over et krav om at undlade at slette allerede registrerede oplysninger jf. ovenfor, er dette omfattende krav ganske uden støtte i lovforslaget og de tilhørende bemærkninger. Dels er der slet ikke tale om oplysninger om tele- eller internettrafik, dels indeholder kravet et så omfattende element af overvågning, der tilmed ligger langt over, hvad man som borger med rimelighed kan forvente registreres af sin teleudbyder, at det ikke med nogen ret kan anses for hjemlet i loven.

Indførelsen af et sådant krav uden fuldstændig klar hjemmel, rejser derfor i Cybercitys øjne så principielle juridiske betænkeligheder, at det ikke bør opretholdes. Dertil kommer i øvrigt, at det er helt uacceptabelt, at kravet alene fremgår af vejledningen, jf. nedenfor.

Lovgivning i en vejledning
Cybercity kan tilslutte sig det generelle grundlæggende princip om, at administrativt fastsatte regler bør udformes med så stor præcision og klarhed, at ingen individer bør kunne være i tvivl om rammerne for den pågældende regulering – og konkret i denne sammenhæng nøjagtig hvilke oplysninger, som vil skulle registreres om dem. Det er således den tekniske udmøntning, der i sidste ende afgør, hvor stort et indgreb i privatlivets fred de berørte personer må tåle og desuden hvor omfattende en forpligtelse bekendtgørelsens målgruppe - teleudbyderne - pålægges.

På denne baggrund finder Cybercity det yderst betænkeligt, at de forpligtende regler, som nu indføres, i vidt omfang alene kan læses ud af den til bekendtgø-

relsen udarbejdede vejledning. Det er i vores øjne af retssikkerhedsmæssige årsager helt uacceptabelt at indføre forpligtende regler i en vejledning, som dels kan ændres uden forudgående offentlig debat og politisk stillingtagen, og som samtidig ikke udgør en juridisk bindende retsforskrift. Cybercity finder det derfor påkrævet, at alle forpligtende krav klart og tydeligt fremgår direkte af bekendtgørelsesteksten.

Endvidere er der adskillige eksempler på bestemmelser og anvendte begreber, som efterlader en helt urimelig fortolkningstvivl, såvel i selve bekendtgørelsesteksten som i den tilhørende vejledning. Ved indskrivning af kravene i bekendtgørelsen bør disse samtidig tydeliggøres, så de berørte parter - borgere samt teleudbydere - kan indrette sig i fuld tillid til, at bekendtgørelsen udtømmende beskriver hvad der skal registreres.

Vejledningen indeholder en opregning af, hvilke data den efterforskende myndighed forventer at få oplyst fra udbyderne i tilknytning til udlevering af data vedrørende de enkelte kommunikationsformer. Sådanne forpligtende krav bør som nævnt overføres til bekendtgørelsen.

Pligten for udbydere af e-mail tjenester til at registrere de tidspunkter, hvor borgeren har haft adgang til sin e-mail konto er et særlig grelt eksempel på et krav, der ikke kan læses ud af bekendtgørelsen, hvorfor kravet bør udgå.

Tilsvarende vurderes kravet i vejledningen om, at registrere IP-adressen for hver enkelt kommunikation, som initieres og termineres hos den enkelte kunde at ligge langt ud over, de oprindelige rammer som var tiltænkt med § 786, stk. 4.

Det forhold, at bekendtgørelsens § 9 pålægger strafansvar for manglende overholdelse af logningspligten, gør det netop bydende nødvendigt, at de strafsanktionerede pligter beskrives udtømmende og klart i selve bekendtgørelsesteksten.

Behov for dialog med tele- og internetudbyderne
Det har gennem hele forløbet været forudsat, at reglerne om logningspligtens indhold skulle fastsættes efter dialog med tele- og internetudbyderne. Dette er ikke mindst afgørende for at sikre en teknologisk hensigtsmæssig udformning af reglerne.

Udover det møde, der blev afholdt i Justitsministeriet den 19. december 2002 imellem Telekommunikationsindustrien og de involverede myndigheder har der imidlertid, så vidt Cybercity er orienteret, ikke været taget initiativ fra ministeriets side til at inddrage branchen yderligere i udformningen af reglerne.

Henset til det meget tidlige tidspunkt i forløbet, hvor mødet i Justitsministeriet blev afholdt, er det Cybercity's opfattelse, at branchen reelt ikke har været inddraget ved udformningen af det foreliggende udkast, således som forudsat. Det forekommer særligt uheldigt, henset til, at man i bemærkningerne til lovforslaget netop henviser til inddragelsen af branchen som én af begrundelserne for, at ministeriet ikke har fundet det nødvendigt at mødes med branchen i godt 1½ år forud for fremsendelsen af udkastet.

Der skal ikke herske tvivl om, at Cybercity fremadrettet meget gerne deltager i et udredningsarbejde, der nærmere kan belyse og søge løsninger på de tekniske problemer det foreliggende udkast rejser. Nedenfor vil Cybercity forsøge at redegøre for de mange (formentlig utilsigtede) tekniske vanskeligheder og uhensigtsmæssigheder udkastet giver anledning til.

Hvilke udbydere er omfattet
I henhold til udkastets § 2 skal en række oplysninger registreres hos såvel originerende, transiterende som terminerende part. Kravet gøres gældende over for udbydere af telenet og teletjenester, og det er således begrænset til de tilfælde, hvor en kommunikation formidles af en udbyder, der er underkastet dansk lovgivning.

Dermed er al elektronisk post, der formidles af virksomheder eller institutioners postservere undtaget. Det er karakteristisk for udviklingen, at stadig flere tjenester afvikles som applikationer uden brug af en udbyder for de pågældende tjenester. Dette forhold undergraver logningspligtens effektivitet og det øger kundernes muligheder for at undgå logning. Det skaber samtidigt en forskelsbehandling og dermed en konkurrenceforvridning mellem forskellige kommunikationsformer.

Virksomhedsinterne ydelser
I henhold til forslaget skal virksomheder ikke logge trafikdata for de ansattes teletrafik, idet denne trafik alene logges i forbindelse med virksomhedens eventuelle brug af udbydere af telenet og teletjenester for ekstern trafik. For telefonopkald betyder dette, at afgående trafik fra en virksomhed typisk logges med et fælles A-nummer. For E-post er virkningen, at trafikken ikke logges, hvis virksomheden anvender egen postserver.

Det forekommer imidlertid ikke proportionalt og det vil være konkurrenceforvridende, hvis nævnte produktionsformer med outsourcing af en virksomheds kommunikation er underkastet logningspligt for medarbejderes trafik i større omfang end de tilfælde, hvor virksomhedsinterne net opbygges som et særskilt privat net.

De foreslåede regler medfører, at registreringen af virksomhedsintern teletrafik og medarbejdernes kommunikation med omverdenen afhænger af den teknologiske løsning, der vælges for det virksomhedsinterne net. Reglerne bør i stedet udformes på en sådan måde, at registreringen i et privat net i alle tilfælde er undtaget for registrering og dermed også i tilfælde af outsourcing til et offentligt net.

Begrebet trafikdata
Hverken retsplejelovens § 786, stk. 4 eller den foreslåede bekendtgørelse definerer trafikdata. En sådan definition findes imidlertid i persondatadirektivet og udbudsbekendtgørelsen. Definitionen i bekendtgørelsen lyder:

Ved trafikdata forstås data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf.

Det er således en forudsætning, at data behandles i tilknytning til kommunikationen. En del af de foreslåede registreringer synes imidlertid ikke at opfylde denne betingelse.

Eksempelvis er registrering af anvendere af IP-adresser ikke trafikdata, da de pågældende oplysninger ikke behandles som led i kommunikationen. Man kan sammenligne med brugen af en telefonboks, hvor personidentiteten ikke indgår i samtaleopstillingen. Logning af identitet for de personer, der træder ind i boksen, er således ikke trafikdata.

Det er endvidere ikke i overensstemmelse med normal opfattelse af begrebet teletjeneste, at en chattjeneste omfattes. Uanset definitionen i § 1 stk. 2 nr. 2 er det således tvivlsomt, om det oprindelige lovforslag overhovedet giver hjemmel til en sådan udvidelse af teletjenestebegrebet. Hvis dette er tilfældet aktualiserer det i den grad spørgsmålet, om andre typer internetbaserede ydelser fremadrettet også kan omfattes uden lovændring.

Cybercity finder på denne baggrund, at der bør tilvejebringes et mere fast hjemmelgrundlag i relation til logningskravet for internetbaserede tjenester.

Undtagelserne fra logningskravet
Efter forslaget § 3, stk. 1, undtages bestemte typer af udbydere fra logningspligten, når de har mindre end 100 kunder, og kravet om logning udskydes til 2006 og reduceres til ændringer af identitet, når der er tale om geografisk begrænsede tjenester med mindre end 400 kunder, jf. § 3, stk. 2.

Eftersom lovforslaget i forhold til lovudkastet i sin tid blev ændret med henblik på, at alle udbydere skulle omfattes, står Cybercity fuldstændigt uforstående over for de foreslåede generelle undtagelser.

Af offentlig omtale er det fremgået, at undtagelserne beror på, at registreringskravene skulle være særligt bebyrdende for mindre udbydere. Det synes dog åbenlyst, at den politimæssige interesse i at kunne efterforske spor, der har sit udspring i boligforeninger med mindre end 100 slutbrugere bør være mindst ligeså stor som at kunne foretage tilsvarende tiltag overfor en slutbruger i et parcelhus, der dermed typisk ikke vil være omfattet af bekendtgørelsens undtagelsesbestemmelse i § 3.

Efter Cybercity's vurdering er der intet sagligt grundlag for de foreslåede undtagelser, og det foreslås i stedet, at der skabes mulighed for en administrativt forvaltet tidsbegrænset undtagelse, når dokumentation for nødvendigheden heraf kan fremlægges for udbydere med mindre end 100 hhv. 400 kunder.

Hvilken form skal trafikdata lagres?
Efter bekendtgørelsesudkastets § 8 skal oplysningerne videregives i et læsbart format. Betydningen heraf er uklar. Et mere fundamentalt spørgsmål er imidlertid evt. implicitte krav til opbevaringsformen.

Cybercity skal understrege, at der er markant forskel på krav til et udleveringsformat og krav til et opbevaringsformat. Det vil være forbundet med eksorbitante omkostninger at organisere trafikdata i den struktur, hvori politiet i givet fald ønsker oplysninger om de enkelte borgere udleveret. Eksempelvis kan registreringer fra e-post systemer sandsynligvis principielt gennemføres via den af systemerne genererede hændelseslog. Men det vil være en ekstremt omfattende opgave at bearbejde disse data, kopiere dem og organisere dem efter den enkelte kundes kommunikationer og adgang til e-mail kontoen. Efter Cybercitys opfattelse vil selve eksistensen af et sådant samlet arkiv over borgeres adfærd være betænkelig, da bemærkningerne til loven ikke omtaler en sådan konsekvens.

Det forhold, at de i bemærkningerne forudsete krav til beskyttende foranstaltninger og sikring mod uautoriseret adgang ikke er udmøntet i forslaget, taler ligeledes for, at dette ikke er hensigten. I den forbindelse bemærkes også, at vejledningen omtaler muligheden for, at et konsulentfirma opbevarer de loggede data uden at formelle krav i den forbindelse omtales.

Sammenfattende er det Cybercity's vurdering, at kravet om læsbarhed ikke bør kunne udstrækkes til at omfatte en pligt for den enkelte udbyder til at sammenkøre registrerede dataposter. Sammenkædningen af indsamlede op-

lysninger må i stedet forudsættes at skulle varetages af politiet i forbindelse med en konkret anmodning om udlevering af data fra involverede udbydere.

Dette synes da også i et vist omfang bekræftet i Justitsministeriets besvarelse af 11. maj 2004 af Cybercitys forespørgsel af 14. april 2004. Således fremgår det heraf, at det i høring sendte udkast slet ikke forholder sig til den praktiske udlevering af registrerede oplysninger.

Justitsministeriet bør i forlængelse heraf bekræfte, at den enkelte udbyder udelukkende er forpligtet til at opbevare trafikdata i et format, som er tilpasset produktionsformen og mulighederne for at registrere trafikdata og at der ikke implicit i bekendtgørelsesudkastes er indfortolket en pligt for udbydere til at udvikle nye registreringssystemer med henblik på at kunne imødekomme den efterforskende myndigheds efterspørgsel.

Telefoni i fastnettet
Der er i dag i størrelsesorden 8 mia. opkaldsforsøg i fastnettets telefonitjenester pr. år. Dette vil isoleret set med forslaget medføre, at der løbende opbevares ca. 16 mia. registreringer af opkald, eller ca. 3.000 pr. borger.

En stor del af disse registreringer vil imidlertid ikke indeholde et opkaldende A-nummer, da virksomheder oftest angiver et fællesnummer som A-nummer. Opkald af denne art fra virksomheder, kommuner, institutioner mv. vil således isoleret set ikke være af større efterforskningsmæssig værdi, hvis politiet ikke samtidigt har adgang til virksomhedsinterne registreringer.

Ifølge Brydensholtudvalgets betænkning skulle registreringerne især benyttes i forbindelse med elektroniske spor for brug af internettet, hvor kunder på daværende tidspunkt overvejende brugte modem og telefonforbindelse til adgangen. Imidlertid vil det med de i dag kendte produktionsmetoder være særdeles vanskeligt at spore disse adgange med blot nogenlunde effektivitet gennem registreringer i telefoninettet. A-nummeret logges som udgangspunkt ikke af internetudbydere ved direkte indvalg (ex. 16xxx) som forudsat i betænkningen, og det vil derfor være vanskeligt i alle tilfælde at benytte logningerne til at udpege tilslutningen til et offentligt telefonnet. Oftest vil det således alene være kundens kundenummer og password, der logges af udbyderen i forbindelsen med en dial-in internet session.

I praksis vil udpegningen dermed langt mere effektivt kunne ske gennem kundeidentiteten i internet og en screening af de sandsynlige forbrugssteder for den pågældende borger. Hvis borgeren med hensigt har sløret sin identitet er det dog nærliggende at antage, at borgeren også vil benytte en adgangsvej,

som alligevel ikke kan efterspores – enten fordi de loggede data er tilknyttet en offentlig tilgængelig terminal eller fordi adgangsdata slet ikke logges.

Hertil kommer, at adgangen til internettet via telefonitjenesten er aftagende i takt med udbredelsen af forskellige former for bredbåndsadgang. Det er derfor svært at underbygge det omfattende krav om logning fsva. dial-in access ud fra de oprindelige begrundelser.

Almindelige samtaler mellem brugere kan ligeledes let sikres mod logning. Således kan logning konsekvent omgås ved instant messaging (MS Messenger m.fl) eller hvor kommunikationen foregår via en udenlandsk relay-server. Da udbredelse af sådanne kommunikationsformer bliver større dag for dag, vil registreringerne af almindeligt PSTN-telefoni sandsynligvis være ganske værdiløse i forbindelse med professionelt tilrettelagt forbrydelser eller terrorvirksomhed.

Internet og E-mail
Internettrafik er som bekendt baseret på IP-protokollen, som er en såkaldt forbindelsesfri nettjeneste. Det betyder, at selve trafikken på internettet ikke kan logges på en meningsfyldt måde.

En eventuel registrering af data for hver enkelt kommunikation, herunder de IP-adresser som hver enkelt borger har været i kontakt med, kan alene foretages af udbydere, der for bestemte anvendelser benytter internettet som adgang til udbud af internetbaserede tjenester.

Dette krav, som alene fremgår af vejledningen, er utvivlsomt det mest vidtgående og dermed mest urimelige, som er indeholdt i den logningspligt, som Justitsministeriet ligger op til. Således vil en pligt til at logge oplysninger om hver enkelt initieret og termineret kommunikation foretaget via internettet påføre danske internetudbydere en nærmest uoverkommelig byrde.

Cybercity tillader sig at formode, at dette skyldes, at de personer, der har udarbejdet afsnittet i vejledningen vedrørende internettet ikke er helt klar over, hvad det er de beder om at få logget. Således vil en enkelt borger, der anvender såkaldte peer-to-peer tjenester mv. uden videre kunne generere kommunikation med 2-500 IP-adresser i sekundet. Disse oplysninger vil – betragtet enkeltvis – ikke adskille sig fra de oplysninger som genereres ved enhver anden IP-baseret tjeneste, men selve omfanget af oplysningerne gør, at det vil være grænsende til det umulige at foretage en brugbar registrering af disse, herunder efterfølgende at sammenstykke disse til et brugbart datagrundlag. Cybercity vurderer således at omfanget af den nuværende logningspligt med udgangs-

punkt i det nuværende antal brugere af internettet vil betyde, at mere end 1 billiard IP-kommunikationer vil skulle logges på årsplan.

Udkastet indeholder ligeledes en pligt til logning af e-mails og chattjenester.

For e-mails er den bagvedliggende målsætning, at modtagere og afsendere skal logges hos såvel afsender som modtager. Der findes ingen samlet oversigt over omfanget af e-mails i Danmark, men det antages, at der dagligt bliver sendt ca. 30 millioner e-mails i Danmark.

Ønsket om registrering kan således principielt omfatte op mod 20 mia. registreringer på årsplan.

E-mails afvikles imidlertid overvejende via postservere i virksomheder, institutioner, kollegier, læreranstalter mv. Post afsendt via disse postservere skal efter forslaget ikke registreres.

Hertil kommer, at e-mails afviklet via instant messaging og webmail ikke i praksis vil blive underkastes en registreringspligt. Det er dermed kun de helt almindelige e-mails, der vil blive registreret. Formentlig er der tale om ca. 10 mia. registreringer pr. år. En lang række e-mails vil derfor ikke være omfattet af logningspligten i sin nuværende form.

Via webmail (hotmail mv.) og forskellige former for instant messaging er det dermed muligt for enhver internetbruger at skabe en mail-funktion, der ikke er underkastet registrering.

Den efterforskningsmæssige værdi af registreringerne vil derved med disse "huller" og omgåelsesmuligheder være stærkt begrænset. Hertil kommer, at det vil være vanskeligt at opbevare de ønskede oplysninger i en anvendelig form, da en oversigt for en enkelt borgers e-mail aktivitet for et år tilbage i tiden alene vil kunne genskabes ved sammenkøring og udtræk af en nærmest uoverskuelig lang række datamedier. Forslaget om logning af e-mails er dermed yderst problematisk.

Sammenfattende bemærkes, at det efter Cybercitys opfattelse ikke tilføjer væsentlig efterforskningsmæssig værdi at udbygge logningspligten ud over de registreringer af data, der allerede i dag opbevares af backup-mæssige hensyn.

Det bør derfor meget nøje overvejes, om de økonomiske konsekvenser ved at gennemføre forslaget i sin nuværende form står mål med det forventede udbytte for politiet, henset til de mange nævnte muligheder for at unddrage sig logningen.

Forbedringsforslag
Som belyst i dette høringssvar er det ikke muligt at efterleve de i bekendtgørelsesudkastet anførte regler, der tilmed på mange områder er uklare som implementeringsgrundlag.

Som anført forekommer den praktiske værdi af reglerne ikke at være proportional med de helt uoverskuelige omkostninger, som det både på kort og længere sigt vil påføre udbydere af teletjenester i Danmark at være underlagt den påtænkte regulering.

Endvidere er det ovenfor beskrevet hvorledes de foreslåede regler ganske enkelt ikke vil være effektive da der ud over de indbyggede mangler omkring de omfattede systemer inden for Danmarks grænser er talrige muligheder for at undgå lovens bestemmelser ved at placere kommunikationsservere uden for landets grænser, hvad der i praksis reelt betyder at reglerne er ineffektive fra første dag og aldrig vil opnå den tilsigtede virkning som ligger til grund for den politiske beslutning.

Endelig rejser udkastet en række grundlæggende juridiske problemer, som efter Cybercity's opfattelse betyder, at bekendtgørelsen i sin nuværende form ikke under nogen omstændigheder bør træde i kraft. Især det forhold, at visse elementer i logningspligten alene er beskrevet i den tilhørende vejledning, giver anledning til alvorlig bekymring.

Cybercity foreslår på denne baggrund en stand-still, hvor bekendtgørelsen i første omgang alene kræver en udvidelse af tidsperioden for opbevarelse af de trafikdata, som allerede registreres.

Cybercity foreslår endvidere, at der iværksættes et udredningsarbejde mellem involverede myndigheder, teleindustrien og internetbranchen med henblik på at belyse eventuelle videre tiltag for den danske indsats i forbindelse med forberedelsen af forslag til fælleseuropæiske regler på området.

Brydensholtudvalgets betænkning, som for nærværende er eneste offentliggjorte grundlag for de foreslåede krav, og det foreliggende forslag til udmøntning viser med al tydelighed, at der er behov for et opdateret udredningsarbejde, hvor den udførende sektor også selv er repræsenteret.

--oOo--

cybercity

Cybercity har ikke yderligere at bemærke til Justitsministeriets udkast til bekendtgørelse om telenet- og teletjenesteudbyderes registrering og opbevaring af oplysninger om tele-trafik samt praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden.

I det omfang Justitsministeriet måtte have spørgsmål til ovenstående står Cybercity naturligvis til rådighed.

Venlig hilsen

Nicholai Pfeiffer
Regulatorisk Chef
Cybercity A/S

Boligneteforeningen

Justitsministeriet
Politikontoret
Att: Lennart Lindblom

Høringssvar vedr. bekendtgørelse om registrering og opbevaring af teletrafik.

Hermed fremsendes Boligneteforeningens høringssvar til ovennævnte bekendtgørelse.

Med venlig hilsen
Rune Hansen
Boligneteforeningen

Rune Hansen

Indledning

Boligretforeningen er fundamentalt enig om, at det er vigtigt at politi og efterretningstjenester sikres fornuftige efterforskningsværktøjer i kampen mod alvorlig kriminalitet. Imidlertid er det vores vurdering, at den politimæssige betydning af bekendtgørelsen vil blive marginal, samtidigt med at konsekvenserne for bolignetforeninger tegner til at blive meget alvorlige. Det skal dertil siges, at bekendtgørelsen gennemgående er så uklart formuleret, særligt indenfor datadelen, at det i praksis er umuligt at kommentere den uden først, at foretage en subjektiv fortolkning af hvad der menes. Dette er i sig selv et væsentligt problem, idet systemadministratorer ikke med denne bekendtgørelse i hånden vil kunne vide sig sikre på at overholde loven.

Når bekendtgørelsen er blevet så tvetydig, synes det at hænge sammen med, at der kontinuerligt skiftes mellem to overordnede målsætninger for bekendtgørelsen.
På den ene side synes bekendtgørelsen at lægge op til, at det primære formål er at sikre at data der opbevares i anden forbindelse nu skal opbevares i 1 år. På den anden side synes bekendtgørelsen at lægge op til at kræve en yderligere registrering af specifikke oplysninger, der typisk ikke registreres i dag. Det nødvendige indhold af bekendtgørelsen vil være kraftigt afhængig af hvilken af disse to målsætninger, der er den gældende, og bekendtgørelsens konsekvenser for bolignetforeninger vil ligeledes være kraftigt afhængige heraf.

Havde man holdt sig til, at data, der i anden forbindelse opbevares, skal opbevares i et år, havde bekendtgørelsen været umiddelbart anvendelig. Bekendtgørelsens mål havde dermed været begrænset til at sikre allerede eksisterende elektroniske beviser, der ofte vil have en kort levetid. Hvilke data, der vil blive registreret, vil afhænge af hvilken type netværk der er tale om, og bekendtgørelsen ville således have været teknologineutral, hvilket vil betyde, at bolignetforeningerne ikke skal ud og investere voldsomme summer i opgradering af deres netværksudstyr, og endvidere betyde, at bekendtgørelsen ikke vil blive forældet af den teknologiske udvikling.

Imidlertid indeholder bekendtgørelsen også afsnit hvor man pålægger bolignetforeningerne at registrere og opbevare oplysninger der ikke normalt registreres som en naturlig del af vores virke. Bekendtgørelsens målsætning synes nu ikke at begrænse sig til sikring af eksisterende beviser, men til egentlig "produktion" af beviser (data registreres alene med det formål at de skal være tilgængelig for politiet på et senere tidspunkt). Da teleloven, persondataloven og registerloven pålægger os at slette data efter endt brug hvis de ikke er omfattet af denne bekendtgørelse, må bekendtgørelsen med denne målsætning nødvendigvis indeholde meget specifikke definitioner af hvilke data der skal registreres og opbevares og hvilke der ikke skal. Imidlertid glimrer bekendtgørelsen i sin nuværende form ved at være meget lemfældig i sin omgang med begreberne indenfor datatransmission, hvorfor det ikke er muligt ud fra bekendtgørelsen entydigt at fastslå hvilke yderligere oplysninger, der nu skal til at registreres (jvf. dette høringssvars tekniske del). Imidlertid vil en bekendtgørelse der meget specifikt søger at definere hvad der skal registreres meget hurtigt blive overhalet af den teknologiske udvikling. Endvidere vil en sådan bekendtgørelse pålægge bolignetforeninger meget store omkostninger til at opgradere deres systemer, så det bliver teknisk muligt at registrere disse data. Bekendtgørelsen er således alt andet end teknologineutral i denne tolkning. Den efterforskningsmæssige gevinst vil ligge i at politiet på forhånd vil vide hvilke beviser der vil være til rådighed på en given lokalitet. Dog må det forventes at folk med et vist IT kundskab meget nemt vil kunne omgå logningen, f.eks. ved kryptering.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Kombinationen af en uklar overordnet målsætning kombineret med en meget uklar og til tider tvetydig omgang med tekniske termer gør at bekendtgørelsen i sin nuværende form er uanvendelig som hjælp til den IT-ansvarlige i at kunne opfylde lovens bogstav.

Boligretforeningen ser derfor ikke andre muligheder end at bekendtgørelsen for nuværende begrænses til at pålægge teleudbydere at gemme oplysninger registreret i anden forbindelse i et år, dvs. fjerne § 2 stk. 1 fra bekendtgørelsen.

Såfremt der er et politisk ønske om at udvide registreringspligten med specifikke oplysninger ud over hvad der i forvejen registreres, vil Boligretforeningen foreslå, at der nedsættes et arbejdsudvalg med repræsentanter fra de relevante aktører, således at det sikres at bekendtgørelsens krav er juridisk entydige og teknisk gennemførlige. Et sådant arbejde vil kunne reducere byrden for de berørte aktører samtidigt med at politiet vil kunne sikres bedre efterforskningsværktøjer end med herværende bekendtgørelse. For nuværende udskrives en stor regning der vil gøre IT dyrere end det er i dag, uden at der synes at være nogen væsentlig samfundsmæssig gevinst ved dette.

Endelig har Boligretforeningen meget vanskeligt ved at se den efterforskningsmæssige logik bag kravet om døgnbetjent kontaktpunkt. Formålet med et døgnbetjent kontaktpunkt synes at knytte sig til en hurtig sikring af beviser. Med herværende bekendtgørelse pålægges telebranchen og bolignetforeningerne jo netop at opbevare alle registrerede data i et år, hvorfor beviset er sikret uden politiets indgriben. Samtidigt er den økonomiske byrde, bolignetforeninger dermed pålægges, helt ude af proportioner. Et døgnbetjent kontaktpunkt koster typisk omkring 3 mill. kr. om året at opretholde, hvilket er væsentligt større end den samlede årlige omsætning for en række af de bolignetforeninger der pålægges at etablere døgnbetjent kontaktpunkt. Såfremt man fortsat ønsker bolignetforeningernes indsats i udbredelsen af højhastigheds internetforbindelser, er det således helt nødvendigt at dette krav udelades i den endelige bekendtgørelse.

I det følgende skal ovennævnte konklusioner blive uddybet og underbygget. Vores høringssvar er inddelt i en generel del, en teknisk del og et appendiks til den tekniske del.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Generel del

Bolignetforeningen er overordnet set enig om, at det er vigtigt at politiet sikres gode arbejdsbetingelser i opklaringen af alvorlig kriminalitet.

Samtidigt mener vi dog også, at omkostningerne til tilvejebringelse af opklaringsværktøjer bør stå i et rimeligt forhold til den opklaringsmæssige gevinst ved tilvejebringelsen af nye opklaringsværktøjer. Dette mener vi ikke er tilfældet med herværende bekendtgørelse, da logningens kvalitet er defineret utroligt uklart, og et stort antal aktører er helt undtaget fra logningspligt, samt at kriminelle organisationer må forventes at anvende kryptering af data. Dette vil gøre det særdeles nemt for kriminelle at undgå logning. Samtidigt pålægger logningspligten bolignetforeninger en række voldsomme økonomiske og administrative byrder, der i praksis vil gøre bolignetforeningernes store frivillige arbejde med at udbrede IT kendskabet til den danske befolkning meget vanskeligt fremover.

Bekendtgørelsen omhandler netop oplysninger som udbydere ikke normalt vil opbevare, da de ikke er nødvendige for produktion af tjenesteydelsen. De ønskede oplysninger skal således opsamles og opbevares med det ene formål at sikre, at oplysningerne kan tilvejebringes i det tilfælde politiet eller andre med en dommerkendelse får brug for dem. Logningen foretages således alene af hensyn til politi og efterretningstjenester.
Hidtil har overvågning og efterforskningsarbejde været monopoliseret hos Politi og efterretningstjenester, og Bolignetforeningen stiller sig uforstående overfor, at bolignetforeninger nu skal pålægges at udføre politiopgaver. Bolignetforeningerne kan således ikke forventes at ligge inde med den tekniske, økonomiske og administrative kompetence der skal til at løfte denne politimæssige opgave på forsvarlig vis. Vi finder derfor logningspligten overordentligt problematisk og mener, at såfremt den skal gennemføres som der er lagt op til i bekendtgørelsen, bør der for bolignetforeninger være tale om, at dette gøres af en ekstern partner, betalt af politiet. Dette kunne f.eks. ske ved at logfilerne opbevares hos en central uafhængig myndighed i krypteret form hvor den dato- og personspecifikke krypteringsnøgle opbevares af bolignetforeningerne.
Denne eksterne myndighed bør af hensyn til troværdigheden ikke høre under Justitsministeriet men kunne eksempelvis være Datatilsynet.
Samtidigt må det anses for rimeligt at den dataopbevarende myndighed kan udføre gratis konsulentvirksomhed overfor de logningsforpligtede udbydere og på denne måde sikre at den loggede information er tilstrækkelig og korrekt.

Det er særligt problematisk for bolignetforeninger at skulle opbevare personspecifikke oplysninger om vore naboer - herunder deres sexvaner, religiøse overbevisning, og generelle gøren og laden på internettet - netop fordi disse oplysninger berører mennesker som vi har personlig kontakt med i det daglige. Hertil kommer at bekendtgørelsen er meget uklart afgrænset i forhold til persondata- og registerloven.
For nuværende er området primært reguleret i form af regler for hvor længe man må opbevare forskellige typer af oplysninger. Som bekendtgørelsen er udformet nu, vil det i praksis være umuligt for bolignetforeninger at administrere deres netværk på en måde, der hverken strider mod logningspligt eller persondata-/registerloven.
Endelig mener Bolignetforeningen at bekendtgørelsen pålægger bolignetforeninger og televirksomheder betragtelige ukompenserede meromkostninger til udførelse af en samfundsmæssig opgave (terroristbekæmpelse og efterforskning).

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Bolignetforeningen har vanskeligt ved at se hvilke efterforskningsmæssige kriterier, der adskiller bolignetforeninger fra f.eks. private virksomheder, universiteter, biblioteker m.v., der i bekendtgørelsen er helt undtaget for logningspligt. Bolignetforeningen mener derfor, at bekendtgørelsen bør omfatte alle der stiller en internetforbindelse til rådighed for andre, idet logningen ellers vil blive meget nem at omgå for kriminelle. Det vil således uundgåeligt virke kraftigt demotiverende på de mange frivillige, når de pålægges voldsomme administrative byrder i forbindelse med logningen, og det samtidigt er selvindlysende, at den efterforskningsmæssige værdi af dette arbejde vil være meget ringe.

Bolignet vil (ligesom universiteter og private virksomheder) typisk være opbygget på en måde, der teknisk set gør det ganske vanskeligt at opfylde bekendtgørelsens krav, idet netværksinfrastrukturen ikke er designet ud fra et behov om at kunne fakturere forbrugsafhængigt. Dette betyder at bekendtgørelsen i en række tilfælde vil kræve at bolignetforeninger udskifter netværkskomponenter for anseelige beløb og betyde en forøgelse af etableringsomkostningerne ved nye bolignet.

Hvis logningspligten skal opnå den maksimale efterforskningsmæssige værdi, mener Bolignetforeningen det er nødvendigt, at der må være lighed for loven - dvs. at alle der stiller en internetforbindelse til rådighed for andre bør være forpligtet til at logge de samme data. Som det ser ud nu er både mindre bolignetforeninger, offentlige institutioner og private virksomheder helt eller delvist undtaget fra logning.
Bolignetforeningen mener afgjort, at dette vil mindske den efterforskningsmæssige værdi af de logningsdata der indsamles hos bolignetforeninger og andre teleudbydere, idet det vil være overordentligt nemt for kriminelle at skaffe sig internetadgang gennem en ikke logningsforpligtet part, f.eks. bibliotek, universitet, internetcafe eller arbejdsplads. Hertil kommer problemer med at afgrænse de forskellige typer aktører, f.eks. ved hjemmearbejdende.
Det er overordentligt svært, at se de efterforskningsmæssige hensyn der berettiger, at bolignetforeninger pålægges logningspligt, når et større antal sammenlignelige aktører slipper. Hertil kommer, at det må forventes at kriminelle allerede anvender kryptering af data, hvilket yderligere må forventes at gøre den efterforskningsmæssige værdi af logningen begrænset.

Kravet om døgnbemandet kontaktpunkt er særdeles problematisk for bolignetforeninger uanset størrelse. Dette krav vil være særdeles omkostningstungt, og i praksis økonomisk umuligt at honorere for en række bolignetforeninger, der med herværende bekendtgørelse vil være omfattet af dette krav. Selv hvis Bolignetforeningens medlemmer i fællesskab gik sammen om at etablere et døgnbemandet kontaktpunkt for medlemsforeningernes til sammen ca. 10.000 slutbrugere ville omkostningerne hertil typisk betyde kontingentstigninger i størrelsesordenen 20-40 %. For en Bolignetforening med 500 brugere vil omkostningen overstige foreningens årlige omsætning. Kravet om døgnbetjent kontaktpunkt vil således umuliggøre etableringen af bolignetforeninger fremover, og være praktisk umuligt at honorere for de fleste af de allerede eksisterende bolignetforeninger.

Endvidere finder Bolignetforeningen kravet om døgnbemandet kontaktpunkt ganske besynderligt, set i forhold til indholdet i herværende bekendtgørelse, idet logningspligten jo netop sikrer at registrerede data vil være tilgængelige for politiet i op til et år efter registreringen. Det vil således ikke være nødvendigt hurtigt at skulle sikre beviser.
Behovet for døgnbetjent kontaktpunkt synes ydermere uforståeligt når bekendtgørelsen ikke indeholder krav om tidsfrister for udlevering af data til politiet.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Bolignetforeningen foreslår derfor, at kravet om døgnbetjent kontaktpunkt erstattes med tidsfrister for udlevering af oplysninger, eventuelt kombineret med et krav om at Politiets Teletjeneste er bekendt med systemadministrators telefonnummer.
Opretholdes kravet om døgnbemandet kontaktpunkt for bolignetforeninger, vil det reelt betyde dødsstødet for det store frivillige arbejde, der foregår rundt omkring i lokalmiljøerne med at fremme udbredelsen af internet.

Bekendtgørelsen forholder sig ikke til hvilken juridisk person der er ansvarlig for logningens gennemførsel. For en bolignetforening er ansvaret ofte meget uklart defineret. Er det således de lokale kræfter der står for den daglige drift af en bolignetforening, afdelingsbestyrelsen for boligforeningen der i sin tid initierede netværkets etablering, og muligvis ejer netværket helt eller delvist, eller er det boligforeningens hovedbestyrelse, der står med strafansvaret for logningens gennemførelse?
Uanset hvem, der står med det strafretslige ansvar, så vil strafansvar i denne sammenhæng gøre etablering og drift af bolignetforeninger overordentligt vanskeligt fremover. Der er ingen tvivl om, at de frivillige der i dag udfører et stort og ulønnet arbejde i bolignetforeningerne rundt omkring i landet, vil have ganske vanskeligt ved at påtage sig et strafansvar igennem udførelsen af et stykke frivilligt arbejde. Såfremt ansvaret placeres hos hovedbestyrelsen for boligselskabet, vil dette ganske givet betyde, at der kommer et pålæg ovenfra om at sådanne anlæg ikke kan etableres fremover, idet hovedbestyrelsen næppe vil være interesseret i at pådrage sig et strafansvar, som de i praksis ikke kan styre - i og med at de intet har at gøre med den daglige drift - herunder logning.

Bolignetforeningerne har spillet en ganske væsentlig rolle i etableringen af Danmark som foregangsland på internettet. Etableringen af bolignetværk har således i væsentligt omfang fået de lidt teknologiforskrækkede borgere på internettet, idet de har fået den fornødne hjælp fra naboer og netværksfolk i boligområdet. Bolignetforeningerne er ofte etableret og drevet af frivillige kræfter i lokalmiljøet på ikke kommerciel basis. Bekendtgørelsen vil påføre disse ildsjæle, der i forvejen udfører et stort ulønnet arbejde, endnu en tung teknisk-administrativ byrde. I praksis kan dette give en række bolignetforeninger store problemer, idet ildsjælene simpelthen bukker under for arbejdspresset og kaster håndklædet i ringen.
Bolignetforeningen synes selvsagt at det er ærgerligt, hvis det ikke også fremover vil være praktisk muligt at etablere bolignetforeninger.

I de tilfælde hvor en bolignetforening vælger at kontrahere med tredjepart til gennemføring af logning, hvilket for en del foreningers vedkommende vil være deres eneste reelle mulighed for at leve op til bekendtgørelsen, da de ikke besidder den nødvendige tekniske ekspertise, påtager tredje part sig dermed også strafansvar for logningens gennemførelse?

Det er Bolignetforeningens opfattelse, at der i dag er en generel mangel på viden om hvad bolignetforeningers rettigheder og pligter er overfor politiet. Dette bliver ikke bedre når herværende bekendtgørelse træder i kraft. Specielt mener vi, at det er helt afgørende, at der udarbejdes minimumsretningslinier for hvorledes bekendtgørelsen **samt** relevant lovgivning omkring opbevaring af persondata kan honoreres i praksis.
Såfremt bolignetforeningerne skal udføre dette arbejde, er det nødvendigt at det ikke skal gennemføres på baggrund af vores skøn, men kan baseres på vejledninger indeholdende minimumskrav til tekniske specifikationer samt softwaremæssige forhold. Dette er ikke tilfældet med herværende bekendtgørelse.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Teknisk del

På det tekniske område er bekendtgørelsen efter Bolignetforeningens opfattelse alt for uklar. I sit udgangspunkt synes bekendtgørelsen at lægge op til at hvad der kan registreres skal registreres, og hvad der ikke kan registreres skal ikke registreres. Bekendtgørelsens manglende specifikation af præcis hvad der kræves registreret vil medføre, at det er op til domstolene at afgøre om fx en bolignetforening har gjort sit arbejde ordentligt. Det er ikke et ønskværdigt forhold for hverken domstolene eller bolignetforeningerne.
Endvidere finder Bolignetforeningen det yderst uheldigt at pålægge bolignetforeninger og andre et strafansvar, når det reelt er umuligt at finde ud af hvornår man som registeringspligtig har opfyldt sin logningsforpligtelse.

De tekniske uklarheder medfører som beskrevet, at det er uklart præcis hvilke oplysninger der skal registreres, og det er derfor også uklart hvilke omkostninger denne registrering vil påføre fx bolignetforeninger. Indsamling af en række af de i bekendtgørelsen skitserede registreringsoplysninger vil kræve en betydelig investering i udstyr. Endvidere fremgår det ikke af bekendtgørelsen og tilhørende vejledning, at pålideligheden af de registrerede oplysninger af rent tekniske grunde kan være endog yderst tvivlsom. Eksempelvis kan opkaldende IP adresser og e-mail adresser forfalskes og datakommunikation kan krypteres (fx i netbanksystemer og netbetalinger).

I de følgende afsnit beskrives en række af de tekniske uklarheder som Bolignetforeningen mener kræver afklaring. Beskrivelserne er forsøgt holdt i et letforståeligt sprog, og hvor nødvendigt henvises der til appendiks.

Med udgangspunkt i de nedenfor beskrevne forhold mener Bolignetforeningen, at det for al datakommunikation alene er meningsfuldt og hensigtsmæssigt at registrere opkaldende og opkaldte IP adresse, tidspunkt, eventuelt TCP portnummer, og geografisk lokation forstået som den lejlighed i foreningen som kommunikationen hidrører.

Registrering af trafik

Udbyder skal ifølge bekendtgørelsen registrere trafik (§ 2, stk. 1, nr. 5), hvilket i den tilhørende vejledning specificeres som den anvendte trafiktype.
Trafiktype er ikke noget veldefineret begreb indenfor datakommunikation, og derfor er det yderst uheldigt at vejledningen til bekendtgørelsen ikke indeholder et eneste eksempel på hvad der forstås ved trafiktype for datakommunikation.

Headerinformation fra netværksprotokoller (fx Internet Protocol) og transportprotokoller (fx Transmission Control Protocol) er umiddelbart tilgængelige i systemer der viderebefordrer datakommunikation, mens information om hvilken applikationsprotokol der anvendes (fx Hypertext Transport Protocol [HTTP] eller Simple Mail Transfer Protocol [SMTP]) ikke er umiddelbart tilgængelige (se appendiks).
Hvis der med trafiktype menes applikationsprotokol vil det pålægge bolignetforeninger betydelige omkostninger til registrering. Endvidere kan applikationsprotokollen være umulig at fastlægge fordi kommunikationen krypteres eller der er tale om en ubeskreven applikationsprotokol. Derfor vil pålideligheden af informationen om den anvendte applikationsprotokol være forbundet med betydelig usikkerhed.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk

Boligretforeningen finder det derfor uklart hvad, der i bekendtgørelsen forstås ved trafik/trafiktype i forbindelse med datakommunikation.
Det er Boligretforeningens opfattelse, at den endelige bekendtgørelse klart bør specificere hvad der menes med registrering af trafik i forbindelse med datakommunikation, ellers vil det være umuligt at afgøre om man som registreringspligtig opfylder kravene til registrering. Endvidere vil omkostningerne til registrering være særdeles afhængige af hvad der menes med trafiktype.

Det er Boligretforeningens opfattelse at den endelige bekendtgørelse ikke bør kræve specifikation af trafik udover transportprotokol og eventuelt dertil knyttet portnummer. Dette er begrundet med, at identifikation af anvendt applikationsprotokol i visse tilfælde vil være umulig (krypteret kommunikation, fx netbank, eller en ubeskrevet applikationsprotokol), og hvor den er mulig vil være forbundet med betydelige meromkostninger for udbyder, idet disse informationer ikke er umiddelbart tilgængelige i dennes systemer og derfor vil kræve intensiv pakkeanalyse at fremskaffe.

Af bekendtgørelsen fremgår det endvidere, at det skal registreres om kommunikationen blev gennemført, om der blev etableret forbindelse til den opkaldte identitet og, hvis dette ikke er tilfældet, hvorfor kommunikationen ikke blev gennemført. Vedrørende datakommunikation vil det i en lang række tilfælde være umuligt, at indsamle disse oplysninger. Eksempelvis har visse almindeligt anvendte transportprotokoller (fx UDP) ikke nogen defineret sekvens eller forløb, og dermed ingen afslutning. Det giver i så fald ikke mening, at tale om kommunikationens afslutning.
Det vil oftest også være umuligt at afgøre, hvorfor en given netværkspakke ikke nåede den opkaldte identitet (var serveren slukket, forbindelsen afbrudt eller noget helt tredje).
Boligretforeningen mener derfor ikke, at en registrering af om kommunikationen blev gennemført giver mening for datakommunikation, og derfor bør et sådant krav bortfalde.

Opkaldende og opkaldte identitet

For datakommunikation fremgår det af bekendtgørelsen og dertilhørende vejledning, at opkaldende identitet og opkaldte identitet (og ændring af disse) er IP-adresser (se fx vejledningen, side 17, eksemplet om internet ADSL).

En IP adresse identificerer i sig selv alene en computer tilkoblet internettet, og indeholder derfor hverken information om hvem, der anvender denne computer eller hvor, den rent geografisk er lokaliseret (se appendiks).

Det er for Boligretforeningen uklart hvordan en IP adresse kan anvendes i efterforskningsøjemed, medmindre denne IP adresse specifikt identificerer en slutbruger (fx et medlem af en boligretforening) eller en præcis geografisk lokation (fx en lejlighed som har forbindelse til foreningens netværk).
Trods dette er slutbrugeridentitet (fx navn og CPR-nummer) ikke nævnt i bekendtgørelsen eller dertilhørende vejledning, og lokaliseringsdata er ikke anført i typeeksemplet på de oplysninger, som udbyder af datakommunikation typisk skal udlevere til myndighederne (vejledningen, side 17, eksemplet om internet ADSL).

I eksisterende boligretforeninger identificerer en opkaldende IP adresse indenfor foreningen i dag enten

Tlf: 36 96 30 56
kontakt@boligretforeningen.dk
www.boligretforeningen.dk

i) en arbitrær computer tilsluttet foreningens netværk,
ii) en specifik lejlighed som er tilkoblet foreningens netværk, eller
iii) en unik slutbruger (fx hvor login er påkrævet for etablering af forbindelse til internettet).
I en række bolignetforeninger vil det være forbundet med betydelige udgifter at indkøbe udstyr der kan fastlægge hvilken lejlighed der kommunikerer med en given IP-adresse.

For Bolignetforeningen er det afgørende at den endelige bekendtgørelse klart specificerer hvad, der forstås ved opkaldende identitet og opkaldte identitet i forbindelse med datakommunikation. Såfremt der med opkaldende identitet menes identiteten af en slutbruger, pålægges bolignetforeninger en identifikationsbyrde som er langt tungere end det er tilfældet for fastnettelefoni, hvor lokaliseringsdata for kommunikationsudstyret synes tilstrækkelig (fx en adresse tilknyttet et givent telefonnummer).
Såfremt bolignetforeninger skal identificere slutbrugere, bør det endvidere fremgå af den endelige bekendtgørelse hvilke legitimationskrav bolignetforeninger pålægges i forbindelse med identifikation af medlemmer (fx billedlegitimation i form at pas eller kørekort).

Hvis den opkaldende identitet fastlægges udfra sammenkobling af IP adresse med lokaliseringsdata (den fysiske adresse hvor slutbrugerens kommunikationsudstyr er koblet på udbyderens netværk) bør disse anføres blandt de informationer, som udbyder af datakommunikation typisk skal udlevere til myndighederne (vejledningen, side 17, eksemplet om internet ADSL).
Anvendelse af trådløse netværk umuliggør endvidere en præcis fastlæggelse af geografisk lokation. Kravet om registrering af geografisk lokation (fx lejlighed) kan derfor hindre udbredelsen af trådløse netværk i fx bolignetforeninger.

For Bolignetforeningen er det endvidere uklart, hvilke oplysninger der kræves opsamlet, når en opkaldt IP-adresse udenfor foreningen dækker over hvad der kan opfattes som flere forskellige identiteter. Et ofte forekommende eksempel på dette er såkaldte hosting-firmaer, som tilgængeliggør hjemmesider tilhørende flere forskellige domæner (fx www.dr.dk, www.pol.dk) fra samme IP adresse (dvs. samme computer). I disse tilfælde vil en IP-adresse i sig selv ikke entydigt identificere hvilke af disse domæner som opkaldes. Fastlæggelse af hvilket domæne, der i en sådan situation opkaldes, forudsætter analyse af kommunikationens indhold (se appendiks) og vil påføre bolignetforeninger væsentlige omkostninger til analyseudstyr.

Bolignetforeningen finder det derfor af afgørende betydning, at det i den endelige bekendtgørelse nærmere specificeres hvad der menes med opkaldte identitet.

Registrering af e-postadresser

Ifølge bekendtgørelsen og dertilhørende vejledning skal en udbyder, som overfører elektroniske postbeskeder mellem en bruger og en e-postserver, registrere e-postadresserne på afsender og modtager. Endvidere skal dato, tid, og unik identitet involveret i alle adgange til en e-postadresse tilknyttede e-poster registreres.

Begreberne afsenders og modtagers e-postadresse er uklart beskrevet i bekendtgørelsen. Det er eksempelvis muligt at anføre hvad som helst i e-postens "To"-felt, eftersom det er "RCPT to"-kommandoen i (SMTP-)kommunikationen med e-postserveren, som har betydning for hvem e-posten afleveres til. Med andre ord er det temmelig ligegyldigt at registrere "To"-feltet.

Tlf: 36 96 30 56
kontakt@bolignetforeningen.dk
www.bolignetforeningen.dk