Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 166 | januar 2001

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

Total kontrol på Internettet

Terror er løftestang for at give politiet vide muligheder for at overvåge borgerne

Terrorlove begrænsninger retten til at kommunikere frit >

Efter terrorangrebene på New York og Washington d. 11. September 2001 har en række lande gennemført lovgivning rettet mod at bekæmpe terror. Fælles for meget af denne lovgivning er, at den griber ind i borgernes ret til at kunne kommunikere frit uden at nogen overvåger, hvem man taler med, hvor man taler fra og hvad man taler om.

Tre nye sæt retsregler på vej om overvågning og registrering af kommunikation >

I denne uge skal den danske regerings terrorpakke behandles, men den er blot en af tre nye sæt retlige regler, der vil gribe ind i kommunikationshemmeligheden. De to andre er Europarådet konvention om cyberkriminalitet og et nyt direktivforslag fra Europa-Kommissionen.

Samlet kan de resultere i "særdeles høj" grad af overvågning, advarer professor >

Teknologirådets sekretariat har bedt professor, dr. Jur. Peter Blume fra Københavns Universitet om at vurdere rækkevidden af de tre sæt regler. Han konkluderer, at de samlet kan medføre en "særdeles høj" grad af overvågning af borgerne, og advarer mod, at det kan få borgerne til at bruge elektronisk kommunikation mindre i strid med ønsket om at fremme Danmark som IT-samfund.

Notat om effekterne på med dette nyhedsbrev og på Teknologirådets hjemmeside >

Notatet er vedhæftet dette nyhedsbrev, og kan også findes på Teknologirådets hjemmeside: www.tekno.dk

I de kommende måneder vil Folketinget og regeringen skulle tage stilling til tre nye sæt retlige regler, der alle omhandler overvågning af borgernes brug af elektronisk kommunikation:
Regeringens Terrorpakke, Europarådets Konvention om Cyberkriminalitet samt Europarådets forslag til direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.
Særligt Terrorpakken og Europarådets konvention kan give politi og andre myndigheder bedre muligheder for at overvåge og registrere borgernes kommunikation og færden.
Teknologirådet har bedt professor, dr.jur. Peter Blume, Københavns Universitet om at vurdere effekten for borgernes ret til at kunne kommunikere i fred af de tre regelsæt i sammenhæng. Hvis de vedtages og indføres i dansk lov.

Konklusionen er at finde i notatet "Overvågning af og i cyberspace" udarbejdet af Peter Blume for Teknologirådet, og den er klar: "Al internettrafik registreres fremover", "Alle vil være overvågede" og "disse bestemmelser medfører at computeren i større udstrækning kan blive opfattet som et utrygt kommunikationsmiddel."

Hvad, hvor og med hvem

Indgreb i meddelelses- eller kommunikationshemmeligheden kan opdeles i tre efter hvilke oplysninger, der bliver registreret:

1. indholdsdata – hvad siger eller skriver vi til hinanden. Dette kan være en telefonaflytning eller adgang til at læse e-mails.
2. de såkaldte trafikdata – hvem har talt i telefon eller på anden måde kommunikeret

elektronisk med hinanden, og hvornår er det sket.
3. lokaliseringsdata – hvor var vi, da vi talte sammen. Dette indebærer også overvågning og registrering af, hvor mobiltelefoner har været, mens de har været tændt.

Terrorpakken og Europarådets konvention kan begge siges at trække i retning af en begrænsning i retten til fri kommunikation. Europa-Kommissionens direktivudkast er derimod først og fremmest rettet mod at beskytte borgerne mod overvågning og registrering af deres elektroniske kommunikation. Men i notatet advarer professor Peter Blume mod at tro, at direktivet kan fungere som modvægt til terrorpakken og Europarådets konvention.
"Direktivet vil kun gælde for områder omfattet af EU-retten..., og i artikel 15 (1) fastslås udtrykkeligt, at direktivets regler kan fraviges i forbindelse med kriminalitetsbekæmpelse og af hensyn til statens sikkerhed," hedder det.

Samlende konkluderes det i notatet: "..i et demokratisk samfund kan politiet ikke have alle muligheder. Et demokrati forudsætter, at borgerne har et frihedsområde og i nutidens samfund omfatter dette område muligheden for fri og uovervåget kommunikation. Denne mulighed kan ikke være ubegrænset. Men samlet fører de regler, der er omtalt ovenfor, let til en situation med en særdeles høj overvågningsintensitet. Dette bestyrkes af den øgede internationale udveksling af oplysninger, som bl.a. Cybercrimekonventionen indebærer" Denne situation kan let føre til, at nogle, lovlydige borgere vælger andre kommunikationsformer, således af digitaliseringen ikke bliver så udbredt som det samfundsmæssigt er ønskeligt."

Notatet i sin fulde længde er vedhæftet dette nyhedsbrev og kan også findes på Teknologirådets hjemmeside www.tekno.dk

Terrorpakken

Regeringens terrorpakke er fremsat som lovforslag L 35 den 13. december 2001. Store dele af pakken er en overlevering fra tidligere justitsminister Frank Jensens forslag til terrorpakke fra 30. oktober 2001.
Terrorpakken giver politiet større adgang til trafik- og lokaliseringsdata, men berører ikke direkte adgangen til indholdsdata. I de fleste tilfælde vil det også være nødvendigt for politiet at få en dommerkendelse før de får adgang til de registrerede data.
Peter Blume advarer dog i sit notat mod at have for meget tiltro til, at dette vil garantere borgernes retssikkerhed:
"... konsekvensen af forslaget [er], at adgangen til indholdsdata udvides. Det er ikke kun kommunikationen, der bliver mere åben."
Og:
"... retsgarantien [er] måske ikke så stor og under alle omstændigheder må fremhæves, at det ikke i sig selv kan begrunde de forskellige regler, at deres anvendelse forudsætter en retskendelse."

L 35 kan findes på Folketingets hjemmeside:
http://www.ft.dk/Samling/20012/lovforslag_oversigtsformat/L35.htm

Europarådets konvention om Cyberkriminalitet

Konventionen er resultatet af flere års arbejde. Det er således ikke – som terrorpakken – en direkte reaktion på terrorangrebene på New York og Washington 11. september 2001.
Danmark har endnu ikke underskrevet konventionen (den blev underskrevet 23. november 2001 blot tre dage efter det danske valg), men alle vores EU-partnere bortset fra Irland og Luxembourg har.
Konventionen, der udvider adgangen til at registrere oplysningerne om borgernes brug af elektronisk kommunikation, er rettet mod såkaldt cyberkriminalitet. Dette defineres meget bredt i konventionen som "enhver form for kriminalitet, der begås ved hjælp af en computer.
Om konventionen skriver professor Peter Blume:
"Det er åbenbart, at kommunikationshemmeligheden hermed får trange kår... [der] vil opstå utryghed og et ubehag ved, at man ved, at ens data og kommunikation opbevares. Alle vil være overvågede."

Europarådets konvention om cyberkriminalitet, samt liste over lande, der har underskrevet den, kan findes på:
http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm

Kommissionens direktivforslag

Direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000) 385 skal afløse direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren. Det sidstnævnte direktiv skulle være omsat til national lov senest den 24. oktober 1998. dette er dog ikke sket i alle lande endnu.

Fra rådet til tinget udgives af Teknologirådets sekretariat. Dette nummer er skrevet af Mette Bom på baggrund af resumé af projektleder Morten Jastrup

De seneste fem numre af Fra rådet til tinget er:
165: En naturlig udvikling?
Særnummer om bioteknologi.
164: Stejl debat om beriget mad
163: Udstøder teknologien ældre?
162: Kroppen som identifokation
161: Open Source er ikke slået igennem

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm

Overvågning af og i cyberspace

1. Dette notat kommenterer i hovedtræk en række forslag til nye retlige regler, der tager sigte på at øge mulighederne for at overvåge og efterspore den digitale kommunikation. Disse tiltag indebærer i almindelighed en reduktion af kommunikationshemmeligheden og kan ligeledes begrænse privatlivets fred. De har således betydning for udøvelsen af de rettigheder, der er fastslået i artikel 8 og 10 i den europæiske menneskerettighedskonvention. Formålet med de nye regler er at forbedre og effektivisere mulighederne for at efterforske kriminalitet, herunder terror. Problemstillingen er herefter om de modstridende hensyn er tilstrækkeligt afbalancerede.
Grundlaget for det følgende er Europarådets konvention om cyberkriminalitet af 23.11.2001, som endnu ikke er underskrevet af Danmark, jfr. under 4-6, Europa-Kommissionens forslag til direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000)385), der skal erstatte direktiv 97/66 EF og som forventes vedtaget i starten af 2002, jfr. under 3, samt lovforslag L35 af 13.12.2001 om ændring af bl.a. retsplejeloven, jfr. under 7-10.

2. Som nævnt er de forskellige tiltags overordnede formål, at politiet i forbindelse med efterforskning af kriminalitet skal have gode muligheder for at fa adgang til de data, der befinder sig på eller har været formidlet via Internettet. Adgangen til at foretage indgreb i meddelseshemmeligheden, der reguleres i retsplejelovens kapitel 71, skal styrkes. Dette er aktuelt i forhold til (1) oplysningernes indhold, (2) kommunikationsforløbet, de såkaldte trafikdata, og (3) lokaliseringsdata, der giver viden om, hvor kommunikationen har fundet sted. Der er tale om en vidtgående aspiration, der kan gøre digital kommunikation mere gennemsigtelig end traditionel analog kommunikation.

3. Ved vurderingen af disse tiltag har konventionen og det fremsatte lovforslag størst interesse. Direktivforslaget tager sigte på at beskytte den enkeltes kommunikation, jfr. især artikel 5(1) og begrænser som udgangspunkt adgangen til at fa kendskab til såvel trafikdata som lokaliseringsdata. Dette forslag kunne opfattes som en modvægt i forhold til ønskerne om en bedre adgang til digitalt kommunikerede data, men direktivet vil kun gælde for områder omfattet af EU-retten, jfr. præamblens betragtning 10, og i artikel 15(1) fastslås udtrykkeligt, at direktivets regler kan fraviges i forbindelse med kriminalitetsbekæmpelse og af hensyn til statens sikkerhed. Dette svarer i øvrigt til artikel 13(1) i det almindelige databeskyttelsesdirektiv (95/46 EF). Selvom Europaparlamentet har vedtaget et ændringsforslag, hvorefter det skal præciseres, at indskrænkninger i de fastsatte rettigheder kun kan gennemføres, såfremt dette er nødvendigt af hensyn til demokratiet, må det formodes, at formuleringer af denne karakter næppe vil have reel betydning og at det kommende direktiv i forhold til kriminalitetsefterforskning ikke vil udgøre en beskyttelse af den enkelte. I det følgende lægges vægten derfor på konventionen og det fremsatte lovforslag.

4. Det fremgår af konventionens artikel 14(1)b, at den finder anvendelse i forhold til enhver form for kriminalitet, der begås ved hjælp af en computer, idet dog umiddelbar overvågning af trafikdata (artikel 20) af konventionsstaterne kan begrænses til at angå visse former for kriminalitet. De under 5 og 6 nævnte regler har dermed ikke kun betydning for den særlige edbkriminalitet, der er opregnet i artikel 2 til 1 l. Som udgangspunkt er der således ikke nogen begrænsninger, men i dansk ret som i mange andre lande er det anerkendt, at der skal være et rimeligt forhold (proportionalitet; retsplejelovens § 782, stk. 1) mellem forbrydelsen og de efterforskningsskridt, der bliver taget. Konventionen

bryder ikke med dette princip, jfr. artikel 15(2), hvilket yderligere bestyrkes af artikel 15(1), der betoner, at menneskerettighedskonventionen skal respekteres. I denne forbindelse må
understreges, at disse grundlæggende rettigheder kun indebærer mere overordnede begrænsninger i forhold til de foranstaltninger, der omtales i det følgende.

5. Ifølge artikel 16(1) kan det bestemmes, at opbevarede data, incl. trafikdata, skal udleveres. Teleselskaber m.fl. kan efter artikel 16(2) pålægges at opbevare data i op til 90 dage, jfr. hertil under 9. I artikel 17 præciseres yderligere, at trafikdata kan kræves opbevaret og udleveret. Dette gælder efter artikel 18 for enhver person samt for teleskaber/ISPer. Det er åbenbart, at kommunikationshemmeligheden herved far trange kår og at private selskaber far pålagt funktioner, som det ikke er naturligt, at de varetager, jr. de allerede gældende regler i retsplejelovens § 786 og yderligere under 9.
Heroverfor anføres ofte, at alle os, der er lovlydige og ikke har noget at skjule, jo ikke behøver at frygte noget. Dette argument er dog ikke tvingende, eftersom der let vil opstå en utryghed og et ubehag ved at man ved, at ens data og kommunikation opbevares. Alle vil være overvågede. Denne iagttagelse er også relevant i forhold til det fremsatte lovforslag, jfr. nedenfor.

6. Konventionen åbner mulighed for en række andre former for indgreb overfor den digitale kommunikation. Ifølge artikel 19 skal det være muligt at søge og beslaglægge data. Efter artikel 20 skal der kunne ske umiddelbar ("real time") indsamling af trafikdata (aflytning), medens artikel 21 indebærer at oplysningernes indhold skal kunne opfanges umiddelbart, ligesom ISPer skal kunne pålægges at gøre dette. Også disse bestemmelser medfører, at computeren i større udstrækning kan blive opfattet som et utrygt kommunikationsmiddel.

7. Regeringens lovforslag henviser til en række FN-vedtagelser, men ikke til cybercrimekonventionen, der som nævnt endnu ikke er underskrevet af Danmark. En række af de fremsatte forslag minder dog om konventionens. Lovforslaget er særdeles omfattende, men i det følgende inddrages kun de bestemmelser, der har betydning for moderne kommunikation.

8. Lovforslaget vedrører ikke direkte spørgsmålet om politiets adgang til indholdsdata. Det er en pointe i det fremsatte forslag, at der skal være bedre muligheder for at overvåge kommunikation (trafik- og lokaliseringsdata) og at disse nye muligheder herefter suppleres af de allerede i retsplejeloven (§ 780) etablerede muligheder for forskellige former for aflytning. Selvom dette fremhæves i forslagets bemærkninger (f.eks. side 46 og 72) er konsekvensen af forslaget, at adgangen til indholdsdata udvides. Det er ikke kun kommunikationen, der bliver mere åben.

9. I § 786, stk. 4, foreslås indført en regel, hvorefter teleudbydere skal have pligt til at registrere og opbevare trafikdata i 1 år. En betydelig længere periode end konventionens 90 dage, jfr. under 5. Bestemmelsen suppleres af stk. 5, hvorefter der kan fastsættes regler om udbydernes bistand til politiet, og en række strafferegler i stk. 6 og 7. Opbevaringspligten omfatter bl.a. de anvendte (dynamiske) 1P-adresser. Opbevaringspligten er bredt bestemt, idet den skal være "til brug for efterforskning og retsforfølgning af strafbare forhold". Dette betyder reelt, at alle trafikdata skal opbevares, idet disses efterfølgende udlevering til politiet vil bero på andre bestemmelser, herunder § 780. Formålsangivelsen er i og for sig overflødig. Al Internettrafik registreres fremover.
Denne ordning sætter som tidligere nævnt fokus på de private teleudbyderes position. I bemærkningerne til stk. 5 nævnes (side 48), at personale vil kunne sikkerhedsgodkendes,

men spørgsmålet om en autorisationsordning er uomtalt. Det er ikke kun staten, der kan true privatlivet, og det forekommer ikke betryggende, at private udbydere, der kan være hvem som helst, kan foretage denne opbevaring. En nærmere registrering af adgangen til at være teleudbyder bør derfor overvejes.

10. Efter forslagets § 791b gives der mulighed for, at politiet kan foretage såkaldt datalæsning, f.eks. ved at installere et snifferprogram. Denne bestemmelse, der kan karakteriseres som en art distanceransagning, angår også trafikdata. Den kan kun anvendes ved efterforskning af særlige former for kriminalitet (stk. 1, nr. 3) og kun når dette er af afgørende betydning og når dette er proportionalt. Uanset disse egrænsninger er datalæsning et vidtgående skridt, der svækker tiltroen til computeren. Den kan blive en fjende.
§ 791b gælder for datalæsning "af ikke offentligt tilgængelige oplysninger", men altså ikke når der søges tilgængelige oplysninger på hjemmesider etc. Ifølge bemærkningerne (side 73) er læsning af sidstnævnte ikke et tvangsindgreb og politiet kan frit gøre dette. Denne opfattelse, der muligvis formelt juridisk er rigtig, forekommer ikke betryggende og mindsker yderligere tilliden til computeren.

11. Forinden nogle sammenfattende iagttagelser angives, er det hensigtsmæssigt at inddrage spørgsmålet om de processuelle betingelser for, at politiet kan benytte de nye muligheder, der kan blive en del af dansk ret inden længe. I langt de fleste tilfælde vil de forskellige indgreb i meddelelseshemmeligheden forudsætte en retskendelse, hvilket ofte fremhæves som en væsentlig retsgaranti. Dette er nok også berettiget, men der savnes så vidt vides undersøgelser af i hvilket omfang, domstolene i sager af denne karakter ikke giver den ønskede kendelse. Det forekommer nærliggende, at sådanne kendelser især i sager vedrørende terror og statens sikkerhed stort set altid vil blive givet.
Er dette rigtigt, er retsgarantien måske ikke så stor og under alle omstændigheder må fremhæves, at det ikke i sig selv kan begrunde de forskellige regler, at deres anvendelse forudsætter en retskendelse.

12. Der er ingen tvivl om, at det er samfundsmæssigt ønskeligt, at kriminalitet bekæmpes. Desto grovere kriminaliteten er, jo mere ønskelig er dens bekæmpelse. Det er ligeledes klart, at samfundet må værge sig imod terrorisme. Dette udgangspunkt er der næppe nogen uenighed om og det er ligeledes klart, at det er en konsekvens heraf at politiet skal have gode efterforskningsmuligheder, hvilket selvsagt også må gælde i den digitale verden. Det er dog ligeledes klart, at i et demokratisk samfund kan politiet ikke have alle muligheder. Et demokrati forudsætter, at borgerne har et frihedsområde og i nutidens samfund omfatter dette område muligheden for fri og uovervåget kommunikation. Denne mulighed kan ikke være ubegrænset, men samlet fører de regler, der er omtalt ovenfor, let til en situation med en særdeles høj overvågningsintensitet. Dette bestyrkes af den øgede internationale udveksling af oplysninger, som bl.a. cybercrimekonventionen indebærer. Denne situation kan let føre til at nogle, lovlydige, borgere vælger andre kommunikationsformer, således at digitaliseringen ikke bliver så udbredt som det samfundsmæssigt er ønskeligt.
Det er derfor nødvendigt med stor omtanke og besindighed. Det er velkendt, at har man først givet nye efterforskningsmuligheder, vil disse ikke forsvinde igen. Dette gælder uanset en revisionsbestemmelse som lovforslagets § 8. En nøje gennemtænkt afbalancering af de modstridende hensyn er derfor det mål, der bør være styrende for den fortsatte retspolitiske proces.

Peter Blume Januar 2002