

København 4. november 2005

## Digital Rights kommentarer til rapport om "Det Danske Samfunds indsats og beredskab mod terror" af 3. november 2005.

Torsdag den 3. november 2005 fremlagde Regeringens embedsmandsudvalg 49 forslag om udvidede beføjelser til brug for bekæmpelse af terror. Efter en drøftelse af forslagene vil Regeringen medio november fremlægge et forslag til ny terrorkpakke. Forslagene omfatter markante nye overvågningstiltag og udvidede beføjelser til politiet, som vil ændre balancen mellem borgerne og staten og leder tanken hen på et overvågningssamfund. Digital Rights opfordrer til en grundig debat om forslagene, deres brugbarhed i terrorbekæmpelsen og konsekvenser for almindelige borgere.

I 2002 blev der med den første terrorkpakke indført lovhjemmel til at påbyde tele og internetudbydere at opbevare oplysninger om telefoni og email i et år. En bekendtgørelse skulle præcisere, hvordan det skulle foregå i praksis. Det er stadig ikke lykkedes. Efter to år kom et udkast, der blev skarpt kritiseret af blandt andet teleindustrien, fordi det ville medføre omfattende lagring af oplysninger i en grad, der ville koste enorme summer for teleselskaberne. Derudover vil der altid være muligheder for at undgå registrering, hvorfor forslaget, ifølge IT og Tele branchen, var at sammenligne med "et hegn med et stort hul i". Endvidere var der principielle problemer med den omfattende registrering, som også er kernen i de nye forslag. I forhold til implementering af loven fra 2002 har man valgt at vente på en eventuel lovgivning fra EU. Men det ændrer ikke ved, at omfattende overvågning af borgerne på mange måder er problematisk.

Helt grundlæggende er det tvivlsomt, om selv omfattende overvågning af borgerne kan hindre terror. Samtidig er der vigtige hensyn, som skal tages med i overvejelserne. Overvågning ændrer borgernes adfærd i frygten for at opføre sig mistænkeligt, og overvågning skader demokratiet og tilliden mellem borger og stat. Det uddybes sidst i dette papir.

### Adgang til personlige oplysninger

Arbejdsgruppen anbefaler, at PET skal kunne indhente oplysninger fra andre myndigheder, som ikke er knyttet til på forhånd navngivne personer, når videregivelsen kan have betydning for varetagelsen af tjenestens opgaver (punkt 10). Der skal ikke være tale om en konkret begrundet mistanke mod en person. Forslaget giver derfor PET meget vidtgående beføjelser til at få alle slags oplysninger, som *kan* have betydning for varetagelse af tjenestens opgaver. Det anføres, at de oplysninger, som Politiets Efterretningstjeneste vil kunne indhente hos andre myndigheder, ofte må forventes at ville have et "ikke ubetydeligt omfang". Da der er tale om til tider ganske følsomme, personlige oplysninger om borgerne, ville det være rimeligt, at de kun videregives, såfremt det kan sandsynliggøres, at de er vigtige for

eftersforskningen af en straffesag. Derfor bør adgangen til oplysninger bør være specifikt rettet mod de oplysninger, der er behov for.

## **Samfundet indrettes med henblik på overvågning**

Arbejdsgruppen anbefaler, at man indretter kommunikationsteknikken sådan, at politiet altid kan overvåge (punkt 15). Arbejdsgruppen bemærker, at det muligvis vil være nødvendigt at udvikle nye tekniske løsninger for at kunne opfylde en sådan forpligtelse. Der skal altså ikke kun være muligt at udlevere tilgængelige oplysninger, men samfundet skal indrettes med henblik på politiets eftersforskning. Arbejdsgruppen fremhæver selv det vanskelige ved at pålægge private udbydere at indsamle oplysninger til politiet. Det nævnes, at der ud over de store "traditionelle" teleselskaber findes en række foreninger (der skal tælles i tusinder) – f.eks. boligforeninger eller antenneforeninger – der typisk udbyder internettjenester eller telefoni gennem etablering af lokale net. Da omkostningerne ved at ændre de tekniske systemer vil kunne virke meget byrdefulde for især mindre udbydere, bør det efter arbejdsgruppens opfattelse overvejes at undtage de helt små udbydere, herunder f.eks. andelsbolig- og antenneforeninger. Med andre ord et tydeligt eksempel på, at det alligevel ikke er muligt at gå hele vejen og overvåge alle samfundets kroge. Og at det altid vil være muligt – hvis man virkelig har noget at skjule, at undslå sig den overvågning, der skal hindre terror.

Arbejdsgruppen foreslår også, at eksisterende muligheder for at foretage sig noget uden for statens overvågning, afskaffes. Der peges specifikt på taletidskort netcaféer, der skal 'elimineres' eller – hvis dette ikke er muligt – reduceres i videst muligt omfang. (punkt 16). Hvorledes dette skal ske, er et åbent spørgsmål. Internettet har muliggjort en række nye fleksible og billige kommunikationsformer, f.eks. offentlige internetterminaler, anonyme taletidskort, IP-telefoni og anonyme chatrooms. Flexibiliteten og den lave pris hænger netop sammen med, at disse tjenester fungerer uden registrering af store mængder data, etablering af centrale servere, ansættelse af stort personale m.v. Et krav om at muliggøre aflytning af teleoplysning kan reelt betyde, at disse meget populære og udbredte tjenester må afvikles. Det vil indskrænke borgernes kommunikationsmuligheder. Billig og udbredt internetadgang styrker informations og ytringsfriheden, som er vigtige dele af et åbent og frit samfund og som vi – ikke mindst i terrorbekæmpelsens navn – har god grund til at styrke.

## **Systematisk og omfattende overvågning af alle borgere**

Arbejdsgruppen anbefaler, at politiet hos alle teleudbydere skal have mulighed for at indhente tele- og masteoplysninger. (punkt 18). For at politiet til enhver tid skal kunne have oplysninger om brugernes kommunikation tilbage i tiden, skal teleudbyderne hele tiden gemme disse oplysninger. Der skal altså hos private teleselskaber oparbejdes enorme lagre af oplysninger om borgerne. Ikke fordi teleselskabet skal bruge oplysningerne til at drive deres virksomhed, men fordi alle borgere potentielt senere kan blive interessante for politiet i forbindelse med en straffesag. Dette er et af de mest

vidtgående forslag, både fordi overvågning ikke begrænses til bestemte typer information, og fordi opbevaringen ikke tidsbegrænses til en kort periode, fordi borgernes kommunikation overvåges systematisk og generelt. Der er ikke tale om en konkret mistanke, og der er ikke sikkerhed mod misbrug af alle disse oplysninger. Når politiet skal have adgang, skal det ske hurtigt og uden retskendelse, hvorfor der igen er risiko for, at der indhentes alt for mange oplysninger på et løst grundlag. Endvidere er det uklart, hvilke virksomheder der vil være omfattet. Skal for eksempel udbydere af web-mail og chat også overvåge? Og gælder det i givet fald virksomheder og privatpersoner, der giver mulighed for chat på deres hjemmeside? Der er altså tale om overdreven kontrol i visse tilfælde, kombineret med en række smuthuller i andre. Samme betragtninger gør sig gældende for anbefalingen om udlevering af abonnementsoplysninger til politiet uden retskendelse (punkt 28).

Endnu et overraskende forslag er arbejdsgruppens anbefaling om, at teleselskaber og internetudbydere som forudsætning for at drive denne virksomhed skal registreres hos Rigspolitiets Telecenter (punkt 20). At kommunikationsformidling skal forhåndsgodkendes af politiet er et kendetegn ved en politikontrolleret stat, som vi slet ikke kender det i Danmark. Samtidig anbefales det, at undtage de helt små udbydere samt udbydere, der ikke stiller kommunikationsnet og -tjenester til rådighed på et kommercielt grundlag.

Endelig anbefales, at politiet i ganske særlige situationer kan foretage scanning af indholdet af telefonsamtaler eller anden tilsvarende kommunikation inden for et nærmere angivet område (punkt 29). Der er tale om situationer, hvor politiet ikke er nået så langt i efterforskningen, at man ved, hvem man konkret går efter. Scanning af kommunikation inden for et område vil betyde, at en større kreds af helt almindelige borgere får 'scannet' deres kommunikation. Det ville svare til, at man satte en maskine til at aflytte alle telefoner på Nørrebro og reagere, når særlige ord blev nævnt. Selvom forslaget alene tænkes anvendt ved fare for alvorlige forbrydelser, er der tale om en meget vidtgående overvågning af en bred kreds af personer, hvoraf de fleste i sagens natur vil være lovlige borgere. Man vil ikke blive informeret om, at man har været involveret i en sådan aflytning.

## **TV overvågning**

Der anbefales øget videoovervågning af større centrale pladser, væsentlige trafikknudepunkter, herunder eksempelvis Københavns Hovedbanegård, Nørreport og andre centrale stationer, Metroen, Storebælts- og Øresundsforbindelserne, turistattraktioner, forlystelsesparker, koncertsteder, stadioner, indkøbscentre med videre (punkt 33). Endvidere foreslås, at undersøge mulighederne for at opsætte helt eller delvist automatiserede overvågningsfunktioner, herunder navnlig anvendelsen af systemer, der kan aflæse biometriske data relateret til genkendelse af konkrete personer eller adfærdsmønstre (punkt 34). Hvis kameraer genkender bestemte ansigtstræk eller konstaterer adfærdsmønstre, der findes mistænkelige – måske at man

særligt tit frekventerer Nørreport station iført stor dynejakke – kan dette få konsekvenser.

Det betyder, at borgerne i langt højere grad vil blive overvåget i det offentlige rum. Ud over konstant at blive mindet om frygten for mulige terrorangreb – en frygt som terrorister formentlig vil være taknemmelig over at få hjælp til at udbrede – vil borgerne skulle vænne sig til at blive iagttaget store dele af tiden. Det er vigtigt at være opmærksom på, at der ikke foreligger nogen undersøgelser der viser, at øget tv-overvågning hindrer alvorlig kriminalitet.

## **Betydningen af at værne om borgernes fri færden**

Det vil altid være i politiets interesse at indsamle flest mulige oplysninger hurtigst og nemmest muligt. Dette hensyn er det overordnede og gennemgående grundlag for arbejdsgruppens anbefalinger, og der synes ikke at være lagt vægt på andre hensyn, som borgernes rettigheder og den generelle samfundsmæssige udvikling. De omtales kort her.

### Tvivlsomt, om overvågning hindrer terror

Helt grundlæggende bør det overvejes, om selv omfattende overvågning af borgerne kan hindre terror. Der vil altid være mulighed for at undslå sig overvågning. Der er derfor risiko for, at personer der har noget at skjule, eller borgere, der er opmærksomme på den omfattende overvågning og ønsker at være 'i fred', vil finde måder at kommunikere og færdes på uden om de overvågede steder. Derved risikeres både, at forbrydere går fri, og at der mere bredt skabes et "parallelsamfund" i protest mod myndighedernes indgriben.

### Overvågning ændrer adfærd

Overvågning har utvivlsomt en virkning på borgernes adfærd. Som borger skal man konstant have i baghovedet, hvordan ens udseende, handlinger og færden eventuelt ville se ud på et kamera eller en oversigt over ens telefon-, mail- og internetbrug. Et kamera eller en oversigt over teleoplysninger kan mangle nogle oplysninger eller give et ufuldstændigt billede af en persons handlinger. Helt lovlige borgere kan være bange for at virke mistænkelige og derfor opføre sig anderledes, end de ellers – helt lovligt – kunne have gjort. En sådan 'selvbegrænsning' skaber igen nye standarder for, hvad der er det normale og hvad der er afvigende. Hvis alle opfører sig på en bestemt måde, skal der ikke meget til, for at afvige fra normen. Derfor vil overvågning gennemgribende ændre det samfund, vi har i dag.

### Overvågning skader demokratiet

Overvågning har store konsekvenser for borgernes frihed og for demokratiet. Det personlige 'rum', hvor borgerne selv har ret til at beslutte, hvad andre skal vide, og hvad der skal blive i privatsfæren, er en vigtig forudsætning for grundlæggende værdier i et demokratisk samfund. Man kan ikke lige så frit udveksle tanker og meninger eller blive afklaret omkring religion, seksualitet eller politisk overbevisning, hvis man konstant har nogen 'kiggende over skulderen'. En illustration af dette princip er stemmeafgivelse til

kommunalvalg eller Folketingsvalg. Man er helt alene i stemmeboksen, netop for at sikre, at stemmeafgivelsen ikke påvirkes af andre personer, der kunne lægge et pres – måske indirekte - på den, der skal stemme. Det kunne være venner eller familie, eller en opfattelse af, hvad der er rigtigt eller normalt. Selv en myndighedsperson, for eksempel en politibetjent, er af denne grund utænkelig som ledsager i stemmeboksen.

## Overvågning skader tilliden mellem borger og stat

I Danmark er der en udstrakt tillid til myndighederne og til, at oplysninger om borgerne behandles forsvarligt. Denne tillid bygger blandt andet på gode erfaringer. I Danmark har man ikke oplevet, at der er sket alvorlige krænkelse af borgernes rettigheder. Men det er vigtigt at sikre, at der er grænser for statens magtudøvelse, så der ikke i fremtiden kan ske overgreb, hvis en folkestemning vender. Borgernes tillid er også en naturlig spejling af tilliden den anden vej, fra staten til borgerne. I Danmark er der tradition for, at staten ikke går borgerne for nær. Når man som borger føler sig gået for nært eller begrænset i sin mulighed for at agere frit, vil tilliden og den positive opfattelse af staten automatisk lide et knæk.

Som det fremgår, har de nævnte forslag alvorlige konsekvenser for borgernes privatliv og brug af Internet. Der er med andre ord gode grunde til at tænke sig alvorligt om, før man indfører øget overvågning.

---