# Overvågning

**Resumé og redigeret udskrift af høring**
**i Folketinget den 24. oktober 2001**

**Teknologirådets rapporter 2001/8**

**Overvågning**
Resumé og redigeret udskrift af høring
i Folketinget den 24. oktober

**Projektledelse i**
**Teknologirådets sekretariat**
Morten Jastrup

Projektmedarbejder:
Bjørn Bedsted

Projektsekretær:
Marian Schrøder

**Resumé og redigeret udskrift**
Thomas Dinesen
Journalistbureauet Ex-press

**Omslag**
Bysted HQ A/S

**Tryk**
Folketingets Trykkeri

**ISBN**: 87-90221-61-3
**ISSN**: 1395-7392

**Rapporten bestilles hos**
Teknologirådet
Antonigade 4
1106 København K
Telefon 33 32 05 03
Fax 33 91 05 90
tekno@tekno.dk

Rapporten findes også på Teknologirådets
hjemmeside www.tekno.dk

**Teknologirådets rapporter 2001/8**

# Forord

Denne rapport er en redigeret udskrift af en åben høring om overvågning, som blev afholdt på Christiansborg den 24. oktober 2001. Høringen blev afholdt af Teknologirådet for Folketingets Retsudvalg og Forskningsudvalg.

Høringen havde baggrund i arbejdet med loven om masteoplysninger. På den baggrund ønskede de ovennævnte folketingsudvalg en grundig gennemgang af problematikkerne vedrørende overvågning.

Formålet med høringen var derfor at afklare problemstillingerne omkring overvågning og identificere de områder, hvor der er mest grund til politisk bevågenhed.

Udvalgene valgte i forarbejdet til høringen at nedprioritere fokus på begivenhederne den 11. september. Udvalgene ønskede at vente med denne diskussion til man havde set regeringens udspil til en terrorpakke. Derfor valgte man at fastholde den oprindelige – brede – fokus på høringen.

Denne rapport indledes med et resumé, som giver læseren mulighed for at orientere sig i nogle af de centrale spørgsmål, der blev diskuteret på høringen. Udskriften fra høringen er opdelt i afsnit svarende til emneopdelingen i høringens program. Afsnittene indledes med oplægsholdernes mundtlige indlæg fulgt af en spørge- og debatrunde med Folketingets Sundhedsudvalg og Socialudvalg. Oplægsholdernes skriftlige indlæg er trykt senere i rapporten.

Denne høringsrapport kan ses på – og hentes fra – Teknologirådets hjemmeside, www.tekno.dk. Den kan også bestilles i Teknologirådet.

Teknologirådet vil gerne benytte lejligheden til at takke høringens oplægsholdere, der bidrog væsentligt til debatten, samt Folketingets Udvalgsafdeling og administration.

Endelig skal der lyde en særlig tak til baggrundsgruppen, der har bistået Teknologirådet i planlægningen af høringen. Baggrundsgruppen består af:

Professor Peter Blume, Københavns Universitet
Steffen Stripp, PLS Rambøll
Arne Vedsted Gram, sekretariatschef, Det Kriminalpræventive Råd

Teknologirådet, november 2001
Morten Jastrup

# Indhold

# Resumé

*Udarbejdet af Thomas Dinesen, journalistbureauet Ex-press*

Overvågningen af og kontrollen med danskerne stiger i takt med at informations-teknologien giver øgede muligheder for upersonlig og teknologisk overvågning. Det var en af hovedpointerne på Teknologirådets høring om overvågning 24. oktober 2001. Høringen foregik i Landstingssalen på Christiansborg og var bestilt af Folketingets Retsudvalg og Forskningsudvalg.
Og overvågning kan desværre tit, fremhævede prof., dr.jur. Peter Blume på høringen, blive et slags universalmiddel, man griber til i mange forskellige situationer, i stedet for at forsøge at løse det oprindelige problem. Men når man diskuterer overvågning er det grundlæggende demokratiske værdier og menneskerettigheder, som kommer på spil, og regler om overvågning bør derfor gennemføres med omtanke, påpegede Peter Blume.

Han pegede ligesom flere andre fra panelet på, at der i dag ikke er nogen, der har overblik over udviklingen i - eller omfanget af - overvågningen. Han opfordrede derfor Folketinget til at sænke tempoet på nye lovgivningsinitiativer og forsøge at få et sådant overblik.

Kultursociolog og forskningslektor Kim Rasmussen pegede i samme forbindelse på, at der, i betragtning af, hvor hurtigt og omfattende fænomenet er blevet udbredt, er forsket meget lidt i konsekvenserne af overvågning. Vi ved med andre ord ikke meget om, hvordan mennesker, reagerer på at blive overvåget. Debatten halter bagefter udviklingen, sagde Kim Rasmussen.
Han påpegede, at når der er en, der overvåger, og en der bliver overvåget, har overvågeren en magt, som den overvågede ikke har. Der vil knytte sig overvågnings-aspekter til mange teknologiske udviklinger fremover. Derfor er det nødvendigt, at snakke konkret om, hvad det er for en type overvågning, hvilken teknologi, og hvilke konsekvenser den har.

En af problemstillingerne drejede sig i den forbindelse om, hvorvidt overvågningen var frivillig, eller påtvungen, mente Kim Rasmussen. Hvor overvågningen foregår automatisk, anonymt og påtvunget vil overvågningen ofte afføde usikkerhed, ubehag og ubesvarede spørgsmål, og store dele af befolkningen oplever i dag, at der er en de ikke informeres godt nok om, at de bliver overvåget, påpegede han.

Per Helge Sørensen, der er forfatter og medlem af bestyrelsen i foreningen Digital Rights mente, at der var sket et skred mod øget overvågning, som ville fortsætte, hvis der ikke blev grebet ind, og at det har forrykket balancen mellem staten og borgeren. Ikke nok med, at mange nye teknologier i sig selv giver en mulighed for at overvåge folk mere. Der er også truffet politiske valg om at tilrette teknologien med henblik på overvågning, sagde han og fremhævede GSM-mobiltelefon-systemet som eksempel.

**Tv-overvågning og beskyttelse af persondata**
Et af de steder, hvor der er sket en kraftig stigning i overvågningen gennem de senere år er gennem tv-overvågning. Professor, dr.jur. Eva Smith, der er formand for Det Kriminalpræventive Råd pegede på, at tv-overvågning kan være et effektivt middel til at tilbyde tryghed for borgere og erhvervsliv. Men at det modstående hensyn er, at tv-overvågning kan medføre, at folk føler sig utrygge og krænkede.

Det Kriminalpræventive Råd har lavet en borgerundersøgelse om folks opfattelse af overvågning. Og de fleste af de adspurgte var positivt stemt over for overvågning i butikker, på tankstationer, banker, togstationer osv., men så snart man nærmede sig den private sfære, altså arbejdspladsen, eller tv-overvågning omkring den private bolig, var de derimod meget negativt stemt over for tv-overvågning, fortalte hun.

Finansrådet ønsker nu mulighed for at foretage udendørs tv-overvågning, fordi det vil forøge den vifte af passive sikringsforanstaltninger, som pengeinstitutterne gør brug af for at hindre røverier, fortalte kontorchef i Finansrådet, Niels Crone Lyngkjær. Grunden til, at Finansrådet gik efter at få udendørs overvågning skyldes, at en røver som regel ikke ifører sig maskering, før han indfinder sig foran et pengeinstitut, og at politiet med disse kameraovervågninger også ville få bedre bevisbyrder, forklarede han.

Eva Smith medgav, at der var noget om, at det kunne lige meget med tv-kameraet, når en bankrøver maskerede sig. Hun var dog ikke sikker på, at forslaget ville være så effektivt, som Finansrådet fremførte, og pegede på, at en røver f.eks. kunne skjule sig bag en paraply, indtil vedkommende tog masken på. Hun var desuden bekymret for, at det kunne udvikle sig til en glidebane, hvis der blev åbnet op for, hvor det var tilladt at videoovervåge, og mente man skulle sætte en grænse et sted.
Desuden kunne det have den effekt, at det måske snarere ville udvikle sig voldeligt, hvis folk havde en maske på. Hun mente desuden, at der ligger en stor udfordring for lovgivningssystemet til at forsøge at løse dilemmaet mellem tryghed og kontrol.

Peter Blume fandt ikke, at loven om tv-overvågning var imponerende og nævnte, at loven af mange kritiseres for at være utilstrækkelig, og måske også har et uklart forhold til EU's direktiv om beskyttelse af personoplysninger og den persondatalov, som Folketinget vedtog for et par år siden. Hvis tv-overvågning kan identificere de pågældende personer, er det en indsamling af oplysninger, og det udløser nogle skiltningskrav, som i dag ikke er opfyldt. I virkeligheden skulle der således sidde et skilt, der forklarede, hvem det var, der overvågede, og hvad formålet var. Dette var vigtigt, når det gjaldt spørgsmålet om, hvorvidt der var adgang til at opbevare oplysningerne bagefter, påpegede han.

**Også børn bliver overvåget**
I visse børneinstitutioner og skoler anbringes der nu web-kameraer, hvor forældre kan klikke sig ind efter behov, fortalte kultursociolog og forskningslektor Kim

Rasmussen. Og hvis der udvikler sig en tendens til, at der skal være video-overvågning i børneinstitutioner, er det et etisk problem, påpegede han; for har ikke også børn ret til privathed og frihed, når de var i institution?, spurgte han. Kim Rasmussen tilføjede, at spørgsmålet i den forbindelse var, om særlige grupper i samfundet skulle have særlige rettigheder, der kan beskytte dem mod overvågning.

Anne-Sofie Dideriksen, der er medlem af Teknologirådets Borgerpanel om overvågning, fortalte, at borgerpanelet konkret havde anbefalet, at der bliver lovgivet på dette område, fordi der ikke er nogen lovgivning, der specielt tog hensyn til børns rettigheder. Panelet anbefalede derfor, at børn skulle kunne beskyttes mod en overvågning, der ofte kun opfylder de voksnes behov for kontrol, sagde hun.

Eva Smith udtrykte i den forbindelse bekymring for, at der kan blive mindre kvalificeret samvær mellem børn og forældre, hvis videoovervågningen i børne-institutioner bliver mere udbredt, fordi forældrene så ville føle, at de vidste alt om, hvad der var foregået med børnene i løbet af dagen.

Birgitte Kofod Olsen, der er seniorforsker på Det Danske Center for Menneske-rettigheder, mente at der i Danmark var et klart behov for at se på, hvordan FN's børnekonvention også på dette område bliver implementeret. Der er behov for klarere regler for, hvordan vi behandler børnene og varetager deres rettigheder.

**Skjult overvågning af ansatte**

Overvågning breder sig også på de danske arbejdspladser med flere forskellige formål. Arbejdsgivere kan have et behov for at sikre, at de mennesker, de betaler for at udføre et stykke arbejde, reelt også gør det. Butiksindehavere kan have et ønske om at afsløre butikstyve – også blandt personalet. Og overvågning kan være med til at øge sikkerheden mod røverier. Skyggesiden ved denne overvågning er, at overvågningen typisk indebærer en indskrænkning i privatlivets fred, og kan medføre en krænkelse af den enkelte borgers og den enkelte ansattes personlige integritet, sagde Peter Blume om den overvågning, der foregår på arbejdsmarkedet.

Faglig sekretær i HK-handel Bjarne Petersen, fortalte at man i butikkerne ikke længere nøjes med at beskytte de ansatte med tv-overvågning, men også systematisk tv-overvåger og aflytter medarbejderne. En leverandør af overvågningsudstyr havde således solgt tv-overvågningsudstyr med indbyggede mikrofoner, til samtlige bagerbutikker. Han nævnte desuden et eksempel fra en butik fra Nørrebro i København, hvor de ansatte selv bad ledelsen om tv-overvågning for at stoppe tyverierne – og endte med selv at blive udsat for skjult tv-overvågning, bl.a. fra et kamera der sad i et rør, og var rettet mod det sted, hvor de ansatte klædte om.

Sektionschef i Dansk Handel og Service Laurits Rønn, fremførte at han ikke kunne nikke genkendende til eksemplet, men erkendte, at der var i strid med loven hvis en virksomhed ikke skiltede med at der var tv-overvågning. Han medgav, at

lydoptagelser som udgangspunkt var ulovligt, men at han ikke havde mødt en eneste sag i sin tid i Dansk Handel og Service. Laurits Rønn mente endvidere, at virksomhederne var meget seriøse, når de opstillede overvågningskameraerne, og skiltede med det. Han mente desuden, at butikkerne skulle have adgang til at opstille kameraer, hvis de havde en konkret mistanke om medarbejdertyveri, og der var skiltning.

Advokat og næstformand for Datarådet Janne Glæsel undrede sig over, at der ikke havde været nogle sager i Registertilsynet og Datatilsynet for nylig omkring den slags forhold, når det lod til, at en del af den videoovervågning, der foregik, var ulovlig og var på kanten af det, som de lovgivningsmæssige rammer opstiller.

Til det sagde Bjarne Petersen, at de ansatte, der havde været udsat for skjult overvågning, måske nok ville anmelde og fortælle om det, men ikke havde lyst til at gå videre i en efterforskning, fordi de følte sig så krænket, at de ikke havde overskud til at gå videre.

Anne-Sofie Dideriksen fra Teknologirådets Borgerpanel om overvågning sagde, at panelet havde anbefalet, at arbejdsmarkedets parter udarbejder et sæt regler for indførelse og regulering af elektronisk overvågning, som ophæves til lov af Folketinget. Desuden anbefalede panelet, at medarbejderindflydelsen skal prioriteres, og at der skal herske åbenhed og klare retningslinjer på den enkelte arbejdsplads.

Janne Glæsel mente dog, at området var tilpas reguleret, dels med persondataloven, tv-overvågningsloven, straffeloven, hovedaftalen, skærmbekendtgørelsen, og ved lov om helbredsoplysninger og diskriminationslove, hvor de mere arbejdsrelaterede forhold også er reguleret.

Hun mente endvidere ikke, der var den store uklarhed mellem tv-overvågningsloven, som regulerer adgangen til at foretage overvågning, og persondataloven som regulerer, hvordan og til hvilket formål man må bruge optagelserne. Hvis man kan identificere en person via en tv-overvågning er det omfattet af persondataloven, og så skal såvel de generelle som de specielle regler i persondataloven, være opfyldt. Der skal være et klart formål, og man må ikke opbevare det længere end hensynet nødvendiggør, påpegede Janne Glæsel.

Det ligger også fast, at overvågning, herunder logning og kontrol af medarbejderes brug af e-mail og Internet, skal være sagligt, og skal ske ud fra hensyn til virksomhedens drift og sikkerhed og internt fastsatte regler fra virksomheden. Desuden skal medarbejderne have en klar og entydig information om disse politikker omkring tv-overvågning, Internetovervågning og overvågning af e-mails, sagde hun.

**Overvågning af Internet og e-mails breder sig på arbejdsmarkedet**
Overvågning på arbejdspladsen er et eksempel på, at overvågning bruges til at løse et problem, der egentlig bunder et helt andet sted, fremførte Peter Christensen fra Co-operative Network and Data Operation. I stedet for, at arbejdslederen går hen og sørger for, at en medarbejder er beskæftiget i sin arbejdstid, så laver man i stedet overvågning for at se, hvem der gør det ene og det andet. Og det betyder, at det bliver brugt imod alle mulige, og at overvågning i dag bliver brugt som en form for kollektiv afstraffelse, var hans pointe.
Han mente desuden, at det var et problem, når tekniske elementer blev vendt til overvågning på arbejdsmarkedet. For at holde det teknologiske samfund oppe at køre, er vi tvunget til at registrere en masse omkring vores systemer, bl.a. en masse logs, som også indeholder nogle elementer af persondata. Det betyder, at en arbejdsgiver f.eks. kan sammenholde flere af den type logs eller scanne et bestemt log og udlede en bestemt profil af sine ansatte, sagde han.

Per Helge Sørensen fra Digital Rights fremførte, at selv om man gemmer e-mails af sikkerhedsmæssige årsager og i princippet kan gå ind og se, hvor mange der henholdsvis er private og faglige, skulle man måske lade være, og i stedet vurdere de ansatte på, hvad de havde præsteret, eller hvordan man opfattede dem i det daglige. Og tilsvarende, hvis de ansatte gik ind på lidt mange sportssider under Tour de France, skulle man måske ikke undersøge det gennem kontrol, men i stedet snakke med de ansatte om, hvad der var rimeligt, og hvor meget man kunne tillade at produktiviteten af den grund faldt i juni, mente han.

Janne Glæsel sagde, at hun kunne forestille sig, at mange virksomheder var tilbageholdende med at tildele både officielle og private e-mailadresser, fordi det måske kunne være vanskeligt at skelne mellem, hvad der var privat, og hvad der var virksomhedsrelateret. Hun tilføjede, at straffeloven og brevhemmeligheden klart siger, at man ikke må bryde post, herunder e-mails, som har privat karakter. Men at der er virksomheder, som definerer al post, også det, der står privat på, som virksomhedsrelateret ud fra driftsmæssige hensyn eller sikkerhedsmæssige hensyn, hvor det så også er kommunikeret klart ud til virksomheden, sagde hun.

Laurits Rønn fortalte, at man i Dansk Handel og Service anser e-mails som almindelig post, og at virksomhederne har behov for at kunne se e-mails, hvis man kommunikerer med andre virksomheder via e-mail. Men at man også følger den praksis, Datatilsynet har tilkendegivet, og ikke åbner posten, hvis der står privat på en e-mail.

Han tilføjede at det desuden var vigtigt, at medarbejderne fik at vide, hvad virksomheden kontrollerede i forbindelse med medarbejdernes brug af Internettet, og hvad de f.eks. måtte logge ned. Det er helt afgørende, at man har nogle retningslinjer, som overholder lovgivningen, ligesom der er nogle etiske regler at tage hensyn til, og

både medarbejderen og virksomheden er interesseret i at man har en politik og en åbenhed på området, mente han.

**Fyret for vittighed om chef**
Professor, dr.jur. Peter Blume nævnte, at der havde været eksempler på, at ansatte var blevet fyret på grund af en vittighed om chefen, som følge af, at der havde været overvågning af korridorsnakken på den interne anvendelse af Internettet i virksomheden. Det er en sådan øget overvågning, som gør en regulering nødvendig, mente han.

Det drejer sig om grundlæggende værdier som privatlivets fred, og personlig integritet på arbejdsmarkedet. Derfor er det en lovgivningsopgave og ikke en aftaleopgave. Hvis man ønsker at lave mere præcise retningslinjer, og måske, som nogle gør, finder, at det Datatilsynet er nået frem til, er for arbejdsgivervenligt, så ender aben tilbage på politikernes bord, fremførte han.

Peter Blume fandt også, at de offentlige myndigheders stigende brug af overvågning var betænkelig. Det er et grundlæggende etisk problem, at borgeren bliver alt for synlig, i forholdet mellem stat og borger, og at borgerens frihedsrum, hvor vi er os selv, bliver mindre og mindre, fremførte han.

Som eksempler nævnte han, at offentlige myndigheder prøvede at pålægge hjemmehjælpere informationspligt over for kommunen, når de gik ind i folks private hjem, og de udvidede muligheder, som kommunerne har fået for at samkøre registre, f.eks. med henblik på at afsløre socialt bedrageri. Disse regler har medført, at borgeren er blevet endnu mere "informations-nøgen" i samfundet, end vedkommende var før, fremførte han.

Peter Blume medgav, at det måske havde en præventiv effekt når nogen blev fanget i systemet, men tilføjede, at det i virkeligheden var meget få, der blev fanget, og at politiet og anklagemyndigheden i disse sager tit var nået frem til, at der ikke var grundlag for en straffesag. Han opfordrede derfor myndigheder til i stedet, at gøre noget ved de årsager, der frister folk til, at prøve at skaffe sig lidt flere offentlige ydelser, end de var berettiget til.

Eva Smith mente generelt, at den kriminalitet, man ønsker at opklare, skal være meget alvorlig, før man skal komme med et indgreb over for en hel gruppe, der ikke er nogen som helst mistanke imod. Man går ind i deres intimsfære, og så bliver det betænkeligt, hvis folk ikke er mistænkte, sagde hun.

**Kommunikationsteknologi skal give mulighed for overvågning**
Per Helge Sørensen fremførte, at der i dag bliver registreret en masse oplysninger, som bliver brugt i forbindelse med efterforskning af kriminalitet. Det giver i sig selv

en øget overvågningsmulighed og forrykker balancen mellem staten på den ene side og borgeren på den anden side.

Men man kan også lade være med at give efter for et ønske om at mindske barriererne for at benytte de efterforskningsmidler, som den elektroniske overvågning giver mulighed for. Teknologien vil blive mere og mere præcis, mobiltelefoner vil kunne give oplysninger om positioner helt ned til fem til tre meters nøjagtighed, og vi vil bruge Internettet mere og mere, så skredet vil fortsætte, hvis der ikke bliver grebet ind, tilføjede han.

Per Helge Sørensen fremførte i den forbindelse, at der ikke kunne herske tvivl om, at der blev skabt utrolig mange data via mobiltelefoner i masterne rundt omkring, og at det tilsyneladende ikke har været noget problem at finde de data, der tilhører Kurt Thorsen eller Rasmus Trads, og bruge dem i forbindelse med efterforskningen af sagen. Man må konstatere, at de data der ikke fandtes for 10 år siden, nu bliver brugt, og det samme ser vi på en række andre teknologiske områder, sagde han

Når vi får en øget overvågning, og f.eks. Internettet bliver tilrettet med krav om at lagre oplysninger tilbage i tiden, så er det fordi man ønsker, at den overvågnings-mulighed skal være til stede. Det er nemlig eksplicit besluttet, bl.a. ved at efterretningstjenesterne og politiet deltager i standardiseringsarbejdet, at vores kommunikationsteknologier bliver anderledes indrettet, sagde Per Helge Sørensen.

**Elektronisk overvågning ikke nok til at afsløre børneporno**
Troels Ørting Jørgensen er vicekriminalinspektør i Rigspolitiets afdeling A, og den enhed han er chef for, har ansvaret for bekæmpelse af IT-kriminalitet. Han fortalte, at politiet stort set ikke bruger elektronisk overvågning i deres arbejde på Internettet, og at de i hans afdeling ikke overvåger Internettet for kriminalitet, men at de til gengæld har 70 pct. af befolkningen, til at gøre arbejdet for dem.

Politiet får hvert år et sted mellem 4.000 til 6.000 anmeldelser om IT-kriminalitet, der bl.a. handler og racisme, trusler, børneporno eller andre former for kriminalitet. I de fleste efterforskninger af IT-kriminalitet er politiet fuldstændig afhængig af, at der er logning, for at de kan komme videre. Logning er registrering af trafikken på internettet. Politiet er således nødt til at have et trafik- eller transaktionsspor, der kan lede dem hen til den computer eller server, hvorfra kriminaliteten er blevet begået, fremførte han.

Og i øjeblikket står det temmelig skralt til omkring logningsprocedurerne, mente Troels Ørting Jørgensen. Som eksempel nævnte han, at ISP'erne (”Internet service provider”, de firmaer, der sælger og formidler adgang til internettet) ikke er regulerede. Der kræves ingen autorisation for at starte en ISP-virksomhed. Det krævede blot, at man købte tre servere og noget kabelkapacitet, sagde han. Det

betyder, at organiserede forbrydere kan lave deres egen ISP og bruge internettet uden at politiet har mulighed for at komme til oplysningerne fra en log.

Inden Troels Ørting Jørgensen var gået til høringen i Folketinget havde der på hans bord ligget nogle børnepornobilleder af blebørn, der blev voldtaget. Det var formentligt digitale billeder, og de var uploadet klokken 04.49 fra en provinsby i Danmark til en mailserver i en folder, fortalte han.

Men på grund af, at man dels havde brugt et bestemt selskab, som kun logger IP-nummeret, når man opretter sin konto og så ikke siden, og fordi man gemmer sig bag en router, var det, med den eksisterende lovgivning, ikke muligt for politiet at opklare denne sag, selv om man kunne lokalisere den til en sjællandsk provinsby, sagde han.

**Nemmest at fange de dumme kriminelle**

Per Helge Sørensen fra Digital Rights havde dog ikke tiltro til, at man ville komme ret mange vegne ved at indføre en autorisationsordning af ISP`er. Man ville desværre nok heller ikke komme den mest alvorlige kriminalitet til livs, uanset om man lavede en autorisationsordning eller indførte et lovkrav om logning for ISP'erne. Fordi de alvorligt kriminelle vil vide, hvordan man laver sin egen ISP eller kobler sig på via et trådløst netværk. Så vi er i den sædvanlige situation, at vi kan fange de halvalvorlige og de smådumme, men de allermest alvorlige, f.eks. terroristerne, får vi nok ikke på den konto, mente han.

Vicekriminalinspektør Troels Ørting Jørgensen medgav, at hvis man kiggede på kriminaliteten generelt, så var det altid nemmest at fange de dummeste, og at det var det, politiet ofte var bedst til. Produktudviklingen og sofistikeringen inden for kriminaliteten, hvor man udgiver sig for at være en anden, gør også, at det næsten er umuligt, forklarede han.

Kultursociolog og forskningslektor Kim Rasmussen fortalte, at der er forsket meget lidt i overvågningskonsekvenser, og om overvågning får folk til at ændre adfærd. Men der er masser af eksempler på, at de kriminelle tager deres forholdsregler, og at overvågning ikke afholder dem fra at foretage sig det som de gør, påpegede han.

**Efterretningstjenesten omfattet af retsplejeloven**

Politiets Efterretningstjeneste interesserer sig ikke for overvågning, men interesserer sig for at have nogle rimelige efterforskningsmuligheder, svarende til den teknik, eller den teknologi, som de kriminelle bruger, sagde Jørn Bro, der er politimester i Glostrup, og tidligere souschef i Politiets Efterretnings Tjeneste. Og de er hele tiden et pænt stykke foran os, vi halser bagefter. Og det er det, der i virkeligheden bekymrer os, forklarede han.

Han fremførte, at de to danske efterretningstjenester ikke beskæftiger sig med, at overvåge borgerne. Det har de hverken bemyndigelse eller ressourcer til. Det ville kræve helt andre rammer og regler, og et meget større personale. PET har til opgave at overvåge, forebygge, modvirke og forhindre foretagender og handlinger, der må antages at rumme en fare for rigets selvstændighed og sikkerhed og den lovlige samfundsorden. Man har nøjagtig de samme virkemidler som det øvrige politi, og det vil sige, at PET også er omfattet af retsplejeloven, sagde han.

Jørn Bro pegede i den forbindelse på bestemmelserne i retsplejelovens kapitel 71 og om indgreb i meddelelseshemmelighed og observation. Der er her mulighed for at indhente kendelser til aflytning af rum, telefoner og teleoplysninger samt til brevåbning og brevstandsning. Der er også fastsat regler for, hvis man skal observere inden for et område, der ikke er frit tilgængeligt og ved hjælp af særlige virkemidler, sagde han.

For at politiet og efterretningstjenesten kan gøre brug af disse muligheder kræver det en retskendelse, som skal hvile på nogle kvalificerede krav. Der stilles i retsplejeloven krav om, hvornår der kan opnås telefonaflytning, og de følges striks. Da telefonaflytning og efterfølgende bearbejdning af disse teleoplysninger er ressourcekrævende, gør politiet og PET, kun i meget begrænset omfang brug af disse virkemidler, og er nødt til at være yderst selektive for ikke at drukne i det rene pladder og vrøvl, sagde han.

Jørn Bro oplyste desuden, at de oplysninger, der indgår over en telefonaflytning, eller som skabes igennem anden efterforskning, vil stå skrevet op et stykke tid, indtil sagen er færdigbehandlet. Ellers vil det være meningsløst at indsamle oplysningerne, som han formulerede det.

PET's registre er fortegnelser over de personer og organisationer og emner, som forekommer i PET-sager. Tidsperspektivet er langt i den slags sager, og derfor er de undertiden mere omfattende end i andre sager, fremførte Jørn Bro. Man er i dag i stand til at håndtere og bearbejde og uddrage mere præcise oplysninger af et stort datamateriale, men PET er måske den politiafdeling i landet, der er mest kontrolleret og reguleret og bliver kigget mest i kortene, betonede han.

**Persondatalov gælder ikke for efterretningstjenester**

Professor, dr.jur. Peter Blume fremførte, at det var rigtigt, at retsplejeloven også gjaldt for PET, men at det samtidig var interessant at konstatere, at persondataloven f.eks. ikke gjaldt for PET eller FET, hvad den ellers godt kunne med visse modifikationer. For selv om PET måske ikke overvåger – hvad der på en måde er overraskende for nogle af os - så har de i hvert fald nogle registre og nogle oplysninger, som altså ikke er omfattet af den lovgivning, der specielt gælder for, hvordan man skal behandle personregistre, sagde han.

Birgitte Kofod Olsen, der er seniorforsker på Det Danske Center for Menneskerettigheder, fortalte, at Menneskerettighedsdomstolen i Strasbourg i en konkret sag fra Schweiz, hvor efterretningstjenesten var involveret, havde fastslået, at loven skal sikre, at borgeren beskyttes mod vilkårlige indgreb. Når man rejser spørgsmålet om vilkårlige indgreb i en efterretningsmæssig sammenhæng er det, fordi risikoen er særlig stor, fordi vi har et krav om hemmelighedsholdelse af nogle af de efterforskningsskridt, som efterretningstjenesten foretager, sagde hun.

Men på grund af den øgede risiko for vilkårlighed stiller man derfor ekstra strenge krav til beskyttelse af borgeren. Der er altså et generelt krav til lovgivningen, som danske politikere skal være opmærksomme på, når de vedtager en lovgivning, der giver adgang til overvågning. I den forbindelse skal menneskerettens krav om klarhed og præcision i lovhjemmelen samt det lovlige hensyn og nødvendigheden være til stede. Derudover skal man også være opmærksom på, at når den bestemmelse, man vedtager bliver anvendt af politi og efterretningstjeneste, skal de samme krav være opfyldt i den konkrete situation, påpegede Birgitte Kofod Olsen.

**Mangel på fornuftige løsninger til kryptering**

Peter Christensen fra Co-operative Network and Data Operation fremhævede, at der ikke var tvivl om, at den teknologiske udvikling gav mange muligheder for overvågning. Og når man blev overvåget, så fandt man måder at omgå det på, og det var vel det samme, der foregik, når vi enten brugte kryptering, eller forskellige andre måder til at omgå overvågning, også på nettet, sagde han.

Krypteringsværktøjer er et forsøg på at skjule den kommunikation, vi foretager frem og tilbage mellem to parter. I dag bruger man kryptering i almindelige samhandels-funktioner inden for Internettet, og til at skjule de meddelelser, som man ikke synes, at andre skal læse, fortalte Peter Christensen.

Hvis f.eks. en a-kasse i dag skal kommunikere med sine afdelinger rundt omkring i landet, vil man typisk bygge det, der hedder et VPN-net, hvor man krypterer en tunnel over Internettet, så andre på Internettet ikke kan aflæse, hvad der foregår. Det gør man af hensyn til medlemsoplysninger, og fordi det også er et krav fra myndighederne, sagde han.

Men når det handlede om den individuelle kryptering til almindelige mennesker, troede Peter Christensen, at der var et problem med udbredelsen, fordi der for brugerne var et vist problem, ved at bruge krypteringsværktøjer, og fordi der ikke altid var en forståelse for, hvorfor man skulle gøre det. I dag har man ikke de fornuftige løsninger til, at det bliver mere udbredt, og måske har folk heller ikke altid tillid til de værktøjer, der er. Måske var opgaven derfor, at stille bedre værktøjer til rådighed og måske gøre noget mere pædagogisk for at motivere folk til at bruge det, sagde Peter Christensen.

Peter Landrock der er professor og administrerende direktør i Cryptomathic forklarede, at man løser privates brug af kryptering ved hjælp af det, der hedder et certifikat, som knytter en bestemt person og vedkommendes e-mailadresse til den nøgle, man skal have fat i. Med sådan et certifikat, kan man uden særligt besvær kommunikere sammen og kryptere, sagde han.

Problemet var bare, tilføjede han, at den teknik, man benytter, er den såkaldte public-key teknik, hvor man har et par af nøglerne: En offentlig nøgle og en hemmelig nøgle. Og for at man kan modtage en krypteret information fra en anden person, skal vedkommende have fat i ens offentlige nøgle, ligesom hvis vedkommende skulle have fat i ens telefonnummer for at ringe. Vi har ikke den infrastruktur, der skal til, fordi vi mangler telefonbøgerne, som han formulerede det. Det svarede nærmest til, at folk skulle mødes og udveksle telefonnumre, hvis de ville telefonere til hinanden, fordi alle numrene var hemmelige, sagde Peter Landrock.

Hvis man interesserede sig for at give den enkelte borger adgang til kryptering, havde han derfor svært ved at forestille sig, at det ville blive videre udbredt, medmindre staten gik foran. Ellers ville det kun være noget man brugte i virksomheder, hvor man allerede bruger det mange steder. Det var med andre ord i stort omfang et spørgsmål om at lave det mere brugervenligt, og det koster penge. Hvis borgerne skulle have almindelig adgang til kryptering, var Peter Landrock derfor bange for, at staten blev nødt til at spille en aktiv rolle og måske bære nogle af udgifterne.

Per Helge Sørensen sagde, at udbredelsen af kryptering og digital signatur formentlig ville ske langsomt og gradvist i samfundet, og han mente, at prisen skulle betragtelig under nul, før man kunne få folk til at bruge digital signatur. De skal have noget for det, ligesom man, i overført betydning, får for at bruge sin homebanking, hvor man rent faktisk bruger kryptering, sagde han.

**Kryptering og kodebrydning**

Det ville i kommunikationen mellem almindelige mennesker være smart at bruge de samme krypteringsværktøjer, som man bruger i almindelig e-handel. Men der er et enkelt problem, og det er, at meget amerikansk software har en tendens til, at have forbindelser til den amerikanske efterretningstjeneste NSA, som gør, at man ikke altid kan være sikker på, hvad det er, der kommer ud af det, sagde Peter Christensen fra Co-operative Network and Data Operation.

Specielt meddelelser, der går via satellittransmission, og det er typisk over Atlanten, vil blive opsamlet, og man vil kunne mønstergenkende ting. Og det gør selvfølgelig, at man på europæisk plan burde overveje at lave sit eget system eller sine egne værktøjer, så man er sikker på, hvad man får ud af det, når man krypterer, sagde han.

Politimester og tidligere souschef i Politiets Efterretnings Tjeneste Jørn Bro fremhævede, at man siden Første Verdenskrig har arbejdet med problemet kode-brydning elektronisk, og troede derfor, at man skulle være varsom med at knytte alt for store forhåbninger til, at der findes krypteringsprogrammer, der ikke kan brydes. Det gav en falsk tryghed. De fleste brevkoder ville formentlig i dag kunne knækkes på et par timer. Det er muligt, at det vil tage lidt længere tid, hvis den var online, men det finder man ud af på en eller anden måde, sagde han.

Jørn Bro tilføjede, at der måske var et klart behov hos store statsforetagender, regeringen og store firmaer for at kunne kode deres kommunikation. Men for landets private borgere og for almindelige firmaer mente han ikke der var et nævneværdigt behov for at kunne foretage kodning, også fordi de kun ville være i stand til at kunne lave kodning, der kunne knækkes, hvis det var det, man ønskede. Det ville kun gøre opklaringsarbejdet vanskeligere, påpegede Jørn Bro.

**Uanede muligheder for aflytning**

Per Helge Sørensen var uenig i, at almindelige borgere ikke havde behov for at kryptere, og mente at netop almindelige borgerne var nogle af dem, der krypterede mest for tiden, når de brugte deres homebanking system, hvor der er et tydeligt behov for at beskytte informationerne. Han var desuden ikke i tvivl om, at man ville se mere og mere kryptering, fordi der er behov for at beskytte kommunikationen efterhånden, som brugen af Internettet bliver mere udbredt, og hvor folk de kommende år f.eks. vil kommunikerer med deres læge eller psykolog.

Til det svarede Jørn Bro, at man i mange år har kunne foretage telefonaflytning af folks samtaler med deres læge og psykolog og bank, hvis det var det, man ville og havde hjemmel til. Han mente derfor, at det var svært at se hvad almindelige mennesker, i det danske samfund, som det så ud i dag, skulle havde brug for af koder, scrambling, kryptering osv. Jørn Bro havde samtidig den opfattelse, at det rummede en falsk sikkerhed, og at det, der i virkeligheden var farligt, var at man bildte folk ind, at der kunne skabes en masse sikker kommunikation, sagde han.

Den bedste beskyttelse er trods alt omtanke, for der lyttes, hvad enten vi kan lide det eller ej, og det meste der bliver aflyttet, ryger ned i den store brokkasse, fordi det er uinteressant. Men der filtreres visse oplysninger ud, og det er meget svært at sige, hvor det som anvendes efterretningsmæssigt ligger henne. Han opfordrede derfor folk til at lade være med at tro, at man kunne skabe et eller andet sikkert rum, hvor man kunne plapre fuldstændig uhæmmet, skriftligt eller mundtligt, som han formulerede det.

Jørn Bro fortalte endvidere, at hvad der råbes ud i verdensrummet over mobil-telefoner og lignende, generelt bliver aflyttet masser af steder. Han troede ikke rigtigt, at det kunne forebygges, for hvis man fandt en kode, så kunne den knækkes, hvilket masser af lande havde arbejdet med siden Første Verdenskrig. Det gav med

andre ord en falsk tryghed, og 99,99 pct. af befolkningen kunne i virkeligheden være ligeglade med, om nogen lyttede. Derimod burde beslutningstagerne måske være en smule forsigtigere med, hvad de råbte ud over mobiltelefonerne i et lidt for klart sprog, advarede han.

**Politiet nervøse for kryptering**

Per Helge Sørensen mente ikke, at man kunne lave en sammenligning mellem, at snakke i telefon med sin bank, og at lave homebanking uden kryptering, fordi trusselsbilledet er et andet på Internettet. De ting, vi foretager os på Internettet, er nogle helt andre end det, vi snakker i telefon om, og det er derfor, at bankerne har lavet kryptering i deres homebanking system. Ligesom Datatilsynet stiller krav om, at kommunikation er krypteret, hvis der skal overføres et CPR. nr., fremførte han.

Per Helge Sørensen påpegede desuden, at der i dag findes software, som krypterer så godt, at det er utrolig vanskeligt at bryde koderne. På Forskningsministeriets hjemmeside om kryptering, ligger der således tre rapporter, hvor disse forhold bliver diskuteret, og hvad mulighederne er for at forbyde eller bremse det, fortalte han.

Og en af de ting, som var meget klart, var, at efterforskningsmyndighederne både i Danmark og i USA var ret bekymrede for kryptering, og at man ønskede at tilrette teknologien, så man sikrede en aflytningsmulighed. Det viser, at det er ikke rigtigt at sige, at politiet altid vil kunne finde en måde af aflytte folk, hvis de krypterer. Det mente folk i hvert fald ikke, dengang vi diskuterede kryptering. De var faktisk bekymrede over, at de moderne krypteringssystemer ikke kunne aflyttes, sagde Per Helge Sørensen.

Peter Christensen tilføjede, at den krypteringsform, som generelt anvendes af private i dag, under alle omstændigheder kan forsinke og måske helt afvise en dekryptering. Og fordi det ofte er »real time«, der er interessant vil forsinkelsen i sig selv betyde, at man ikke får noget ud af det. Og så er der også den kryptering, som med de maskiner, vi har i dag, ikke kan knækkes, sagde han. Også professor, og administrerende direktør  Cryptomathic Peter Landrock fortalte, at der efter hans ekspertvurdering, i dag findes masser af praktisk ubrydelige koder.

Vicekriminalinspektør Troels Ørting Jørgensen fremførte i forbindelse med krypteringsdebatten, at man - i hvert fald i den åbne del af politiet - var meget bekymrede for kryptering. Faktisk var man så bekymrede, at man var meget opsatte på, at der lovgivningsmæssigt blev taget højde for, at der kunne skaffes nøgler til kryptering. Når vi bare er oppe over 256 bite kryptering, så er vi jo på den, sagde han.

Det vil sige, at man kan kommunikere og gøre det vanskeligt, for ikke at sige umuligt, for politiet, at se det. Hvis man ikke på en eller anden måde kan dekryptere kommunikationen, så skal politiet i hvert fald efter rettens kendelse tillægges andre

metoder for at kompensere for den manglende mulighed for indgriben i kommunikationen, mente Troels Ørting Jørgensen

**Generationer og overvågning**

Der blev også rejst spørgsmål, om hvorvidt de unge generelt havde et mere afslappet forhold til overvågning, eller om det kun var på nogle områder. Professor, dr.jur. Peter Blume mente, at det måske var rigtigt, at børn og unge var vokset op i en anden teknologisk virkelighed, end de voksne, og at de måske ville vænne sig til at opfatte visse former for det, vi kaldte overvågning, som helt naturligt. Han troede imidlertid, at det helt afhang af, hvad overvågningens formål var, og hvem det var der overvågede, og mente ikke, at de unge f.eks. havde et afslappet forhold til offentlige myndigheders overvågning, mens de måske havde et mere afslappet forhold til brug af f.eks. dankortet og Internettet.

Kultursociolog og forskningslektor, Kim Rasmussen fremførte, at der nok er en generationsforskel i forhold til måden at omgås teknologi på. Og det hang for ham at se, delvist sammen med, om man oplevede, at noget var selvfølgeligt, fordi det havde eksisteret hele ens liv, eller om man oplevede, at noget udgjorde en ændring. Det skabte selvfølgelig nogle forskelle, men rent forskningsmæssigt vidste vi meget lidt om det, sagde han.

Per Helge Sørensen fra Digital Rights mente, at der var stor forskel mellem den selvvalgte overvågning, som det, der sker i tv-programmet »Big Brother«, hvor nogen sælger deres privatliv for at opnå status og blive set af samfundet, og så den overvågning, man ikke kunne vælge fra. Der var nogle ting, hvor der var noget på spil, og andre ting, hvor man ikke synes, der var noget på spil. Han var af den overbevisning, at alle mennesker havde et sted, hvor der var noget på spil, og var sikker på, at der også var noget på spil i forholdet mellem unge og deres forældre eller andre autoriteter, og at de unge ikke bare ville lade overvågningen få frit løb.

**Overblik og kvalitet i lovgivningen**

Medlem af Teknologirådets Borgerpanel om overvågning Anne-Sofie Dideriksen, fortalte, at borgerpanelet havde vurderet, at den rivende teknologiske udvikling medførte et behov for en særdeles tæt opdækning af lovgivning og retssikkerhed. Panelet anbefalede i den forbindelse, at der til stadighed bør holdes øje med person-dataloven, og andre love vedrørende overvågning, og at loven bliver revideret, så den kan blive ved med at beskytte den enkelte borgers kontrol over sine persondata, sagde hun.

Når det bliver sagt, at det teknologisk iler så stærkt, at en lovgivning er forældet fra det tidspunkt, hvor den træder i kraft, så bør man måske finde et samspil mellem nogle grundlæggende standarder i lovgivningen og noget mere aftalemæssigt, sagde formanden for Advokatrådet Jon Stokholm. Han mente endvidere, at revisions-bestemmelser, på det her område, ville være en god ting, og at man følger den

lovgivning, man end går ind og laver, hurtigt op, og ser hvordan den lov om overvågning så fungerer, sagde han.

I forbindelse med Folketingets indsats i forbindelse med overvågning fremførte Jon Stokholm desuden, at der var behov for kvalitet i lovtilblivelsen og for at undgå hurtige løsninger. De lovgivningsinitiativer, der eventuelt skulle tages, burde desuden tages i en bred offentlig debat. Og den lovgivning, som man i givet fald havde, skulle have en bred accept af dem, den rettede sig til. Hvis den ikke havde det, havde den sådan set ingen mening, mente han

Professor, dr.jur. Peter Blume, ville ikke ligefrem anbefale en lovpause, men foreslog, at man måske sænkede tempoet lidt, og fik nogle eksperter til at prøve, at tage temperaturen generelt på overvågningssituationen i lovgivningen i dag. At man med andre ord prøvede at få et overblik, for det var det man ikke havde i dag, og det troede han heller ikke, der var nogen af eksperterne, som havde, sagde han.

# Folketingets spørgepanel

Folketingets spørgepanel er sammensat af repræsentanter for Folketingets partier fra udvalgene, der har taget initiativ til høringen. I dette tilfælde Folketingets Retsudvalg og Folketingets Forskningsudvalg.

Spørgepanelet er i centrum for høringen og fungerer som udspørgere af de indbudte eksperter.

Spørgepanelet ved høringen bestod af:

S: Sandy Brinck / Thomas Adelskov
V: Kristian Jensen
KF: Helge Adam Møller
SF: Knud Erik Hansen
CD: Sonja Albrink
RV: Elisabeth Arnold
EL: Søren Søndergaard
KRF: Tove Videbæk

Ordstyrere:
Lissa Mathiasen (S), Formand for Folketingets Retsudvalg.
Hanne Severinsen (V), Formand for Folketingets Forskningsudvalg.

# Redigeret udskrift af høringen

*Udarbejdet af Thomas Dinesen, journalistbureauet Ex-press*

## Indledning

**Ordstyrer**, **Lissa Mathiasen** (S), formand for Folketingets Retsudvalg:
Jeg vil på vegne af både Forskningsudvalget og Retsudvalget byde velkommen til alle til høringen her. Og i den forbindelse skal en særlig velkomst lyde til vores ekspertpanel. Jeg vil godt sige jer tak for, at I så beredvilligt har villet stille op her i dag. Jeg skal ikke lægge skjul på, at vi ønsker at gøre brug af jeres viden. Vores håb er, at I vil være vores sparringspartnere her, for at vi kan drage nytte af det her i dag.

Emnet overvågning er stort. Det er svært og uoverskueligt. Vi må jo erkende, at overvågningen breder sig i vores hverdag. Nogle gange, fordi vi selv vælger det. Men andre gange har den almindelige borger ingen indflydelse. Men én ting er sikkert: Folketinget og vi som politikere har ansvaret for, at borgernes retssikkerhed ikke krænkes af overvågning. Og det er også grunden til, at vi har ønsket at tage diskussionen op her i dag.

Jeg er jo så nødt til at sige, at det er ikke en traditionel høring. Høringen er et arrangement for folketingsudvalgene og eksperterne. Vi får lov til at være tilhørere og tilskuere. Og som I kan se af programmet, så er det opdelt i fem blokke. Og hvis vi skal nå godt igennem det til den fastsatte tid, og det skal vi, ja så kræver det i høj grad selvjustits. Også til vores oplægsholdere. I har maksimum 5 minutter til jeres rådighed.

Jeg vil lige give jer et lille praj, når der er 1 minut tilbage. Jeg håber, at I vil have forståelse for, at jeg også med lidt hård hånd vil håndhæve det. Derfor skal jeg heller ikke være tidsrøveren her og sige meget mere på nuværende tidspunkt andet end en lillebitte smule praktisk. Jeg skal bede de tre første oplægsholdere om at komme herop og tage plads.

Og så skal jeg bede om, at alle, når man tager ordet, husker at aktivere den grønne knap, sådan så vi også har mulighed for at høre, hvad det er, I siger. Og så er jeg nødt til at sige, fordi det kan se lidt sjusket ud: Undervejs vil I opleve, at der nok er enkelte fra panelet her, der er nødt til at forlade deres plads for en kortere bemærkning.

Det er jo et hus, hvor der foregår alt muligt andet, og der er også nogle ting, som skal ske andre steder i huset, og det er altså grunden til, at nogle bliver nødt til hurtigt at forlade deres stol, men vender tilbage for at kunne stille spørgsmål. Nok engang: Velkommen til jer alle sammen og ordet er dit, professor Peter Blume.

## Hvad er overvågning?

**Peter Blume**, prof., dr.jur., institutleder, Retsvidenskabeligt Institut B, KU

*Overvågning med kontrolformål stiger i takt med, at informationsteknologien giver øgede muligheder for upersonlig og teknologisk overvågning. Når man diskuterer overvågning er det grundlæggende demokratiske værdier og menneskerettigheder, som kommer på spil, og regler om overvågning bør gennemføres med omtanke.*

Overvågning er jo grundlæggende dette at iagttage noget. Det kan bero på almindelig menneskelig nysgerrighed, eller det kan tjene et andet formål, f.eks. kontrol.

Den overvågning, der tager sigte på mennesker og har et eller andet kontrolformål, opfatter jeg som dagens tema. Og det tema er særdeles aktuelt, fordi overvågnings-omfanget er stigende, og fordi den moderne informationsteknologi skaber mange fristelser, og fordi tidens overvågning kan karakteriseres som upersonlig og teknologisk. Det er en anden type overvågning end den gamle, hvor nogen måske fulgte efter nogen på gaden og den slags.

Overvågning kan tjene gode og fornuftige samfundsmæssige formål, som f.eks. at forebygge kriminalitet, at beskytte væsentlige samfundsværdier eller beskytte privat ejendomsret. En særlig form for overvågning, er den, der tager sigte på at sikre, at de, der lønnes for at udføre et arbejde, også rent faktisk udfører dette. Skyggesiden er, at overvågning typisk indebærer indskrænkning i privatlivets fred og kan medføre en krænkelse af den enkelte borgers og den enkelte ansattes personlige integritet.

Argumenterne for overvågning i konkrete tilfælde er typisk håndfaste og ofte lette at forstå, mens argumenterne, der fremføres imod en konkret overvågningsidé eller tanke, ofte er vage og kan virke abstrakte. De står tit svagt i den retspolitiske debat, og de er tit under pres.

**Generationsforskelle**
Samtidig foreligger der også nok i dag generationsforskelle i den forstand, at måske især de unge er tilbøjelige til at være tiltrukket af, hvad man kunne kalde "overvågningens dubiøse charme". Der er sagt, eller nogen har sagt, at de unge har erkendt, og ved godt, at man ikke kan have så mange hemmeligheder i dag, som man kunne tidligere.

Og som vores ordstyrer også har nævnt, er der tendenser til selvovervågning. Men selv om det er tilfældet, er det fortsat grundlæggende demokratiske værdier og grundlæggende menneskerettigheder, som kommer på spil, når man skal diskutere overvågning.

**Lovgivning og regler**
Det, der så er det politiske eller lovgivningsmæssige problem, er at foretage en afvejning eller en afbalancering mellem disse modstridende hensyn. Det er ikke let. Og svarene, der bliver givet i lovgivningen, har stor betydning for individets stilling i samfundet, og i det hele taget for den retskultur vi har i landet.

Hvis man derfor kigger på vores lovgivning, så indeholder den en lang række svar. Nogle af disse er helt uproblematiske. Mens nogle er lidt vage, kan man sige, som f.eks. tv-overvågningsloven, der af mange - men ikke af alle - kritiseres for at være utilstrækkelig, og som måske har et lidt uklart forhold til EU's direktiv om beskyttelse af personoplysninger og den persondatalov, som Folketinget vedtog for et par år siden. Det er jo en lov, vi kommer til at diskutere i løbet af dagen.

Andre svar, man kan opfatte som problematiske eller i hvert fald diskutable, er f.eks. retsplejelovens regler om teleoplysning. Og på det område, der drejer sig om arbejdsmarkedet, kan man også diskutere, om det er lovgivere, eller om det er arbejdsmarkedets parter, som skal fastsætte reglerne via arbejdsretten. Min egen opfattelse er, at det sidste nok ikke er nogen god vej at gå, men det kommer der også til at blive diskussion om.

Under alle omstændigheder er de regler om overvågning, der er gennemført - om det nu er af lovgivere eller arbejdsmarkedets parter eller nogle andre - alvorlige, og bør gennemføres med omtanke. Og det gælder ikke kun de enkelte regler, men det gælder også, når man ser reglerne under det samlede perspektiv og ser på, hvilket samfund de skaber.

Og måske er et af de problemer, der kan foreligge i dette hus (Folketinget, red.), at det måske nogen gange - i hvert fald, hvis man ser det udefra - kan opfattes således, at idéen med at have et stående folketingsudvalg, som på mange måder er en glimrende idé, måske nogen gange kan skabe visse koordinationsproblemer, hvor den ene hånd måske ikke altid helt kan overskue, hvad den anden hånd foretager sig.

Alvoren kommer også frem og vil komme frem snart, når man her i Folketinget skal vurdere, om begivenhederne den 11. september, som vi jo ikke kan komme uden om at diskutere i dag, gør lovændringer, der øger overvågning nødvendig. Efter min opfattelse er det vigtigt på det punkt ikke at være naiv, men på den anden side heller ikke at gå i panik. En panik som man i parentes bemærket kunne sige hersker lidt ude i samfundet omkring hysteriet om det meget pulver.

Men grundlæggende gælder med stor vægt på dette område således, at man skal passe på ikke at bekæmpe demokratiets fjender på den måde, at man samtidig fjerner demokratiet.

**Kim Rasmussen,** kultursociolog og forskningslektor, Center for Institutionsforskning, Højvangsseminariet

*En af problemstillingerne drejer sig om, hvorvidt overvågningen er frivillig eller er påtvungen. Der, hvor overvågningen foregår automatisk, anonymt og påtvunget, vil overvågningen ofte afføde usikkerhed og ubehag, og ubesvarede spørgsmål. I dag oplever store dele af befolkningen, at der er en informationsmangel omkring overvågning.*

Jeg skal fremhæve et par udvalgte problemstillinger, der ud fra demokratiske værdier påkalder sig særlig opmærksomhed, når vi drøfter overvågning. Den ene problemstilling drejer sig om, hvorvidt at overvågningen er frivillig, eller om den er påtvungen.

Kernen i spørgsmålet drejer sig om, hvorvidt at vi som myndige borgere har mulighed for at vælge overvågning til og fra. Har vi overhovedet valgmuligheder? Eller er vores myndighed ved at blive afmonteret over for det her fænomen? Er vores hidtidige form for privathed og integritet ved at blive ophævet og omformet?

Da spørgsmål om overvågningens positive og negative side ofte hænger mere eller mindre sammen med, om den er frivillig, eller om den er påtvungen, så er skellet ikke uvæsentligt. Ældre borgere, oplever det som positivt at være overvåget i eget hjem, så de kan få hjælp, når de har behov for det, og hjertepatienter oplever det også som positivt, at de er overvåget på hospitalet, så de kan få hjælp i tide, når det er påkrævet.

Meget tyder på, at overvågning ikke er helt så problematisk, når man selv har bedt om den, ej heller selv om den er personrettet. Blot man kender dens mål, dens form, dens omfang, og at man selv aktivt har givet accept. Omvendt, der hvor overvågningen foregår automatisk, anonymt og påtvunget - hvilket den i stigende grad gør, ved pc`ere, i butikker, indkøbscentre, togstationer, alle steder efterhånden - der vil overvågningen ofte i lige så høj grad afføde usikkerhed og ubehag, og ubesvarede spørgsmål, selv om det vil bidrage til en følelse af tryghed og sikkerhed.

Det må ikke ignoreres, at en del mennesker siger, de føler sig sikrere på togstationer og i parkeringskældre, når der er kameraovervågning. Også selv om det er relativt nemt at afvise som en falsk sikkerhed. Erfaringerne viser jo, at hvis man vil omgå alt det teknologiske grej, så tager man blot en maske over hovedet eller sprøjter linserne til eller kaster jakker over kameraerne.

## Overvågning af børn

En særlig problemstilling, som rejser sig i forbindelse med spørgsmål om, hvorvidt overvågningen er frivillig eller påtvunget, gælder de yngste generationer, især børnene. Der er ingen grund til at antage, at børn adskiller sig væsentligt fra voksne i

forbindelse med at blive overvåget. Hvad der er anderledes er, at hvor de voksne har bedre mulighed for at kunne sige fra på deres arbejdsplads, institution osv., der er børn uden egentlige midler til at kæmpe imod.

I dag tilbringer børn i stigende grad mere og mere tid i institutioner og i skoler, ofte på et begrænset område, der ikke er vanskeligt at overvåge. De er med andre ord ofte tvunget til at lade sig overvåge, dels nærovervåge af pædagoger og lærere, og visse steder nu også fjernovervåge af forældre og andre. Og det er sket i en udstrækning, at der i visse børneinstitutioner og skoler nu anbringes web-kameraer, hvor de voksne kan klikke sig ind efter behov.

Men har børn ingen ret til privathed og til frihed, når de er i institution? Har børn ingen ret til at bestemme og være medbestemmende om deres eget liv længere, blot fordi at barndommen er blevet institutionaliseret? Spørgsmålet er her, om særlige grupper i samfundet skal have særlige rettigheder, der kan beskytte dem mod overvågningstendenserne.

**Manglende information om overvågning**

En anden særlig problemstilling drejer sig om den forskel, der er på overvågnings-formen. Om den er personlig og synlig, eller om den er upersonlig og automatisk. Nutidens overvågningstendenser går i retning af at lade overvågningen være automatisk og upersonlig. Teknologi og medier er blevet skubbet ind imellem mennesker. Det er der utvivlsomt visse fordele ved nogle steder og i visse tilfælde. Men er det altid ønskeligt?

Den automatiske og afpersonaliserede overvågning er båret af flere samvirkende forhold. Der søges tekniske løsninger på problemstillinger, som før er blevet løst af mennesker alene, og der er stor tillid og tiltro til teknologi, mens alternativer sjældent overvejes. Og driftsomkostningerne ved teknologisk overvågning er økonomisk billig.

Nogle konsekvenser ved den anonyme, elektroniske overvågning er, at overvågerne bliver ansigtsløse, og at forholdet mellem overvåger og den overvågede bliver upersonligt, følelsesløst og distanceret. Man kan sige, at magten mister sit ansigt.

Tilsyneladende får overvågerne mere magt og kontrol. Tilsyneladende affinder og tilpasser de overvågede sig. »Hvis man ikke har gjort noget, hvad så?« kan et resignerende svar lyde. Der er dog også eksempler på, hvordan der, i samme takt som teknologien udvikles og udbredes, ofte udvikles modmagt og modstrategier, og måske er det sådan, at hvert nyt magtform blot afføder nye modmagtformer og nye modstrategier.

Med tendensen hen i mod den automatiske og upersonlige og teknologiske overvågning rejser der sig en række spørgsmål. Det er ikke altid klart, hvor man er

overvåget. Det er ofte uklart, hvem der præcis foretager overvågningen og registreringen. Og det er heller ikke altid klart, hvorfor man er overvåget.

Det er ofte uklart, hvad overvågningsregistreringer skal bruges til. Og det er uvist, hvor længe disse opbevares og så lignende. Kort sagt: I dag oplever store dele af befolkningen, at der er en informationsmangel og en informationsknaphed omkring overvågning.

**Peter Christensen,** CNDO, Co-operative Network and Data Operation

*På arbejdsmarkedet er det et problem, når tekniske elementer bliver vendt til overvågning, og arbejdsgiveren kan udlede en profil af de ansatte. Og også gennem det software, vi køber, kan man indirekte risikere at få en form for overvågning af den enkelte bruger.*

Jeg har fået lov til at perspektivere det lidt fra den tekniske side, altså balancen omkring hvad overvågning er. For at vi kan holde det her teknologiske samfund oppe at køre, så er vi tvunget til at registrere en hel masse omkring vores systemer, en masse logs. Og firewalls til, hvor der forsøges uautoriseret adgang fra hackere og andre.

Vi er tvunget til at registrere, hvad der er af fejl, så vi kan reparere dem osv. Det har vi gjort i årtier. Det, der sker nu, det er så en udvikling. De samme logs indeholder jo også nogle elementer af persondata. Det betyder så, at en arbejdsgiver f.eks. kan sammenholde flere af den type logs eller scanne en bestemt log og dermed udlede en bestemt profil af sine ansatte.

Det, der er problemet i den sammenhæng, er selvfølgelig, at det ikke er altid er, at den ansatte ved det. Og det er ikke altid, at de oplysninger, der kommer ud af sådan en samkøring, er sikre. Og hvad er sikkert? Ofte vil det være repræsenteret af en arbejdsstation og ikke af en person. Det kunne være en anden, der havde siddet i arbejdsstationen osv. Det, som jeg ser som en problemstilling i den sammenhæng, det er sådan set, at man bruger nogle tekniske elementer, som vi har haft kørende, til at vende mod at bruge det til overvågning.

Vi ser også nogle andre teknologiske udviklinger. Specielt med de nyeste former for Office-systemer. Vi ser nogle agenter komme ind i software. I første omgang nogle positive agenter på den måde, at de kan fortælle, at nu har du ikke opdateret dit virus-program, nu skal du opdatere det ene og det andet.

Det, det også bliver brugt til nu, det er til at opsamle oplysninger om den enkelte arbejdsplads og sende til den, der f.eks. har solgt softwaret. Der bliver også samlet oplysninger om den enkelte person, der er registreret som bruger af det her software.

Og det betyder, at det nyeste Office-software faktisk sætter en profil for den enkelte bruger, som skal anvendes i en clearing på nettet.

**Hjælp eller overvågning**
Den form for overvågning, kan man sige, kommer indirekte af nogle systemer, som vi bruger i vores daglige arbejde, og problemstillingen ligger, som jeg ser det, at: Hvornår er det her overvågning? Og hvornår er det overvågning, kan man sige, fra en helt anden side, nemlig fra en software-agent eller en softwareleverandør? Og hvornår er det faktisk noget som, man kan sige er hjælp til den enkelte bruger af systemerne?

Man kan sige, at i øjeblikket foreligger der ikke rigtig nogen retstilstand i denne her sammenhæng, men det store problem er selvfølgelig, at der jo ikke er nogen, der tager en overvågningsdiskussion, før man opgraderer sit software i dag. Men med det software, vi bruger, risikerer vi indirekte at få den form for overvågning af den enkelte bruger.

## Spørgsmål fra Folketingets spørgepanel

**Ordstyrer, Lissa Mathiasen** (S):
Tak for det. Det var den første blok: »Hvad er overvågning?« Overvågning i lovens forstand, skellet frivillig/ikke frivillig, elektroniske spor. Nu er det spørgepanelets tur, men jeg skal også sige: Skulle der være nogen fra ekspertpanelet, der sidder og brænder med at komme med bemærkninger, så må I også godt komme ind.

**Kristian Jensen** (V):

| |
|---|
| *Ændrer folk adfærd, når de ved, at de bliver overvåget?* |

Tak for det og tak for oplæggene. Jeg vil godt stille mit første spørgsmål til Kim Rasmussen. Noget af det, som er interessant, når man snakker overvågning og den overvågning, der i stigende omfang foregår, det er: Ændrer folk adfærd, når de ved, de bliver overvåget?

Det synes jeg, vi godt kunne bruge lidt belysning af, og jeg håber, at du er en af dem, der kan bidrage til det. Du er bl.a. inde på det der med, at der er sådan et mantra, der hedder: »Overvågning gør jo ikke noget, hvis ikke man har gjort noget forkert«.

Men hvis det er sådan at alene det, at overvågningen finder sted, betyder, at folk, de ændrer adfærd fra måske det, de gerne ville have gjort, til det, de forestiller sig er socialt acceptabelt, så har overvågningen jo stor betydning. Også selv om man ikke

har gjort noget, der i lovens forstand er ulovligt. Kan du uddybe, om der er nogen undersøgelser på, hvorvidt overvågningen i sig selv får folk til at ændre adfærd?

**Kim Rasmussen:**

*Der er forsket meget lidt i overvågningskonsekvenser og om det får folk til at ændre adfærd. Men der er masser af eksempler på, at de kriminelle tager deres forholdsregler og at overvågning ikke afholder dem fra at foretage sig det som de gør.*

Altså generelt kan jeg sige, at der er forsket meget, meget lidt i overvågnings-konsekvenser. Vi kender faktisk ikke nogen undersøgelser fra Danmark eller fra de skandinaviske lande, ikke mig bekendt. Så i forhold til, hvor hurtigt det fænomen har udbredt sig, og hvor omfattende det er, så er der altså forbløffende lidt forsknings-baseret viden omkring det her.

Det, vi jo så i offentligheden vil sige - det er, at vi kan se, at der er der en hel del eksempler på, at forbryderne eller de kriminelle tager deres forholdsregler, sådan at selv om der er flere kameraer, og man skulle tro, at det så skulle bevirke, at der så ikke kunne laves de kriminelle handlinger, så er det altså ikke noget, som afholder kriminelle fra at foretage sig det, som de gør.

I forhold til den ganske almindelige borger, der tror jeg faktisk, at det deler sig. Jeg tror, at en del mennesker føler sig vældig generet af det og har lidt ubehag og den slags følelser, som tydeligvis også mange af de tilstedeværende i dag vil kunne nikke genkendende til. Og så vil der være andre, som det ikke berører noget særligt. Så der er ikke noget entydigt svar på dit spørgsmål.

**Sandy Brinck** (S):

*Hvor er uklarhederne mellem persondataloven og lov om tv-overvågning? Vælger vi teknikker, der indebærer overvågning fordi det er komfortabelt?*

Tak for oplæggene. Jeg har et par spørgsmål. Først til Blume, som påstår, der kan foregå noget så exceptionelt som manglende koordinering mellem folketings-udvalgene. Det er jo slet ikke til at forstå. Så nævner du et eksempel, som faktisk er inden for samme udvalg. Så er det helt utænkeligt.

Du siger, der er en uklarhed mellem loven om tv-overvågning og persondataloven. Så vidt jeg husker, så blev det sådan, at tv-overvågningsloven vedtog vi først, og så endelig, endelig - fordi det tog lang tid med persondataloven - så kom persondata-loven. Kan du prøve at præcisere lidt, hvori uklarhederne ligger?

Så er både du, Blume, og Kim Rasmussen inde på spørgsmålet om frivillighed kontra der, hvor man ikke kan vælge overvågning fra. Blume kalder det selvovervågning i det skriftlige oplæg. Det synes jeg er en spændende skelnen, hvis vi kan lave den. Og derfor vil jeg godt spørge Kim Rasmussen, fordi de eksempler, du fremhæver, hvor man bliver overvåget på sygehuset og andre steder, er indlysende for enhver, at det er positivt, men om der ikke også er andre situationer, hvor man kan sige, at vi i vores ønske om komfort vælger nogle redskaber, som vi godt ved har den bieffekt, at de afleverer elektroniske spor?
Jeg tænker på dankort, jeg tænker på mobiltelefoner. Og at der også i de valg ligger en mulighed dels for selvfølgelig at vælge det helt fra, men også at begrænse antallet af spor, man lægger efter sig. Her tænker jeg på taletidskort og at vi hæver store summer penge ved automaten osv. Så den der frivillighed kontra tvunget overvågning, kan den afgrænsning også indeholde denne her slags remedier, hvor der jo altså også foregår en vis form for overvågning?

**Peter Blume:**

*Hvis tv-overvågning kan identificere de pågældende personer, er det en indsamling af oplysninger. Det udløser nogle skiltningskrav, som i dag ikke er opfyldt.*

Nu skal man måske lige præcis i dette hus selvfølgelig være varsom med at sige noget om – eller det er måske en lidt anden diskussion, kan man sige - hvordan Folketinget strukturerer sit arbejde, så det gik sådan set ikke.

Det er selvfølgelig rigtigt, at tv-loven og persondataloven er samme udvalg. Men det gik mere på f.eks. en fornemmelse af, om man nu var ovre i Trafikudvalget, når man snakker om hvilke regler, der skal gælde for overvågning af nye broer. Det var mere det, som jeg tænkte på.

For så vidt angår tv-overvågningsloven og persondataloven, ja så er det min grund-opfattelse, at hvis der er tale om, at man ved, tv-overvågningen kan identificere de pågældende personer - hvis man nu f.eks. er på en arbejdsplads, hvor jeg går ud fra, at arbejdsgiveren ved, hvem han har ansat - hvad er tv-overvågning så? Ja, det er indsamling af oplysninger.

Det udløser så nogle krav, som i dag ikke er opfyldt. Det krav om den måde, man fortolker skiltningskravet f.eks. i overvågningsloven. Hvis nu der var et kamera her, så skulle der sidde et lille skilt et eller andet sted, hvor der stod »tv-overvågning«.

Men i virkeligheden skulle der sidde et skilt, der forklarede - det giver måske sig selv - hvem det var, der overvågede, og hvad formålet var. Og det sidste er vigtigt, når

man kommer til spørgsmålet om: Er der adgang til at opbevare oplysningerne bagefter, hvis man nu optager?

Altså jeg tror - og man kan også se, at de ting, der diskuteres på EU-niveau i øjeblikket - at der er sådan en kommende diskussion om, hvorvidt det her spørgsmål om tv-overvågning er tilstrækkeligt i overensstemmelse med de grundprincipper, der er omkring beskyttelse af personoplysninger. Det er en lang diskussion, men den kommer, tror jeg. Og når jeg i dag nævner det, så er det, fordi min egen opfattelse er, at den her lov om tv-overvågning ikke er imponerende, for nu at sige det sådan pænt. Og så vil jeg lige sige til sidst, inden Kim Rasmussen får ordet, at der jo er to spørgsmål. Det ene spørgsmål er, om teknologien er overvågelig i sig selv, altså om man ligesom er opmærksom på, når man bruger mobiltelefonen, at så kan ens bevægelser nu følges. Der er en kendt mand, som hedder Thorsen, som nok ikke var opmærksom på det. Og det andet er, om man selv gerne vil overvåges. Hvis man gerne vil med i »Robinson« eller i »Big Brother« eller gerne vil have et web-kamera inden for sit hjem over nettet. Det er det ene sæt overvågning, og der hvor generationsforskellene måske kan vise sig efterhånden.

Og man må også kunne sige omkring børnene f.eks.: Det er rigtigt, der er særlige problemer med børn, men det er også rigtigt måske, at de jo er vokset op i en anden teknologisk virkelighed, end vi er vokset op i. Og de vil måske vænne sig til at synes, at visse former for det, vi kalder overvågning, som vi synes måske er lidt betænkeligt, opfatter de måske som helt naturligt. Altså samfundets ideologier og opfattelser udvikler sig jo trods alt over tid. Men det fører jo direkte denne vej.

**Kim Rasmussen:**

*Der vil knytte sig overvågningsaspekter til al teknologisk udvikling fremover. Det er nødvendigt at snakke konkret om, hvad det er for en type overvågning, hvilken teknologi og hvilke konsekvenser den har. Men debatten halter bagefter udviklingen.*

Jeg vil gerne præcisere sådan to grundpræmisser, som vi taler ud fra, når vi snakker om overvågning. Det er for det første, at vi kan snakke alment om overvågning, men overvågning gør sig altid gældende konkret, og derfor så bliver vi nødt til, selv om det er anstrengende, at snakke konkret om, hvad det er for en type overvågning, hvilken konsekvenser, den har osv. i forhold til hvilken teknologi, det er vi snakker om.

Vi kan ikke løsrive det almene til en abstrakt diskussion. Det bliver sådan noget akademisk snak. Det andet, jeg gerne vil sige, det er, at så snart vi snakker om overvågning, så kan man sige, at der altid gør sig et bipolart forhold gældende. Der vil være en overvåger, og der vil være en, der er overvåget. Og i sådan et forhold vil

det også altid være en magtrelation, hvor overvågeren har en magt, som den overvågede ikke har. Så kan de to poler undertiden have et interessefællesskab, men det gør sig langt fra gældende altid.

Og konkret - altså jeg kan godt have en interesse i, at mine økonomiske betalinger - når jeg står med mit kort - at de bliver registreret, og jeg får det oplyst osv., hvor at den, der overvåger mig, og jeg selv langt hen ad vejen har den samme interesse. Men jeg kunne finde adskillige andre teknologier, hvor jeg ikke har den samme interesse som den, der overvåger mig.

Derfor bliver vi nødt til at snakke om det meget konkret. Og det er vanskeligt, fordi teknologien er så udviklet, og fordi selve fænomenet er så udbredt i dag. Altså hvor vi kan sige, at de her debatter osv. faktisk kommer haltende temmelig langt bagefter udviklingen.

Så vil jeg sige omkring den teknologiske tendens i dag er, at vi har stor tillid til, at teknologien kan løse vores problemer, og jeg ser sjældent, at der alvorligt og seriøst bliver drøftet alternativer. Men i stedet for at det bliver måske modeagtigt - de yngre generationer kan måske endda synes, at det er trendy, eller hvad man nu ville kalde det, at indgå i forskellig overvågning osv. - der synes jeg, det ville være vigtigt, at man sådan retspolitisk, og fra politisk hold, tænker i: Er der nu gode grunde?

Altså at man overvejer, når det skal indføres fremover. Fordi for mig at se er det helt stensikkert, at i al teknologisk udvikling fremover, vil der knytte sig overvågningsaspekter til det. Så i al fremtidig teknologiudvikling vil denne her overvågningsproblematik også gøre sig gældende. Og det gør det ikke mindre kompliceret.

**Peter Christensen:**

*Overvågning er tiltagende, fordi den bliver mindre ressourcekrævende.*

Jeg havde en kommentar til videoovervågning kontra registerloven, fordi et af de problemstillinger, som vi har i dag, jo er, at en analog datatransmission er meget, meget svær at overvåge. Tænk på gammeldags telefonsamtaler. Det kræver en mand at overvåge sådan en, mens digitale transmissioner er meget, meget nemme at overvåge. Det er meget mindre ressourcekrævende, fordi man kan lave mønster-genkendelse.

Og det er så også en af årsagerne til, at vi sidder her, fordi overvågning jo delvist er tiltagende, fordi det er mindre ressourcekrævende. Og det vil sige: Det, som vi politisk tager stilling til her, er, at det ikke er økonomien, der i sig selv driver, at vi

har øget vor overvågning, men må være årsagen til, at vi skal have en overvågning. Det må være nogle politiske beslutninger.

Og specielt kan man i den sammenhæng med videoovervågning sige, at video-overvågningsloven blev lavet på baggrund af, at man troede, at det var en analog teknologi, man diskuterede på det tidspunkt.

Hvis man kigger på England f.eks., har politiet i mange år eksperimenteret med mulighederne for at bruge den meget overdrevne overvågning, som de har derovre, af offentlige steder til at mønstergenkende folk, som kunne være kriminelle. Og det betyder bare, at når man kan digitalisere den her form for transmissioner, kan man også bruge det i en form for personregistrering.

**Knud Erik Hansen** (SF):

*Hvor er de etiske problemer konkret i forhold til overvågning?*

Først sådan et mere generelt spørgsmål - også lidt foranlediget af det, Peter Blume sagde med forholdet mellem retssikkerhed og så, når der kommer nogle begivenheder, som terror - om det i virkeligheden ikke er udtryk for noget meget generelt, når vi snakker om overvågning. At når sociale systemer går i stykker, og vi ikke fungerer normalt, så begynder vi at snakke overvågning, altså hvor løsningen måske i virkeligheden ligger i at sikre de sociale systemer.

Jeg vil godt tage det på et andet plan. Altså hvis hjemmehjælpsorganisationen ikke fungerer, er det så dårlig ledelse? Er det god ledelse, der er brug for, eller er der brug for, at man har stregkoder til hjemmehjælpen?

Altså får vi ikke brug for at snakke om de andre løsninger i stedet for at snakke om det andet? Nu snakker vi ganske vist overvågning her. Men er grundlaget i virkeligheden ikke, at der er sociale systemer, der går i stykker, og det er derfor, vi har brug for at snakke om overvågning?

Det andet spørgsmål går på, hvor er det egentlig? Fordi jeg synes, I er kommet med nogle fine oplæg. Der er mange, mange aspekter at tage fat på, men når vi sidder som politikere, så sidder vi jo i den situation nu, at der sker sådan en kæmpeteknologisk udvikling, og vi har ikke vores etiske apparat til egentlig at sige, hvor er det godt og skidt. Og vi har brug for at sige, hvor er det egentlig, det brænder på. Og I har lidt bud på det.

Men jeg vil egentlig godt spørge jer - hvis I skal komme med nogle bud - hvor er det egentlig, I synes, de etiske problemer rigtigt brænder på? Jeg vil godt sige som start,

at jeg synes, der er nogle ting omkring elektroniske spor og åbne kuverter, store dataindsamlinger, som vi ikke har kontrol over, som er dybt problematisk.

Omvendt så synes jeg, der er nogle andre ting, f.eks. som trafik, hastighedskontrol som har en anden karakter. Det svarer lidt til, at man med en dommerkendelse faktisk overvåger kriminelle, fordi det er jo en kriminel handling, man foretager, ikke? Så det har lidt den karakter. Roadpricing - er det overvågning? For det svarer måske i virkeligheden bare til, vi har en elmåler. Altså den plejer vi ikke at kalde for overvågning.

Altså hvor er det, I vil sige præcis, eller kom med et bud på et par steder, hvor I synes, vi har nogle virkeligt etiske problemer konkret i forhold til den overvågning, der foregår rundt omkring?

**Peter Blume:**

*Et grundlæggende etisk problem er, at borgeren bliver alt for synlig i forholdet mellem stat og borger. Og at borgerens frihedsrum bliver mindre og mindre.*

Altså, jeg er jo enig i, at det der med overvågning jo tit kan blive gennemført som noget, man gør, frem for at gå ned til at prøve at løse problemet i stedet for. Det svarer jo til, når man nogle gange finder ud af, at nu skal man kriminalisere eller øge strafferammen for et eller andet, og så konstaterer man måske nogle år efter, at den der forbrydelse og den handling overhovedet ikke blevet reduceret noget som helst. Der er bare nogle mennesker, der måske sidder en anelse længere i fængsel. Så nogle gange, kan man sige, at overvågningen har den karakter.

Hvis man f.eks. tager de udvidede muligheder, som kommunerne har fået gennem årene for at samkøre registre med henblik på at afsløre socialt bedrageri og lignende, ja, så kan man sige, at disse regler har medført, at borgeren er blevet endnu mere sådan informationsnøgen, end han eller hun var før i samfundet. Mens de, man har fanget i systemet, måske har haft en vis præventiv virkning. Det er rigtigt. Men dem, man har fanget, er jo meget få i virkeligheden.

Og når man så har prøvet at køre det hele vejen igennem, ja, så er politiet og anklagemyndigheden jo tit nået frem til, at der ikke var grundlag for straffesagen i virkeligheden. I stedet for måske at gøre noget ved de årsager, der frister folk til at prøve at skaffe sig lidt flere offentlige ydelser, end de egentlig har været berettiget til.

Men der er altså hele tiden de her modvejende hensyn. Altså, hvad angår trafikken, vil jeg bare sige, at det med hastighedsgrænserne, ja, men roadpricing vil jeg jo

mene, at det er et område, som Folketinget skulle se meget nøje på, inden man ligesom siger o.k. til det. Fordi det kan på en måde måske godt gennemføres uden personkontrol, men der er også store muligheder for, at borgernes muligheder for at færdes ubevogtet forsvinder med sådan nogle systemer.

Og på trafikkens område der, som jeg også antydede i papiret, må man udefra altså tænke på, om det nu er af hensyn til trafiksikkerheden eller miljøet, man gennemfører en eller anden form for foranstaltning i trafiklovgivningen? Eller er det af hensyn til statens økonomiske interesser, at det giver flere penge i bødekassen, for nu at sige det lidt firkantet.

Det grundlæggende etiske problem er - efter min opfattelse - altså det der med, at borgeren bliver alt for synlig, kan man sige, i forholdet mellem stat og borger. Og at individet på længere sigt forsvinder ind i kollektiviteten, for nu at sige det meget pænt. Altså at borgerens frihedsrum, hvor vi er os selv, bliver mindre og mindre. F.eks. når man prøver at pålægge hjemmehjælpere informationspligt over for kommunen, når de går ind i folks private hjem og den slags ting. Og det det må man på en måde diskutere konkret.

Sådan helt overordnet kan vi godt sige de her ting, men det bliver mange jo ikke specielt meget klogere af. Men man må jo gøre det i de konkrete tilfælde. Eller man må gøre det, for nu at lufte min yndlingstanke, på den måde, at - nu taler vi altså om eksperter - få nogle til ligesom at prøve at tage temperaturen generelt på overvågningssituationen i dag i lovgivningen. Hvor er det egentlig henne, der er former for overvågning som et instrument, som de forskellige udvalg i Folketinget, og Folketinget i det hele taget kunne bruge, når man går i gang med nye lovgivnings-initiativer på de her områder?

Ikke en lovpause. Det ved alle, at det bliver aldrig til noget, men måske en sænkning af tempoet lidt, med mindre selvfølgelig, der sker store ting, som gør, at man skal sætte tempoet lidt op. Men altså prøve at få et overblik. For det er det, man ikke har i dag. Og det tror jeg heller ikke der er nogen af eksperterne, der har. Men måske er der andre, der kan sige noget.

**Kim Rasmussen:**

*Det kan være med til at forandre barndommen radikalt, hvis der gives tilladelse til videoovervågning i børnehaver, uden at der er saglige grunde til det.*

Jeg vil godt komme med en kommentar til et punkt omkring det etiske. Altså jeg var i mit oplæg inde på, at børns liv har forandret sig i de sidste 30 år, sådan at man kan sige, barndommen er blevet institutionaliseret i dag. Og det betyder i forvejen, at

børn er en hel del mere overvåget og befinder sig en større del af dagen på et meget mindre areal, end de gjorde for et par generationer siden. Så hvis der udvikler sig en tendens til, at der skal være videoovervågning i børneinstitutioner osv., så synes jeg, der er et etisk problem. For jeg savner nogle gode begrundelser for det.

Jeg synes, at det kan være med til at forandre barndommen faktisk ret radikalt, hvis vi giver tilladelse til det, uden at der foreligger nogle saglige grunde for det osv. Jeg vil hævde, og det synes jeg er helt legitimt, hvis forældre presser på og gerne vil vide noget mere om deres børn, som de så er adskilt fra osv., det er jo grundlæggende godt og sundt at ville vide noget om sine børns liv.

Men der er andre måder at tilfredsstille den viden på end ved at normalisere, at der hænger overvågningskameraer oppe alle steder, sådan at børn de ser og oplever det som noget normalt fra barnsben af.

**Peter Christensen:**

*Overvågning bruges som kollektiv afstraffelse.*

Jeg vil nærmest se det fra et moralsk synspunkt. Altså jeg opfatter, at overvågning i dag bliver brugt som en form for kollektiv afstraffelse, hvis man kan sige det sådan. Og jeg kan eksemplificere det fra arbejdspladsen.

Hvis min kollega ved siden af sidder og bruger sin arbejdstid på at surfe eller sende personlige breve osv., så kan man sige, at det, der sker er, at man i stedet for, at arbejdslederen går hen og sørger for, at han er beskæftiget i sin arbejdstid - det er det, der hedder management, som ligesom er en forpligtelse i forhold til retten til at lede og fordele arbejdet - så går man i stedet for hen og laver overvågning i stedet for om, hvem der gør det ene og det andet. Og det betyder, at det jo rammer selvfølgelig også alle mulige og bliver brugt imod dem.

Det kan jo godt være, at det så bagefter bliver brugt til nogle småting, f.eks. problem-stillingen, som man jo har med videoovervågning: Skal man straffe alle forbrydelser, som man ser via video, f.eks. også en, der står og kommer til at pisse op ad en port ved nattetide, skal han også straffes, fordi nu har vi for en gangs skyld set, at han gør det?

Og det problemet er, at når man så bruger overvågning til at lave denne kollektive afstraffelse, så får man opdaget alle mulige bagateller, som man så skal til at sætte sig moralsk ned og finde ud af - skal man så også gå efter dem også?

Og der ser jeg et moralsk problem i vores samfund, om at det er dér, vi gerne vil hen, at vi gerne vil overvåge alle de små detaljer.

**Helge Adam Møller** (KF):

*Har de unge generelt et mere afslappet forhold til overvågning, eller er det kun på nogle områder, de har det?*

Det, jeg godt ville spørge om, og det er nok til Kim Rasmussen - og Peter Blume var lidt inde på det i et af sine svar før: Er der ikke en meget markant forskel sådan statistik set eller generelt mellem, skal vi sige, unge menneskers og yngre menneskers, måske op til 35-40 år, holdning til hele problematikken og så os, der har passeret de 40 år?
Forstået på den måde - jeg tror, det var Peter Blume, der sagde noget om »Big Brother« - altså når de søger unge mennesker til de der udsendelser, hvor de er på 6-8 uger døgnet rundt i alle situationer, så er det jo ikke bare de ti, der er med dér, men der er tusinder og atter tusinder, der forsøger at få lov til selv at eksponere sig for hele nationen og altså synes, det er noget af det mest spændende at blive overvåget og få det ud.

Jeg rejser med toget hver dag fra Næstved til København, og jeg kender efterhånden de fleste af dem under 35 år, deres privatliv, deres kærlighedsliv, deres sygdomme, fordi det sidder de fuldt offentligt og snakker om, så hele kupeen kan høre det hver morgen, og det generer dem overhovedet ikke.

Så mit spørgsmål er altså hen af: Er der i virkeligheden en kæmpe generationsforskel med holdningen til mange af de problemer, vi i øjeblikket diskuterer og kommer til at diskutere resten af dagen? For hvis der er det, kunne man vel godt forestille sig, at typisk folketingsmedlemmer, der er 10-15 eller 20 år ældre, at vi lovgiver på et område, som vores generation føler naturligt, men som overhovedet ikke er noget problem for mange i den yngre generation.

Og så lige til sidst: Jeg kom til at tænke på, at Kristian Jensen spurgte Kim Rasmussen, om det nu ændrede folks adfærd, når de blev overvåget. Gå ned og følg debatten i Folketingssalen, når de bliver overvåget af tv-kameraer - så er debatten dobbelt så lang...

**Kim Rasmussen:**

*Vi ved kun lidt, men må antage, at unge, der har levet med overvågning det meste af deres liv, ikke er så skræmte af det.*

Jeg må jo så igen konstatere, at vi rent forskningsmæssigt ved meget, meget lidt om det. Altså vi kan antage, og vi kan have vores fornemmelser osv., men nogen sikker viden, som er baseret på egentlige undersøgelser, det eksisterer der altså mig bekendt ikke. Men altså personligt er det også min opfattelse, at der nok er en generations-

forskel i forhold til måden at omgås teknologi på og med de kulturmæssige ændringer, der også er afhængig af, hvilken generation man tilhører.

Og det hænger jo for mig at se delvis sammen med, om man oplever, at noget det er selvfølgeligt, altså fordi det har eksisteret hele ens liv, eller om man oplever, at noget det udgør en ændring, fordi at det, man har været vant til indtil en vis alder, det så har forandret sig. Og det skaber selvfølgelig nogle forskelle.

Men du får ikke mig til at tro på, at alle dem, som ser »Big Brother«, at de også gerne selv vil overvåges eller vil være derinde. Der er en meget stor forskel på at være den, der overvåger, den, der ser på og kigger, og så den, der er genstand for »kigningen«, om jeg så må sige.

**Peter Blume:**

*Tror ikke, at unge accepterer alle former for overvågning.*

Jeg tror, der er sådan en vis tendens i den retning, men jeg tror, det afhænger noget af, hvad overvågningens formål er, og hvem der overvåger. Jeg tror ikke, de unge sådan set - det bliver jo igen en trossag - har et afslappet forhold til den offentlige myndigheds overvågning.

Måske har de et mere afslappet forhold til brugen af sådan noget som dankortet og nettet og den slags. Og det med telefonerne det er fuldstændig rigtigt, det er jo et godt eksempel. Den skal ligesom bruges, og nogle siger jo, at de, der taler i mobiltelefon i f.eks. toget, jo i virkeligheden slet ikke taler til dem, de taler med i røret, men taler til alle dem, der sidder i kupeen.

Det er en form for ekshibitionisme, at vi gerne vil vise, hvor interessant eller hvor syge eller hvor forelskede, eller hvad vi nu er, eller hvor mange penge vi nu har, eller hvad det nu kan være. Så jeg tror der nok er visse tendenser, men som sagt, jeg tror ikke, de gælder for al form for overvågning.

**Kim Rasmussen:**

*Forældre føler, at de har bedre kontrol over børn med mobiltelefoner.*

Det er bare en lille ekstra kommentar med et eksempel. Altså omkring mobiltelefoner - uden det er undersøgt - men altså jeg har adskillige eksempler på, at der foregår dybe forhandlinger i hjemmene om børnenes udetider og hvor de må færdes osv., fordi forældrene føler, at de har mere kontrol med børnene, når de er udstyret med mobiltelefoner. Men det foregår i et meget taktisk spil, fordi børn ved også, hvordan

de skal omgås de der ting og sager. Og hver gang der er en magt, er der også en modmagt.

**Per Helge Sørensen**, forfatter, medl. af bestyrelsen i Digital Rights:

*Unge vil ikke lade overvågningen få frit løb. Det er et grundlæggende behov at have et privatliv.*

Nu har vi siddet hernede et stykke tid og overvejet, om vi var unge nok til at tale for den unge generation, og nu nævnte Helge Adam Møller alderen 35. Der er jeg i hvert fald med.

Og jeg tror, man skal passe meget på med at misforstå det, der sker. Jeg tror, der er meget stor forskel mellem den selvvalgte overvågning, det, der sker i »Big Brother«, hvor nogen sælger deres privatliv for at få en status, for at blive set af samfundet, og for at få et tv-show efterfølgende, og så den overvågning, man ikke kan vælge fra.

Jeg tror, du vil opleve, at de folk, der taler i mobiltelefon i kupeen, vil opføre sig helt anderledes, hvis en af deres forældre sad i den kupé. De har måske valgt at sige: Jamen de andre mennesker i den her kupé de er fuldstændig ligegyldige, de berører mig ikke, de har ikke nogen berøring med mit privatliv. Men hvis der sad en person, som havde en berøring, og havde en indflydelse på den persons liv, så tror jeg nok, de kan holde mund, de vil ikke vælge at lade deres forældre eller deres lærere eller andre autoriteter lytter med på den samtale.

De vil formodentlig synes, det var utrolig ubehageligt, hvis deres forældre fik fri adgang til de her positionsoplysninger fra mobiltelefonerne og kunne se, hvem det egentlig var, de besøgte den her eftermiddag, hvorfor var det egentlig helt præcis, de kom hjem efter 23 i forhold til den forklaring, de gav på at komme hjem efter 23 osv.?

Se, jeg tror, jeg må indrømme, at det med at have et privatliv det er noget grundlæggende menneskeligt, hvor vi alle sammen har nogen sfære, hvor der er noget på spil, og andre ting, hvor vi ikke synes, der er noget på spil. Men jeg tror, vi alle sammen har et sted, hvor der er noget på spil, og også mellem unge mennesker i dag og deres forældre eller andre autoriteter der er jeg helt sikker på, at der er noget på spil, og at de ikke bare vil lade overvågning få frit løb.

**Tove Videbæk** (KRF):

*Videoovervågning i børnehaver kan have uheldige konsekvenser. Er det i strid FN's Børnekonvention, når børnene ikke bliver hørt?*

Tak for de meget interessante oplæg og svar, vi allerede har fået. Og Kim Rasmussen talte i sit indlæg bl.a. om børns ret til privattid, og der har også været rørt en hel del omkring videoovervågning omkring børn i daginstitutioner. Vi har også været omkring hele spørgsmålet om overvågningen er frivillig eller påtvungen, og vi har været inde omkring etiske spørgsmål.

Vi har også været omkring det her med, om vi skulle løse det grundlæggende problem i stedet for at sætte overvågning på, og der kunne jeg jo godt måske forestille mig, at problemerne i daginstitutionerne måske var, at der er for få pædagoger i det hele taget, eller også at forældrene egentlig hellere ville være sammen med deres børn, så man derfor sætter overvågning på.

Men mit spørgsmål i det her går ud på, hvordan vurderer du, Kim Rasmussen, eller måske en af de øvrige i panelet, situationen med overvågning af børn med video og web-cam dagen lang i forhold til FN's Børnekonvention?

**Kim Rasmussen:**
Nu ved jeg ikke præcis, hvad det er, du sigter til i den Børnekonvention, så måske du lige ville komme med en replik omkring det.

**Tove Videbæk** (KRF):
Jeg sigter til hele spørgsmålet om frivillighed. I FN's Børnekonvention nævnes der igen og igen, at børnene skal høres, man skal lytte til, hvad de mener. Og jeg har ikke indtrykket af, at børnene bliver spurgt, om de har lyst til at blive overvåget i børneinstitutionerne.

**Kim Rasmussen:**

*Børnene er ikke klar over, at de bliver overvåget i institutioner. Det kan skabe uheldige konfrontationer med voksne.*

Men det er jeg meget enig med dig i. Jeg tror ikke på, at børnene bliver hørt, og det er ikke min oplevelse. Jeg har sågar været i nogle af de institutioner, hvor der er videoovervågning. Det er ikke min oplevelse, at børnene selv er klar over, hvad det er, der foregår. Muligvis er de det momentvis, muligvis er de det ikke.

Og almindeligvis ville det jo også være en måde at normalisere en ting på bare at installere den. Det foregår meget diskret, og man opdager det knap nok, før det

tidspunkt man bliver konfronteret med, at eksempelvis forældrene har set noget, som børnene har oplevet på en anden måde. Og der vil jeg gerne referere til, at jeg for nylig har været med til at lave en undersøgelse om, hvad unge husker, fra dengang de gik i børnehave. Og unge i dag er jo en generation, som generelt er vokset op med institutioner som noget helt normalt.
Noget af det, man husker, det er eksempelvis, at man f.eks. tabte tandbørsten ned i toilettet ved et uheld, og samtidig kom pædagogen forbi og så, at man legede med toilettet og skældte ud. Altså hvor barnets oplevelse og oplevelse af sig selv osv. i den grad blev konfronteret med, at den voksne så noget helt andet, end det man oplevede, der var tilfældet. Og det husker man - det er et spor, som er blevet siddende i mange, mange år.

Og det er nogle tilsvarende ting og sager, man kunne frygte, ville være en af de negative og uheldige konsekvenser, hvis der er videokameraer, fordi i mange tilfælde ville der såmænd ikke ske så meget ved det, tror jeg. Men så ville der være nogle tilfælde, hvor barnets oplevelse i den grad ville blive konfronteret med, hvad forældre eller andre har set. Og den form for konfrontation synes jeg er både uetisk og kan være meget skadelig.

**Eva Smith**, prof., dr.jur., formand for Det Kriminalpræventive Råd:

*Hvis forældrene ved det hele, er der ikke noget for børnene at fortælle.*

Jeg vil sådan set forfølge det spor, du er i gang med. Altså jeg ville være bekymret ved, at der skete et eller andet med børnenes samvær med deres forældre. Moderen kommer hjem, og så siger Lille-Peter: ”Nej, vi har bagt boller i dag.” ”Det ved jeg godt,” siger mor.

Altså der er ikke noget at fortælle, fordi forældrene ved det hele, og jeg kunne også godt være bekymret for, at forældrene på en eller anden måde føler, de har været sammen med deres børn, for de har jo klikket ind syv gange i løbet af dagen og set, at Lille-Peter har det godt. De ville egentlig være kommet tidligt hjem: ”Men det går jo fint det her, jeg har også lidt travlt på arbejdet” og sådan noget.

Så jeg kunne godt være bekymret for, at der bliver mindre samvær mellem børn og forældre, mindre kvalificeret samvær, fordi forældrene følte, at de jo vidste alt om, hvad der var foregået med børnene i løbet af dagen.

Jeg kunne godt tænke mig at vide: Er der ikke nogen planer om at prøve at lave en undersøgelse, mens der stadig er institutioner, hvor børnene ikke bliver overvåget, for at se hvad der egentlig sker?

**Kim Rasmussen:**

*Undersøgelser mangler.*

Jamen det er det samme svar igen. Altså der er forbløffende få undersøgelser omkring konsekvenserne af de her ting og sager. Så jeg kan ikke referere til, at jeg kender en undersøgelse, der.

Ja, jeg arbejder selv med spørgsmålet, det er rigtigt. Men det er egentlig at vi arbejder med en undersøgelse, hvor vi prøver at finde alternativer, hvis pædagoger bliver mødt med det. Altså i børneinstitutioner i dag har man forældrebestyrelser der kan anvise ting og sager, som de gerne vil have, der skal ske med børnenes liv i institutioner, og der arbejder jeg med en undersøgelse omkring, hvilke alternativer der kunne være til, hvis forældrene syntes, at de gerne vil vide noget mere om deres børn.

Det er både legitimt, og jeg synes, det er godt og noget, som skal understøttes, men der er helt andre måder at gøre det på end ved bare den anonyme overvågning. Men det er ikke en undersøgelse, som er færdig, så det kan jeg ikke referere noget til.

**Søren Søndergaard** (EL):

*Udvikles redskaber til brug mod overvågning lige så hurtigt som redskaber til overvågning?*

Jeg vil spørge Peter Christensen, som har beskæftiget sig med den teknologiske udvikling og f.eks. beskæftiget sig med det, at der kommer agenter ind: Hvordan er relationen mellem den teknologiske udvikling, der indebærer overvågning og så den teknologiske udvikling, der indebærer redskaber mod overvågning? Altså vi har det f.eks. med kryptering, hvordan er forholdet mellem de to ting, kan der siges noget?

**Peter Christensen:**

*En del krypteringsfaciliteter bliver delvist undergravet, ved at kommercielle interesser søger for, at der er bagdøre i det software, der bliver brugt.*

Altså man kan sige, det er ligesom på mange områder en optrapningskrig. Der er ligesom, der tidligere blev nævnt, at når man bliver overvåget, så finder man måder at omgå det på, og det er vel præcis det samme, der foregår, når vi enten bruger kryptering, eller man bruger forskellige andre måder at omgå den overvågning - også på nettet.

Så der er ingen tvivl om, at den teknologiske udvikling giver mange muligheder for overvågning. Og så er der klart dem, der har ressourcer, som kan omgå den. Og det betyder selvfølgelig også omvendt, kan man sige, Maren i kæret kan ikke omgå den, men ligesådan kan man sige, at industrien selvfølgelig kan omgå den i det omfang, de har ressourcer til det.
Og der sker en optrapning nu, ligesom der sker den optrapning, som vi kommer til senere, at en del krypteringsfaciliteter delvis bliver undergravet, ved at kommercielle interesser går ind i det, specielt amerikanske, og derfor søger for, at der i nogle situationer er bagdøre i det software, der bliver brugt af forskellige, både på office-siden og på krypteringssiden.

**Ordstyrer:**
Ja tak. Jeg siger tak til vores tre første eksperter og beder jer overlade stolene til vores tre næste eksperter, som vi byder velkommen heroppe ved bordet.

Og det næste, vi skal i gang med af blok, det er spørgsmålet omkring overvågning med et kriminalpræventivt og opklarende sigte. Og i den forbindelse kan jeg byde velkommen til professor Eva Smith. Værsgo, ordet er dit.

## Overvågning med et kriminalpræventivt og -opklarende sigte

**Eva Smith**, prof., dr.jur., formand for Det Kriminalpræventive Råd

*Tv-overvågning kan være et effektivt middel til at tilbyde tryghed for borgere og erhvervsliv. Men det modstående hensyn er, at tv-overvågning kan medføre, at folk føler sig utrygge og krænkede.*

Tak skal du have, og tak for invitationen.
Som vi allerede har hørt, så er overvågning jo et område i stærk vækst. Der udbydes og sælges flere og flere overvågningssystemer også til almindelige mennesker, med henblik på at de kan overvåge deres bolig, når de ikke er hjemme. Og derfor er det tit oppe og vende i debatten, at det sådan er et kriminalpræventivt vidundermiddel, at man ligesom kan overvåge og sikre sig.

Men man skal jo være opmærksom på, at man jo - og det er også det, vi har været inde på her i formiddag - i forebyggelsens hellige navn kan risikere at nå til et samfund, hvor man forvandler tryghed til utryghed, tillid til mistro og forebyggelse til kontrol. Så vi skal passe på, at vi i vores iver for at opklare kriminalitet ikke foretager os ting, der kan være ødelæggende for folks almindelige trivsel.

Og i modsætning til, hvad nogle af foredragsholderne sagde, så mener jeg nu ikke, der er nogen som helst tvivl om, at tv-overvågning kan være et effektivt middel til at tilbyde tryghed for borgere og erhvervsliv. Der er mange undersøgelser fra både ind- og udland, der viser, at tv-overvågning rent faktisk har en forebyggende effekt over for en række former for kriminalitet.

Det er rigtigt, at der måske i et vist omfang måske bare flyttes kriminalitet fra den overvågede butik til den ikke overvågede butik, men at det rent faktisk hjælper, det er der nok ikke nogen tvivl om. Og der er heller ikke nogen tvivl om, at det ofte kan være et godt bidrag til opklaring af forbrydelser, det ved vi jo alle sammen.

Men det modstående hensyn er altså, at tv-overvågning kan medføre, at folk føler sig utrygge og krænkede. I Kriminalpræventivt Råd har vi lavet en borgerundersøgelse, der gik på folks opfattelse af overvågning i, om jeg så må sige, fjernere rum. Og de fleste var meget positive over for overvågning i butikker, på tankstationer, banker, togstationer osv., men så snart man nærmede sig den private sfære, altså arbejds-pladsen, eller tv-overvågning lige omkring den private bolig, så var folk meget negative over for tv-overvågning.

Det kunne være, vi kunne også have lagt snittet på en anden måde: Altså hvornår er tv-overvågning en beskyttelse af dig, og hvornår er tv-overvågning en kontrol af dig.

Jeg tror, de fleste vil føle, at når de kommer ind i en bank, så er det en beskyttelse, eller måske endnu bedre, når man kommer på en station om natten, så er det en beskyttelse. Det er tanken, at nogle skal holde øje, sådan at kriminelle ikke foretager sig ting over for dig, medens hvis det derimod er på din arbejdsplads, så vil der typisk være tale om en kontrol af, om du laver dit arbejde. Men selv på arbejdspladser kan det være en beskyttelse, f.eks. hvis der sættes et tv-apparat over for den dame, der sidder ved kasseapparatet, så kan man godt følge, der er tale om beskyttelse, fordi hvis nogen vil komme og stjæle kassen.

En anden ting, som jeg synes, man skal være opmærksom på med tv-overvågning, er, at den jo også kan give en falsk tryghed, forstået på den måde, at det overvågningskamera, der hænger på stationen, jo ikke er den samme tryghed som et menneske, der havde været til stede på jernbanestationen, ville være.

Der er ikke nogen, der kommer til hjælp, fordi der er et tv-kamera. Ofte vil det være ubemandet, og selv hvis det er bemandet, er det jo ikke usandsynligt, at de mennesker sidder meget langt væk, så du er ikke beskyttet af et tv-kamera på samme måde, som du ville være, hvis der ville være et menneske i nærheden.

En tryghed i samfundet får vi jo, hvis man har en fornemmelse af, at vi, om jeg så må sige, passer på hinanden, at andre vil gribe ind, hvis der sker et eller andet. Det er jo stadig væk sådan, at man siger til sine børn, især sine piger, når de er ude om natten, gå hen et sted, hvor der er befærdet, gå hen et sted, hvor der er andre mennesker, lad være med at gå på stille, mørke veje.

Og det er jo, fordi vi stadig tror på, at andre mennesker vil komme til hjælp, at vi har et samfund, hvor vi forsøger at passe på hinanden. Og der kunne man frygte, at med et tv-kamera, der siger man: ”Nå men o.k. det er noget, tv-kameraet tager sig af, det behøver jeg ikke at blande mig i.” Dertil kommer også, at selve det, at det er der, kan skabe utryghed, fordi det jo minder én om, at man kunne blive udsat for kriminalitet, det er jo derfor, det dér tv-kamera er der.

Jeg tror også, der blev talt om her i formiddag, at jamen man kan jo undgå det, man kan jo bare, hvis man vil ind i en bank og begå et røveri, så kan man tage en maske på, så er det lige meget med tv-kameraet, og det er jo rigtigt. Og dertil tror jeg også, at det har den effekt - det er min personlige opfattelse - at det måske snarere vil udvikle sig voldeligt, hvis folk har en maske på. Jeg tror simpelt hen, det er nemmere at begå vold, hvis du har maskeret dig, end hvis du står ansigt til ansigt med andre mennesker.

Så jeg tror, at der ligger en stor udfordring for jer i lovgivningssystemet til at forsøge at løse dette dilemma imellem tryghed og kontrol, og jeg mener også, der ligger et stort problem i alt det, der allerede nu opbevares. Hvad er reglerne egentlig for det?

Hvem må se det, som opbevares? Hvem må se de bånd, butikker optager?, og hvilke sletteregler er der egentlig for alt det materiale, der ligger rundt omkring?

**Ordstyrer:**
Ja, tak til Eva Smith. Den næste er kontorchef i Finansrådet, Niels Crone Lyngkjær.

**Niels Crone Lyngkjær**, kontorchef i Finansrådet

*Finansrådet ønsker mulighed for at foretage udendørs tv-overvågning, fordi det vil forøge viften af de passive sikringsforanstaltninger, som pengeinstitutterne i forvejen gør brug af for at hindre røverier.*

Også jeg vil gerne sige tak for indbydelsen og tak for initiativet til at holde denne høring. Det er jo således, at spørgsmålet om videoovervågning, specielt at komme uden for den gældende lov om tv-overvågning, det interesserer os stærkt i Finansrådet.

Vi anmodede i januar 2000 Justitsministeriet om en ændring til loven, fordi vi jo gennem årene har været plaget og er plaget af et stort antal røverier, men også anden form for kriminalitet i vores drift af vor forretning. Det, vi gik efter, det var en mulighed for at få adgang at foretage udendørs overvågning i forbindelse med vores filialer.

Som vi har anført i vores oplæg, så er det jo således, at antallet af røverier har været stigende, uanset at vi fra pengeinstitutside gennem årene har ydet en stor indsats, og det mener vi med rette, vi kan sige, for at begrænse røverierne væsentligt.

Vi ved godt, at videoovervågning udendørs - for vi har det jo allerede inden døre i dag, enten videoovervågning eller fotoovervågning - ikke vil forhindre røverier fuldstændigt. Vi tror imidlertid, at der ligger en kriminalpræventiv effekt i, at der bliver opsat sådanne kameraer udenfor, og dermed vil det afholde nogen fra at begå deres forbrydelser. Men vi er jo i den situation, at vi jo ikke ved, hvor mange potentielle røvere og svindlere og andre vi nu møder i vores hverdag, som vi bliver fri for at se, på grund af at vi beskytter os.

Vi mener imidlertid, at den største effekt det er egentlig det offentliges, det er politiet, der får udbyttet af det, vi foretager os. Vores opgave er jo ikke at fange forbrydere. Vores opgave er, når hændelserne er sket, at så give politiet de bedst mulige spor at gå efter i det opklaringsarbejde, der skal følge. Og jo bedre muligheder, vi kan stille til rådighed for politiet, jo bedre, større chance er der for, at de pågældende kriminelle kan blive anholdt.

Vi mener også, at man ved disse kameraovervågninger får bedre bevisbyrder for politiets vedkommende. Når vi går efter det udendørs, så skyldes det jo, at en røver oftest ikke ifører sig maskeringen, før at han indfinder sig foran pengeinstitutfilialen, ligesom han, når han forlader denne, oftest vil tage den af relativt hurtigt, efter at han er kommet uden for døren.

Så ud fra det så mener vi, at der er en mulighed for visse steder, fordi det er jo ikke således, at vi forestiller os, at der skal sættes videoovervågning op udendørs ud for samtlige 2.200 pengeinstitutfilialer. Men visse steder, hvor man må konstatere, at man altså der er særlig udsat, der kunne det være en god mulighed at prøve at sætte sådanne kameraer op.

Man skal også huske på, at når man diskuterer det her, så er det jo ikke billigt at ofre ressourcer på den salgs ting. Har man videoovervågning i forvejen, så er det måske ikke den allerstørste udgift, men skal man etablere videoovervågning i en filial inklusive udendørs for scratch, så må man se i øjnene, at så løber det jo altså op i en omkostning af en vis størrelse. Frygten for, hvad det her skal bruges til? Der kan jeg sige og vil da gerne tage udgangspunkt i, hvad Bodil Udsen for mange år siden sang, nemlig hun sang noget i retning af, at »hvad fanden laver de i banken efter klokken 3?«

Dertil vil jeg sige, at hvis nogen skulle forestille sig og have den opfattelse, at vi i sektoren og medarbejderne skulle være interesseret i at sidde og hygge sig med at se, hvad der nu var foregået på gader og stræder i dagens løb, så tager man ganske fejl. Vi har alt andet rigeligt at se til, så medarbejdernes fornøjelse ved det det behøver man ikke at befrygte. Vi er ikke bange for og forestiller os ikke, at der skulle ske en overvågning af alle detaljer.

Vi har, som jeg nævnte, i dag allerede foto- og videoovervågningsudstyr indendørs i mange af vores filialer, og disse optagelser dem behandler vi selvfølgelig ansvarligt og med største fortrolighed. Det er således, at normalt registrerer man jo op til en måned, og så bliver de pågældende bånd brugt igen, så der er ikke tale om en udnyttelse i, at det ligger i en lang periode.

Finansrådets synspunkt er, at muligheden for en udendørs overvågning vil forøge viften af de passive sikringsforanstaltninger, som pengeinstitutterne i forvejen gør brug for rent præventivt, og for at hindre røverier, checkfalsk eller i hvert fald at have mulighed for, at politiet kan opklare disse sager. Vi er jo udsat for mange forskellige fornøjelser: Angreb på pengeautomater ser vi jo også, vi ser svindel i forbindelse med brug af pengeautomater, og hvad ved jeg. Men det var ordene umiddelbart fra min side.

**Ordstyrer:**
Tak for det. Og værsgo til vicekriminalinspektør Troels Ørting Jørgensen.

**Troels Ørting Jørgensen**, vicekriminalinspektør, Rigspolitiets afdeling A

*Politiet er fuldstændig afhængige af, at der er logning, for at nå videre i de fleste efterforskninger om IT-kriminalitet.*

Tak for det og også tak for invitationen til mig. Jeg er chef for den afdeling i politiet hos Rigspolitiet, som overvåger - vi kalder det »moniterer«, det synes vi lyder pænere. Men vi overvåger organiseret og kompliceret ressourcekrævende kriminalitet og er altså en slags enhed, der kigger på den åbne del af kriminaliteten i modsætning til det, som politimester Bro fortæller om, er i efterretningstjenesterne.

Jeg har valgt at tage udgangspunkt, da det jo er Teknologirådet, der er vært, at tage den mere tekniske del, altså den IT-relaterede del, da vi jo også i den enhed, jeg er chef for, har ansvaret for bekæmpelse af IT-kriminalitet.

Og jeg kan sige med det samme, at der var sådan et spørgsmål, hvordan bruger politiet elektronisk overvågning i deres arbejde? Så kan jeg sige: På Internettet der bruger vi det stort set ikke. Vi overvåger ikke Internettet for kriminalitet i den afdeling, jeg sidder i. Vi har til gengæld 70 pct. af befolkningen, som gør det for os, og som er meget, meget flinke til at anmelde IT-kriminalitet til politiet, uanset om det er racisme, trusler, børneporno eller andre former for kriminalitet. Og der får vi et sted mellem 4.000 til 6.000 anmeldelser om året af svingende kvalitet, men en lang række af dem er direkte anvendelige.

Det er sådan, at kriminaliteten på nettet - stort set har vi i hvert fald grovopdelt det til at være »hacking«, »cracking« og industrispionage i ét spor, kan man sige, og så koncentrerer vi os om et andet spor. Det er e-handelsområdet og piratkopiering. Og det tredje og nok største og mest omfattende spor, som vi kigger på, det er børne-porno, racisme og trusler.

Jeg kan også sige, at på Internettet der fordeler kriminaliteten sig i to blokke igen. Der er den del af kriminaliteten, som er på det åbne web, altså på world wide web-delen, billeder, der ligger sådan mere eller mindre frit tilgængelige. Og så er der hele den mere skjulte del af kriminaliteten, som foregår i de mere lukkede netværk, altså det, der er i IRC-kanalerne og på FTP-serveren.

Jeg skal ikke i øvrigt tage stilling til lovgivningsmæssige initiativer, men blot sådan mere luksusagtigt gøre rede for politiets muligheder for at efterforske den her form for kriminalitet og konstatere, at kriminaliteten jo for en stor dels vedkommende er kendetegnet ved at være international.

Og det vil sige, den kræver altså også en relativ hurtig respons fra politiet til andre myndigheder i andre lande. Og der er det jo altså sådan, at vores nuværende system med udveksling af information på tværs af landegrænserne, som baserer sig på nogle

konventioner om gensidig retshjælp, de fordrer sådan et sted mellem 14 dage til 3 uger, inden de kan effektueres. Og det vil ofte være meget, meget lang tid at vente, hvis man sidder online med en hacking, der foregår fra Tyskland f.eks., at så få noget gjort dér.

Jeg vil også sige, at politiet er fuldstændig afhængig af, at der er logning, for at vi kan komme videre i langt de fleste efterforskninger. Det vil sige, vi er nødt til at have et transaktionsspor, der kan lede os hen til den computer eller server, hvorfra at den her kriminalitet er blevet begået. Og i øjeblikket der står det temmelig skralt til omkring logningsprocedurerne i det her land, og det beror i en meget, meget væsentlig grad på selvjustits hos de enkelte ISP'er.

Lad mig nævne omkring ISP'er - det er dem, der er »Internet service provider«, det vil altså sige, det kan være dem, man melder sig til, når man vil have en internet-konto - at så vidt jeg er bekendt, så er det et fuldstændig ureguleret område. Det vil sige, det er sådan set vanskeligere at få en stadeplads til en pølsevogn på Rådhus-pladsen, end det er at blive IT-ISP'er, fordi det kræver bare, at man køber tre servere og så noget kabelkapacitet hos TeleDanmark f.eks. sammen med E-Business.

Der er ingen form for autorisation, og jeg tror ikke, man kan udelukke, at man på længere sigt vil se, at der er nogle af de mere organiserede kriminelle netværk, der vil se en fordel i selv at være ISP, for det er jo ligesom der, vi henter informationerne, og hvis der så ikke er nogen form for autorisation overhovedet, så er det jo klart, at så kan enhver jo dels blive ISP, og dels kan man jo bare fjerne alt bevisgrundlaget i sin logning, hvis man får et pålæg om at logge.

Her til morgen, inden jeg gik herover, der lå der på mit bord nogle af de grimmeste børnepornobilleder, jeg har set længe. Der var tale om blebørn, der blev voldtaget. Og det så ud, som om det var digitale billeder, der var taget sådan relativt for nylig. Det var i hvert fald billeder, som vi ikke kender til. De var uploadet klokken 04.49 fra en provinsby i Danmark til en mailserver i en folder.

Og på baggrund af, at man dels havde brugt et bestemt selskab, som kun logger IP-nummeret, når man opretter sin konto og så ikke siden, og fordi at man gemmer sig bag ved en router, så er det ikke muligt for politiet med den eksisterende lovgivning at opklare den sag, selv om vi kan lokalisere den til en sjællandsk provinsby. Vi har altså ganske simpelt ikke mulighederne for at opklare den her forbrydelse her, ikke så meget oploadningen af billederne, men mere den krænkelse, der er sket af det barn.

Det var mit indlæg, tak.

## Spørgsmål fra Folketingets spørgepanel

**Sandy Brinck** (S):

| |
|---|
| *Hvad mener Det Kriminalpræventive Råd om bankernes ønske om mere tv-overvågning?* |

Til det sidste er der vel kun lige at sige, at vi håber meget snart også at kunne få lavet regler omkring logning, fordi det er ved gud påkrævet. Jeg kunne godt tænke mig at gribe lidt fat i Niels Crones indlæg, som jo motiveres i et kriminalpræventivt sigte, ønsket om at have denne her øgede overvågning også udendørs. Jeg vil godt sige også i den tilknytning, at det beroliger ikke mig, at der ikke kommer til at være så mange, fordi det er dyrt.

Ja, det er det nu måske ikke? Det er vel en af de ting, vi bl.a. ser: At det bliver mindre, og det bliver billigere, og derfor så øges væksten også af den slags apparatur. Men jeg kunne egentlig godt tænke mig, netop fordi det selvfølgelig er begrundet kriminalpræventivt, at høre Eva Smiths holdning til Niels Crones indlæg. Altså er motivet stærkt nok til, at vi burde overveje det?

**Eva Smith:**

| |
|---|
| *Risiko for glidebane med tv-overvågning.* |

Altså jeg kan jo godt se, at det er fuldstændig rigtigt, som det bliver sagt, at man tager typisk masken på lige udenfor, fordi man kan jo ikke gå ned ad flere gader, uden at det ser lidt besynderligt ud. Så på den måde kan jeg godt se det.

På den anden side er sådan et øje jo til at holde øje med, hvordan man sådan skal gerere sig, når man kommer derhen, ikke? En paraply over hovedet eller et eller andet, der lige gør, at man alligevel kan smutte derhen, og uden at man ser det, får man det ned over hovedet. Så jeg er ikke helt sikker på, at det er helt så effektivt, som du mener, og jeg er også lidt bekymret ved, at: ”Nå, men så var det ikke nok, så må vi så have hele gaden” - så må have den næste.

Altså et eller andet sted bliver man jo nødt til at stoppe det her og sige, jamen det lader sig altså heller ikke gøre helt fuldstændigt at stoppe kriminalitet. Det kan man lige så godt se i øjnene. Og et eller andet sted må vi så sætte en grænse og sige: Dér, der stopper det. Men det er jo en politisk afgørelse. Det er jo jeres afgørelse, hvor I vil sætte grænsen. I siger: ”Fortovet kunne måske en meget god idé, fordi det kan nu alligevel holde en del af dem væk”.

**Kristian Jensen** (V):

*Hvor er forskellen på overvågning af en konkret mistænkt og en gruppe borgere, der ikke er under mistanke?*

Jeg synes, de oplæg, jeg har hørt, meget godt illustrerer det, som Peter Blume var inde på i starten, nemlig diskussionen omkring den meget abstrakte overvågning i forhold til menneskerettighederne og så det helt konkrete, når man står med de konkrete sager - bankrøveri, børnepornografi - at der er det indimellem svært at opretholde argumenterne for den abstrakte rettighed.
Men alligevel er det vigtigt, at vi forsøger, fordi de nye muligheder, som der gives med ny teknologi, er jo positive for langt de fleste af os - desværre også for forbrydelser og forbrydere. Men at ny teknologi kommer til, behøver jo ikke betyde, at vi skal ændre på vores samfund, og vi har jo ikke hidtil registreret i postvæsenet, hvem der sender hvad til hvem. Blot som en lille kommentar.

Men det konkrete spørgsmål det er så også til Eva Smith. Ud fra din juridiske baggrund, bør der være en forskel på de regler, vi sætter op, når vi har fat i en konkret mistænkt, og når vi snakker om en gruppe af borgere, hvor der ikke er nogen konkret mistanke, altså den generelle overvågning og så den konkrete overvågning på en mistænkt person, hvilke forskelle i forholdsregler bør vi tage som politikere?

**Eva Smith:**

*Den kriminalitet, man ønsker at opklare, skal være meget alvorlig, før man kommer med et indgreb over for en hel gruppe, der ikke er nogen mistanke imod.*

Jeg synes klart, der bør være en forskel, fordi man kan sige, at hvis der er en mistanke mod en person, så er der også en god grund til at tage nogle forholdsregler. Og det er klart, at den mistanke kan være ubegrundet, men der plejer vi jo at sige, at det kan vi alle sammen komme ud for.

Vi kan alle sammen komme ud for, at af en eller anden grund så samler der sig nogle mistænkelige ting omkring én, og så kommer man i politiets søgelys, og så kommer man altså ud for nogle indgreb, som var uberettigede. Men det må man ligesom tage med for at få opklaret kriminalitet.

Jeg synes, det er noget andet at tage nogle forholdsregler, som retter sig mod alle, uanset der ikke er nogen konkret mistanke imod dem. Så vil alle komme ud for en eller anden form for indgreb i deres privatsfære. Det synes jeg er en helt anden diskussion, jeg synes, der er en meget, meget stor forskel på det, og jeg synes, den kriminalitet, man ønsker at opklare, den skal altså være meget, meget alvorlig, før

man vil komme med et indgreb over for en hel gruppe, der ikke er nogen som helst mistanke imod.

Eller også skal det være et indgreb, der er så lille som f.eks., at der bliver overvåget på en S-bane-station eller sådan noget lignende, hvor de fleste vil være ligeglade. Men altså går du ind i noget mere personligt, går du ind i deres intimsfære, så synes jeg, det bliver betænkeligt, hvis folk ikke er mistænkte.

**Søren Søndergaard** (EL):

*Kan bankerne straks slette de bånd, der optages, når der ikke foregår røverier?*

Det er et spørgsmål til Niels Crone Lyngkjær. Nu sagde du, at antallet af røverier havde været stigende, det er vel ikke rigtigt. Altså fra 1998-2000 var de stigende, men hvis man tager en længere periode f.eks. fra 1992 ifølge den statistik, I selv offentliggjorde, så har der vel ikke været tale om en stigning.

Men det, jeg godt kunne tænke mig at høre lidt mere om, det var, hvilke krav, I har til den optagelse, I måtte ønske af rummet uden for pengeinstitutterne. For den har vel kun mening i forhold til én ting, nemlig deciderede røverier, og det er vel noget, man ved umiddelbart efter, om et røveri er foregået eller ej.

Det vil sige, er det ønske, I har, er det noget, der kunne løses, ved at man havde en anordning af kameraer, der gjorde, at de så at sige løbende slettede båndet, med mindre de blev standset, sådan at man ikke havde nogen former for opbevaring af båndet i en periode. Du nævnte selv, at I opbevarede båndene fra bankerne i 1 måned, og det må jo siges at være rimelig lang tid i hvert fald i forhold til røveridelen af det.

**Niels Crone Lyngkjær:**

*TV-overvågning giver politiet bedre mulighed for at opklare forbrydelser. Ved ikke, hvor effektivt, det ville være, hvis båndene skulle slettes.*

Som jeg sagde, er der jo forskellige andre former for kriminalitet, som vi også er belemret med, og der er det jo således, at det jo ikke er altid, at tingene lader sig give at opklare, altså man er klar over, der er sket en forbrydelse, før der er gået nogle dage. Og det er så det, der er årsagen til, at man har denne periode, denne cyklus, der ligner 24-30 dage, før at man så skifter båndene.

Men udendørs - vi ved jo ikke, hvornår der indfinder sig en forbryder, og det er derfor, vi siger, at man er nødsaget til i givet fald at overvåge udendørs permanent,

når der er bevægelser i billedet, og så har man så muligheden for at gå ind og kigge på billederne, når forbrydelsen har fundet sted, når politiet kommer, for det er politiet, der får disse ting at gå efter.

Altså medarbejderne i filialen skal jo kun ligesom være med til at sige, det var sådan nogenlunde på det tidspunkt, det er i det interval her, at billederne ligger, man kan måske se det, fordi han er ved at iføre sig masken. Men det er jo ikke altid, tingene er så umiddelbart ligetil, men det er den interesse, der er - det er det, det drejer sig om set med vores øjne, at man kan fokusere på den del af det.

Ligeledes når han løber sin vej, der kan du så sige, at der kunne man aktivere, at det kunne bindes sammen med en aktivering af røverialarmen og det, der går til politiet. Men det ved jeg ikke, hvor effektivt og hvordan det vil komme til at fungere. Den vinkel har vi ikke set det fra.

**Helge Adam Møller** (KF):

| |
|---|
| *Er vi ikke mere restriktive over for ny teknik, bare fordi den er ny?* |

Mit spørgsmål er nok både til Eva Smith og til Troels Ørting, og da det har noget med et pengeinstitut at gøre så måske også lidt til Niels Crone.

Men er det ikke sådan, at vi indimellem, i hvert fald på nogle områder i forbindelse med politiefterforskning, er langt mere restriktive og betænkelige ved at give tilladelse i retsplejelov osv. til efterforskningsskridt, hvor vi benytter den moderne teknik, det, vi tit kalder overvågning, end hvis vi benytter traditionelle og gammeldags metoder. Som i virkeligheden ofte kan være langt mere indgribende i privatlivets fred, men som man bare har kendt i de sidste 50 eller 100 år, og derfor har alle vænnet sig til dem?

Lad mig komme med et helt konkret eksempel: For et års tid siden skete der et indbrud i et pengeinstitut oppe i en lille nordjysk by, og jeg kan ikke huske, om det var Pandrup eller Brovst, men det var en af de to, og det viste sig, at tyvene var brudt ind via en tom lejlighed og så brudt gennem Sparekassens tag om natten mellem lørdag og søndag, og så havde de tømt boksene stille og roligt i løbet af natten. Og det blev opdaget mandag morgen, at der var stjålet en lille million kroner.

Så viste det sig, da politiet gik i gang med efterforskningen, at der var et vidne, der havde set en bil holde uden for Sparekassen netop på tidspunktet mellem lørdag og søndag, og han havde set en mand sidde inde og tale i mobiltelefon. Og så gik man jo i gang og spurgte, om der ikke var mulighed for at få at vide, hvem havde i det område, inden for de par timer, talt i mobiltelefon. Og det kunne vel maks. være

omkring 20 personer i sådan et lille område på det tidspunkt. Det kan man ikke efter gældende regler.

Min pointe er så, hvis den samme mand i stedet for havde kunnet huske, at det var en hvid Golf, der startede med forbogstaverne KL, så kunne man gå ind i politiets motorregister og fundet ud af, at dem fandtes der 719 af i Danmark, og så kunne man have sagt, hvilke af dem opererer i Nordjylland. Og så kunne man have opsøgt 150 mennesker og afhørt dem om, hvem havde været hvorhenne lørdag nat. Alt det fuldstændig legalt ifølge retsplejeloven.

Det andet indgreb, som måske havde drejet sig om 15 eller 20, om de havde talt i mobiltelefon, det har vi forbudt eller i hvert fald ikke tilladt. Altså, der er jo i virkeligheden ingen sammenhæng. Er det ikke sådan, at vi indimellem er meget bange, fordi det er noget nyt? Altså den der naturlige, undskyld udtrykket, konservatisme, som der tit er: Alt nyt det er nok noget, der er farligt. Så er der en frygt også indimellem, bare fordi det er nyt, selv om indgrebet i virkeligheden er langt mindre end traditionelle efterforskningsmetoder?

**Eva Smith:**
Jeg ved ikke helt, om jeg er enig med dig i, at indgrebet er mindre. Jeg kan godt se, at politiets arbejde er mindre, men jeg ved da ikke rigtigt. Altså der kommer en og ringer på min dør og siger, "du har en hvid bil med KL sådan og sådan, og hvor var du"? Det kan jeg jo så svare på, om jeg så må sige, og det er, hvad det er. Men at nogen aflytter min private samtale...

**Helge Adam Møller** (KF):
Undskyld, nej, der er jo ikke tale om at aflytte en privat samtale, det kan man jo ikke, der er kun tale om, at man kan gå ind via de private selskaber og få at vide, den mobiltelefon har talt på det tidspunkt. Det er ligesom med Kurt Thorsen, der er jo ingen, der har aflyttet hans samtaler, men man kan konstatere, hvor hans mobil-telefon har sendt på forskellige tidspunkter mange år tilbage. Så det er derfor, jeg mener, indgrebet er jo langt, langt mindre end at gå ud og blive afhørt, hvor var du henne i din bil på det tidspunkt, men det må man ikke.

**Eva Smith:**

| |
|---|
| *Vi reagerer nok stærkere over for det nye. Men det er jo politikernes opgave at tage stilling.* |

Altså så misforstod jeg, men så er jeg da for så vidt enig med dig i, at det nok har noget at gøre med, at - du har nok ret i - at det er nyt for os, og vi kan ikke rigtig forstå det, vi kan ikke have med det at gøre, vi kan ikke overskue, hvad konsekvenserne er af det. Det har nok noget med det at gøre. Men det er vel jer, det

er nyt for, kan man sige. Det er vel jer politikere, der kan gøre noget ved det der, det er sådan set ikke politiet, der kan gøre noget ved det.

**Troels Ørting Jørgensen:**

*Ny teknik giver ikke forskel i indgrebet. Men der er en berøringsangst over for ny teknik.*

Jeg kan bare føje til, at jeg er enig med Eva Smith, at jeg tror, at bolden ligger hos politikerne, fordi der er jo ikke forskel i indgrebet, synes jeg. Vi har bare fået nogle andre muligheder, og dem skal vi selvfølgelig på alle mulige måder efter jeres direktiver udnytte eller afskrive.

Men der er efter min bedste overbevisning en vis berøringsangst i forhold til at lave indgreb på nye og ukendte områder, hvorimod det gammelkendte fingeraftryk, det er jo så enkelt, det har vi kendt i 100 år, så på den led tror jeg, du har ret.

**Per Helge Sørensen:**

*Ny teknik gør overvågning langt mere effektiv. Derfor er der god grund til at forholde sig ekstra kritisk til de nye teknikker.*

Ja, i forhold til, hvor indgribende det er. Nu var vi jo så heldige, så den forbrydelse blev begået i en lille nordjysk by, kan jeg forstå. Hvis den var blevet begået nede på Vesterbrogade, så havde der måske været 20.000 mennesker på den liste af folk, der havde haft en mobiltelefon tændt i nærheden af gerningsstedet, og så var forholdet måske lidt anderledes.

Og derudover synes jeg også, der er det at sige til det, at det med mobiltelefoner er muligt at gøre det her langt mere effektivt, langt mere systematisk end ved brug af vidner. Og det vil sige, at der også er et vist behov for at begrænse brugen af det her efterforskningsmiddel, fordi det kan bruges med langt færre omkostninger og langt mere effektivt.

Og derfor kan man frygte, at det vil blive langt mere udbredt end netop at gå efter vidner, så man skal ud og snakke med folk, der har hvide Golfer. Så der er nogle situationer, hvor det er mere indgribende, fordi det simpelt hen rammer langt flere mennesker, og så kan det bruges langt mere systematisk. Og derfor synes jeg, der er en vis grund, ud over konservatisme, til at behandle det på en anden måde.

**Peter Blume:**

*Når først vi har accepteret en form for overvågning kommer vi ikke af med den igen. Ville vi mon få et fingeraftryksregister, hvis vi skulle vælge i dag?*

Jeg synes, det er en god og rigtig pointe sådan set. Fordi dette med, at vi engang har godtaget gammel form for overvågning, eller hvad man nu vil kalde det, meget ofte jo på en måde ligner, men blot er blevet mere effektivt måske eller har fået nye dimensioner med den nye teknologi.

Men den viser jo efter min opfattelse, at opmærksomhedsniveauet omkring beskyttelse af integritet, privatliv, eller hvad du vil kalde det, er større, end det måske var engang, for det første. Og det viser for det andet også, hvis vi i dag startede fra scratch og skulle diskutere, om politiet skulle have et fingeraftryksregister eller ej, så var diskussionen en helt anden, end dengang de fik lov til at få sådan et register. Det kan godt være, de fik det som i dag, men det ville være en helt anden diskussion, ligesom da vi havde diskussionen om DNA-profilerne.

Og det viser så, at opmærksomhedsniveauet er et andet, men viser også, at har du først givet en adgang til at anvende en bestemt type af kontrol eller overvågning, ja, så har vi den også for altid. Altså, jeg kan ikke forestille mig noget politisk parti, der vil stille sig op og foreslå, at adgangen til at bruge fingeraftryk skulle afskaffes.

**Jørn Bro:**

*Mængden beskytter mod misbrug. Politiet kan ikke afhøre 20.000 mennesker.*

Jeg vil godt kaste en enkelt lille bemærkning ind. Mængden beskytter imod misbrug og overvågning. Hvis der var tale om, at der var 20.000 samtaler, så er det uden interesse, for det kan man ikke få noget som helst ud af. Men hvis det drejede sig om, at det foregår i en lille jysk by kl. 12 om natten, onsdag nat, hvor det regner, så er de 4-5 mulige samtaler spændende. Så mængden beskytter imod misbrug.

**Tove Videbæk** (KRF):

*Der er flere bankrøverier i Danmark end i andre nordiske lande. Skyldes det dårligere kameraovervågning?*

Ja, det er så tilbage til bankrøverierne. Niels Crone Lyngkjær talte en del om det, og der vil jeg da spørge dig, fordi der var for et par dage siden i medierne blev omtalt en rapport, der viste, at der er langt flere banker, postrøverier i Danmark end i de øvrige nordiske lande tilsammen.

Og der vil jeg da gerne spørge: Skyldes det, at der er bedre eller mere kamera-overvågning i de øvrige nordiske lande, eller skyldes det meget mindre antal røverier i de andre nordiske lande, at man dér løser nogle grundlæggende problemer på en helt anden eller måske bedre måde, eller er det på grund af mere tv-overvågning?

**Niels Crone Lyngkjær:**

*I Sverige må bankerne foretage udendørs overvågning. Men det er ikke skyld i faldet i røverier.*

Det er således, i Sverige har man for 2-3 år siden, mener jeg, ændret lovgivningen, således at pengeinstitutterne har mulighed for at foretage udendørs overvågning. Men det er nu ikke det, der er skyld i, at antallet af røverier er faldet kraftigt i Sverige. Det er meget svært at svare kort på det spørgsmål, der er stillet her, der er mange faktorer, der gør sig gældende. De nordiske lande er forskellige på betalings-systemerne, betalingsmåder.

Tager man et land som Finland f.eks., der er det således, at store dele af befolkningen de betjener sig af kontooverførsler. De betjener sig ved hjælp af kort, der er ikke nær den kontantmængde i omløb i det finske samfund, som vi kender til her. Penge-institutterne er rimelig restriktive med, når der udbetales penge, der er ikke det behov for kontanter i Sverige eller i Finland, som vi har det her i Danmark. Vi er rimeligt atypiske i forhold til de andre tre nordiske lande på det område.

Men det er klart, at mentaliteten, det hænger også sammen med, hvor mange penge-institutfilialer er der i pågældende land. Sverige er et stort land, der er langt imellem pengeinstitutfilialerne. Og den måde at man ligesom har valgt at beskytte sig på i Sverige, som det er fremgået af aviserne på det seneste, der har nogle pengeinstitutter op gennem 1990'erne installeret udbetalingsautomater, som betjenes af kassererne, og det har så medført i hvert fald, at en del røverier de er så forsvundet fra penge-institutside. Det har ikke været så interessant for de kriminelle.

Vi må jo se i øjnene, at de kriminelle de bevæger sig ligesom efter - det ser vi også herhjemme - efter de tiltag, vi påtager. Jeg kan nævne et lille eksempel. Nu er disse tidsforsinkelseslåse jo inde i billedet og har været nævnt også, som i hvert fald et pengeinstitut og andre også så småt er begyndt at betjene sig af. Men det medførte jo ved et røveri oppe i Vestsjælland her i sidste uge, at så stillede to røvere udover med pistoler osv., så stillede de med et brækjern og en stor forhammer, fordi nu skulle de altså se, om de kunne slå denne her anordning i stykker.
I Sverige har man set det samme, ikke helt på den helt måde, men man har så set, røverierne er blevet flyttet over på pengetransporter. Det er i Sverige private selskaber, og de køres ofte om aftenen og om natten og sørger for den side af sagen,

og der har man så til gengæld et rimeligt stort antal. Hvor vi herhjemme, fordi vi beskytter os godt, der er vi fri for røverier mod pengetransporter.

Så der er mange forskellige ting, der spiller ind, når man skal kigge på de forskellige nordiske lande. Vi er trods alt noget forskellige i struktur og i de ting, der er foregået for at sikre sig. Vi her i Danmark har jo været meget interesseret i at have det åbne miljø, og det har altså også sin pris, fordi går man så sydpå i Europa, så er det jo oftest betydeligt sværere at komme ind i pengeinstitutfilialer. Det er det så ikke i Sverige, men de tiltag, de har gjort, har åbenbart gjort, at de kriminelle har søgt andre veje.

Sverige har så også i de sidste halvandet år været plaget af en del kraftige sprængninger af pengeautomater om natten, hvor kriminelle har forsøgt at få noget ud af det. Den største omkostning for sektoren derovre har formentligt været, at der er blevet ødelagt bygninger for gud ved hvor mange penge. Der er måske bare en enkelt sprængning, der har ødelagt for mellem 5 og 10 mio. kr., fordi bygninger og andet er blevet molesteret. Så det at sammenligne fra det ene land til det andet det er ikke bare lige sådan.

**Ordstyrer:**
Eva Smith, har man gjort sig nogle overvejelser fra Det Kriminalpræventive Råd i den her sammenhæng? Har du nogen kommentar til det?

**Eva Smith:**

| |
|---|
| *Danmarks placering indbyder måske til røverier.* |

Jeg var egentlig ikke klar over, at der var så stor forskel på de nordiske lande. Men jeg ville egentlig tro, at Danmarks geografiske placering også betød noget, fordi det synes da, som om der kommer en del fra udlandet, og der er det da nemmere at køre til Danmark, end det er at tage til Finland, om jeg så må sige, ikke? Så det ville jeg egentlig også tro havde en betydning. Men vi har ikke forsket nærmere i forskellen på de nordiske lande på det område her.

**Ordstyrer:**
Det er jo i hvert fald svært at lovgive om vores placering.

**Niels Crone Lyngkjær:**

| |
|---|
| *Kun få udenlandske bankrøvere i Danmark.* |

Ja, jeg vil godt sige om dette med udenlandske røvere. Det er trods alt begrænset, når vi ser på vores statistik. Det er da rigtigt, som det blev sagt på et tidspunkt, at vi

havde 221 røverier mod banker og sparekasser sidste år. Udviklingen på sådan et område vil jo altid bevæge sig i bølgedal.

Som politiet har sagt gennem årene til os - vi har jo et kontaktudvalg med politiet, hvor vi drøfter tingene løbende - og der har man jo flere gange sagt, at det hænger jo også sammen med, at nogle af dem sidder inde i en periode. Det hjælper også på statistikken. Men med hensyn til de udenlandske røvere der vil jeg sige, vi er gudskelov ikke belemret med, at der kommer særlig mange. Det er primært vore egne også visse andengenerationsindvandrere, vi ser, der beskæftiger sig i branchen indimellem.

**Knud Erik Hansen** (SF):

*Hvad har politiet egentligt brug for af oplysninger? Vil flere kameraer ved bankerne virkelig have en effekt?*

Det er jo fristende altid at have gode argumenter for at bruge teknikken til noget, og det var jo også det, som jeg hørt Ørting Jørgensen og Lyngkjær argumentere for. Men jeg synes godt, man kan stille nogle spørgsmål: Hvor meget er egentlig nødvendigt - også til jer? Fordi hvis vi tager det med at logge og gemme data, så er der jo mange tanker rundt omkring i Europa. Der er lande der tænker på, at nu vil de faktisk godt have gemt dataene i 7 år. I første omgang snakker man så kun om et år, ikke?

Men spørgsmålet til dig, Ørting Jørgensen, det er: Hvad har I egentlig brug for? Altså hvor langt? Fordi noget af overvågningen er jo også afhængig af, hvor lang tid man gemmer de her data. Hvis I skal lave overvågning, hvor lang tid har I faktisk brug for, at de der data bliver gemt? Har I brug for, at de bliver gemt 1 år, eller kan I klare jer med et par dage? - som det ene. Og det andet: Det, du snakker om, er det overvågning eller skanning af logning-filer efter dommerkendelse, eller har I brug for generelt at gå ind og se logning-filer?

Og til Lyngkjær: Altså jeg kan sagtens se, at man godt kan blive fristet til at have kameraer udenfor, hvis man er bankmand. Men jeg vil godt også spørge dig som bankmand: Hvor meget tror du faktisk, det vil betyde marginalt? Du er selv inde på det lidt i dit svar før - fra Sverige - at kriminaliteten så måske vil få en anden karakter som det ene.

Men også: Vil de kriminelle, hvis de vil ind i banken, ville de så ikke tage hætten på et andet sted, hvor de kan se, der ikke er kameraer, eller fornemmer, der ikke er kameraer? Hvor proportionaliteten i forhold til det, i foreslår, i forhold til den begrænsning af tyverier, som I forventer at kunne opnå ved at have kameraer udenfor?

**Troels Ørting Jørgensen:**

*Politiets adgang til logning kræver dommerkendelse, intet ønske om at ændre på det. Jo længere tid en log gemmes, jo mere kan politiet opklare. 3 til 6 mdr. er et fornuftigt leje.*

Jeg vil starte med at sige, at alt den logning, jeg taler om her, er efter forudgående kendelse fra retten. Politiet har ikke noget ønske om at få egen access til noget af det her. Det skal ske ved rettens kendelse, ligesom det skal på alle mulige andre områder.

Det, der bare er forskellen, det er, at de oplysninger, hvis de ikke er til stede, så kan vi jo få nok så mange kendelser, vi vil have. Men hvis I nu så sørger for ved logningsprocedurer, at de bliver tilvejebragt, så er det jo så igen et afvejnings-spørgsmål at så sige, hvor lang tid de så skal gemmes. Fordi det er jo et spørgsmål om, hvor mange forbrydere skal vi fange?

Hvis vi kun har det i én dag eksempelvis eller 3 dage, så skal vi være hurtigt ude af røret, om jeg så må sige. Så er beviserne jo forsvundet. Har vi 3 måneder eller 6 måneder, så giver det os mulighed for at opklare flere forbrydelser. Det er jo en afvejning, der dybest set er politisk i virkeligheden. Det er jo hensynet til privatlivets fred på den ene side og så opklaringsprocenter på den anden side.

Men mit eget personlige skøn det vil være, at et sted mellem 3 og 6 måneder er man nødt til at gemme de her log-files, for at der overhovedet er nogen reel mulighed for politiet til at bruge de her oplysninger til noget som helst. Det er den ene side af sagen. Og den anden side af sagen er, at der er også et mængdeproblem. De her lognings-files - der vil jo være nogle ting, det er helt umuligt at logge.

Altså de der meddelelser, der flyver igennem luften, som man bare har ved de der instant boards, hvor går man ind, og så trykker man »hej med dig«, og så kommunikerer man på den måde dér, deres kapacitet er simpelt hen så omfattende, at jeg tror ikke, ISP'erne har nogen jordisk chance for overhovedet at lagre dem. Det mener jeg ikke. Der er måske 500 millioner om dagen bare i USA alene. Så det kan ikke lade sig gøre.

Men Internet-trafikken i øvrigt - det kan lade sig gøre at logge den, og det er den, der er interessant, fordi vi skal huske på, at der foregår rent faktisk temmelig alvorlige kriminalitetsformer nu på nettet, som man politisk set er nødt til at tage op. Altså her er børneporno et af dem. Og der findes faktisk også alvorlige trusler, alvorlige krænkelser også af privatlivets fred.

Det kunne være dig, der blev hængt ud på alle mulige måder og med private billeder, og hvad ved jeg, og så gemmer man sig bag anonymiteten, fordi vi aldrig nogen sinde kan finde ud af noget som helst. Så der er en lang række forhold. Men jeg

mener helt præcist, logning ja. 3, gerne 6 måneder, og politiet skal have adgang til det efter dommerkendelse og ikke egen access.

**Niels Crone Lyngkjær:**

*Antallet af bankrøverier falder. Bankerne vil dog gerne have adgang til mere kameraovervågning.*

Det er da rigtigt, at hvor meget vil vi fange ved at få den adgang? Det er da et relevant spørgsmål. Altså skal vi tage udgangspunkt i de 221 røverier, vi havde sidste år, og vi er så heldige, kan jeg sige, at de tre første kvartaler i år har vist et fald på 20 pct., så det er vi jo kun taknemlige for i sektoren. Til gengæld er postvæsenet så væsentligt hårdere ramt. Så totalt set ligger post og banker og sparekasser på nogenlunde samme niveau som sidste år.

Men for os er det jo en vifte. Vi har jo gennem mange år installeret eller foretaget, eller brugt penge på installation af forskellige løsninger. Vi har i mange år haft foto-overvågning, fordi det var det, der var aktuelt gennem 1980'erne og gennem 1990'erne. Det er så en del steder ved at blive erstattet af videoovervågning, fordi video-overvågning, det er så det, der er tiden. Nogle steder har man en kombination af begge dele.

Vi har så det, der i dagligdagen kaldes de røde penge, og det er også en af mulighederne, vi betjener os af. Dernæst så har vi i visse områder andre tekniske løsninger, som vi ikke taler så højt om, fordi det rent faktisk er noget, som giver ganske gode opklaringsprocenter. Men det egner sig så bare ikke til at blive spredt ud over hele landet. Og der er det så som led i dette, at vi synes og føler, at hvis der er steder, det ville være interessant, når man vurderer helheden, at sætte udendørs overvågning op, så er det, vi føler, at den adgang ville vi meget gerne have.

**Peter Christensen:**

*Kriminalitet på nettet er flygtig. Så langvarige logs giver ikke nødvendigvis adgang til at opklare mere.*

Ja, Troels Jørgensen gjorde det jo meget klart sådan set, at en af de problemstillinger, som politiet har, det er, at det skal være nemt for politiet. Det, der er problemstillingen her, det er, at vi også skal diskutere, hvad der er acceptabelt for samfundet, og det er ikke nødvendigvis den samme hele tiden.

Og jeg vil gerne f.eks. lige præcis gribe fat i det eksempel, som Troels Jørgensen tog op i starten med børneporno. Altså forbrydelsen bliver jo udført i det tidspunkt, man tager nogle billeder. Og det betyder, at hvis man skulle forfølge den forbrydelse, så burde

man jo lave et kontrolsystem, der sørgede for en identifikation af hvert eneste kamera med datomærkning osv., hvis man skulle forfølge på det.

Det, som Troels Jørgensen går ind i, det er at sige, o.k. når vi så sender det over nettet, så har vi heldigvis nogle elektroniske spor, der kan knyttes til den her forbrydelse senere. Men hvis man gav det videre analogt, altså det vil sige gav det videre i hånden, så kunne man så ikke forfølge den. Og det gør jo ligesom, at vi ligesom må vise, hvad er det? Hvordan forfølger vi de her forbrydelser? Fordi det er ikke nødvendigvis Internettet, der er sagen i denne her sammenhæng.

Og det fører tilbage til den logning, der foregår. Logning er nødvendig en gang imellem, og jeg tror også, at man bliver nødt til i en kortere periode måske at have nogle logningsoplysninger af hensyn til efterforskningen, men som Troels Jørgensen også siger: Forbrydelser på nettet er meget flygtige. Og de er flygtig, sådan at sporene bliver meget kolde hurtigt. Det hjælper ikke noget med at have logs i lang tid, fordi så forsvinder de alligevel.

I den sammenhæng må man så sige, at det også ikke altid er troværdigt, hvad der står i loggen. Hvis jeg f.eks. kender Helge Adam Møllers IP-adresse, som er det, der identificerer én i loggen, så tager det mig to sekunder at ændre min IP-adresse til at være den anden, fordi at hvis jeg ved, at jeg overvåges, så bruger jeg selvfølgelig de samme tricks for at undgå at blive identificeret.

Så derfor må man vide, at hvis man indfører den slags ting, så ved man også, at der er nogle, der - ligesom når man har forsinkede låse - begynder at bruge værktøjer på en anden måde. Så gør man det selvfølgelig også for dem, der er interesseret i ikke bliver overvåget. Så man skal lige passe på med, hvad det er man får ud af at tage den slags beslutninger.

**Jørn Bro:**

*Bankrøvere kan identificeres, også når de bærer maske. Derfor er kameraer gode til efterforskning*

Ganske kort: Pengetransportrøverierne er nået til Danmark. Vi har to store i min kreds på i alt 52 mio. kr. Dem er vi ved at få opklaret. Og det gør vi næsten udelukkende på basis af de såkaldte masteoplysninger. Det andet, jeg vil sige, det er, at det er meget vigtigt, at man får fanget bankrøverne, fordi heri ligger der en meget væsentlig prævention. Det er stort set den samme gruppe, der begår de fleste bankrøverier til hver en tid.

Det er også blevet sagt, at hvis nu bankrøveren tager en maske på, så har vi ingen glæde af sådant et videokamera. Jo, masser. Man kan sagtens blive fældet på et par tennissko,

hvis de man matche i øvrigt. Så vi har meget glæde af disse videokameraer i vores efterforskningsarbejde. Det betyder ikke, at jeg er tilhænger af mange videokameraer. Men hvis de er placeret rigtigt, så er de meget værdifulde.

**Sandy Brinck** (S):

*Ønsker politiet både autorisation af ISP'er og adgang til log-oplysninger?*

Jeg får lyst til at gøre en kommentar til det, der blev sagt fra Per Christensen om Internettet. Hvornår er det, forbrydelsen sker med børneporno? Altså hvis jeg ikke er blevet helt misinformeret, så er Internettet faktisk desværre med til at skabe en ny slags forbrydelser i forhold til børnepornografi, fordi man simpelt hen - og undskyld mig, det her det er grimt - kan bestille live overgreb via webbet.

Og så er vi inde i en anden situation, synes jeg. Så Internettet bidrager også til, at vi ud over at få et nyt marked for børnepornografi også får nye forbrydelsestyper, som jeg nok synes er ret alvorlige. Derfor vi jeg godt også spørge Troels Ørting Jørgensen: I dit oplæg for nogen tid siden nævnte du både autorisationsordninger og spørgsmålet om at få logningsoplysninger. Er det ønsket at få den ene eller den anden, eller er det et ønske om at få begge dele?

**Troels Ørting Jørgensen:**

*En international rockerklub driver ISP i udlandet. Deri ligger et politiske misforhold. Adgang til log-oplysninger er et klart ønske fra politiet.*

Altså med hensyn til logning er det et helt klart ønske at få den, og så kan vi så begynde at diskutere, hvor lang tid den skal vare. Og det er jo så jeres valg. Med hensyn til autorisationen så forholder det sig sådan, at det jo selvfølgeligt er et kontroversielt spørgsmål i princippet. Fordi hvis man nu siger, at en ISP han er en slags avis og stiller noget plads til rådighed for en avis for at få nogle oplysninger, noget informations-formidling, så har vi jo herhjemme ikke nogen autorisation for at være redaktør, vel?

Men omvendt, så har man jo ved ophævelse af det udmærkede statsmonopol liberaliseret hele televerdenen, og vi har jo så også gjort det muligt for allehånde mennesker selv at være ISP'ere. Og da vi nu er afhængige af, at de logningsoplysninger, som vi forhåbentligt får, de ligger hos ISP.

Hvis nu det er A/S Fup og Svindel, der er ISP, fordi det kan han bare gøre, han kan godt gå ud og købe det, det er ikke noget problem. Og så lover han selvfølgelig på tro og love, han nok skal overholde logningsforpligtigelserne, så han putter det direkte i makulatoren. Fordi han er fuldstændig ligeglad, for han får måske en bøde på 1.000 kr. for ikke at opbevare det, eller hvad ved jeg?

Så har vi altså et problem, hvis en hvilken som helst kan gå ind og være i ISP, altså autorisationen, og man skal være autoriseret bare for at være dørmand henne på NASA. Det kræver en autorisation. Men det gør det ikke her. Igen vender jeg tilbage til problemstillingen omkring stadepladsen, fordi det kræver altså, at man faktisk gør sig stor umage oppe på Københavns Rådhus for at få sådan en stadeplads.

Men det andet - altså man kan blive ISP uden noget som helst andet end at have en god tegnebog. Og deri ligger der efter min mening et politisk misforhold, som I jo skal drøfte og diskutere hensigtsmæssighederne af. Jeg kan jo bare som fagmand sige, at jeg tror, at det her projekt giver anledning til problemer. Jeg kan sige, at der en global rockerklub, der driver ISP-virksomhed i lande - heldigvis ikke i Danmark endnu, men i udlandet - og jeg tror ikke, vi får meget ud af at komme op og spørge om noget som helst deroppe.

**Sandy Brinck** (S):

| |
|---|
| *Hvad skal en autorisation af ISP'er indeholde?* |

Så bare lige for at blive klar over det. Sådan en autorisationsordning, hvad ville den skulle indeholde, for at vi netop slipper for, at det så er ISP-fup-og-svindel? Kan du give nogle stikord på, hvad det så måske er, vi skulle arbejde med i det tankesæt.

**Troels Ørting Jørgensen:**

| |
|---|
| *Kan ikke svare på stående fod. Men en form for bestalling kunne komme på tale.* |

Nej, det kan ikke på stående fod komme, men altså der må være noget på samme måde som på andre områder, hvor det kræver autorisation. Altså hvor man får en bestalling på en eller anden måde, der er der sådan nogle vandelskrav. Og dem kunne man jo så i hvert fald tage udgangspunkt i og sige, der skulle være noget der.

Det garanterer jo bestemt ikke for, at man ikke har puttet en stråmand ind. Det er jeg fuldstændig klar over. Altså sådan er det bare. Men det er der jo også andre steder, at man kan det. Men det, det kan give et signal om, det er jo, at det kan jo også på en eller anden måde legitimere. Altså så man ved, at der er jo også sidegadevekselerer og ordentlige vekselererfirmaer også, ikke?

Og der kan man altså også her tale om, der kan være sidegade-ISP'er, som man pr. definition ved er sådan, at hvis man i øvrigt er borger, så vil man ikke benytte sig af deres tjenester eksempelvis. Det er en vanskelig afvejning, men der mener jeg, man bør finde afsæt i de eksisterende autorisationsordninger, hvis man vil drøfte den sag.

**Helge Adam Møller** (KF):

*Er et overvågningskamera værre end en betjent?*

Det er en opfølgning på det spørgsmål, Knud Erik Hansen havde før vedrørende disse eventuelle overvågningskameraer uden for banken, der kan kigge 50 m til hver side, og inden man kommer ind i banken, hvor man er overvåget.

Hvis vi nu tænker os, at vi var så rige, at vi havde et par tusind ekstra betjente og sagde: Hver dag så stiller vi en betjent op foran banken fra kl. 9.00 til kl. 15.30, og de lukker. Og han stod ude på trappen, og han kan kigge 100 m til højre, og han kan kigge 100 m til venstre og 20 m frem og se alle, der nærmer sig banken, om der er nogen, der trækker hætter på eller virker mistænkelige, så tror jeg, stort set alle ville sige: "Det var dejligt".

Men det har vi bare ikke råd til, for det koster 300.000 kr. pr. mand om året, og det er mange tusinde kroner, der skal bruges. Nu har vi så en moderne teknologi, der kan erstatte betjenten, og som kun koster 5.000 kr. eller 10.000 kr. om året, og som ikke kan gøre noget som helst mere. Den kan også kigge 100 m til højre og 100 m til venstre og 10 m frem over til den anden side, og pludselig så laver vi det til et stort problem, men de ser nøjagtig det samme.

Mit spørgsmål er lidt i forlængelse af det før: Er det fordi, at betjenten - havde jeg nær sagt - det havde vi vænnet os til, eller hvis det var en vagtmand? Det synes vi er fint nok, han står der og kontrollere, fordi vi går jo kun i offentlige gade, og vi har ikke noget ondt i sinde, andet undtagen bankrøveren.

Men hvis det pludselig bliver erstattet af et kamera, som gør at vi kan gøre det langt billigere, så er der nogen, der siger: "Hov, nu er det pludselig meget betænkeligt". Og hvorfor er det betænkeligt lige uden foran trappen, når det ikke er inde i lokalet? Er der nogen, der kan give en forklaring på det?

**Niels Crone Lyngkjær:**

*En bevæbnet politimand ville holde mange røvere væk.*

Jeg er jo ganske enig i dit synspunkt. Det skal ikke være en almindelig vagtmand, for det tror jeg ikke er tilstrækkeligt. Det skal være en af politiets officielle, som har en skyder i lommen også. Det er nok det eneste, der nok rigtigt kunne afholde en stor del af de forbrydere, vi har med at gøre her fra at komme ind hos os.

Man må jo se i øjnene, at den kreds, der kommer hos os, der er det jo langt de fleste nogen, som formentlig ikke ville komme der, hvis der var en virkelig vagt udenfor, der

var bevæbnet. Om der ville komme nogen overhovedet, det ved jeg ikke. Vi har jo nok en lidt anden mentalitet, end hvis man kommer ned i Europa, hvor man ser mere hårdkogte forbrydere oftest.

Men det, man jo - og som jeg føler, er det meget interessante i den sag her og i diskussionen - det er jo, at der er ingen, der tænker på de ofre, på de medarbejdere, det her går ud over. Man skal gøre sig én ting klart, at de mennesker, der bliver udsat for røverierne, de bliver altså præget af det i lange perioder. Nogle bliver sgu præget af det resten af livet.

Og i Sverige, kan jeg sige, der har man gjort op, at hvert røveri i gennemsnit koster den pågældende pengeinstitutfilial 600.000 kr., og det er ikke fordi, det er udbyttet som sådan, men det er altså de omkostninger, der følger med i kølvandet på medarbejdere i øvrigt, der er i filialen. På de, det er gået ud over, og hvad ved jeg. Så der er en stor pris, der betales for, at man ikke for os at se tager teknologien mere i anvendelse.

**Peter Blume:**

*Problemet er, at kameraet "husker" langt bedre end betjenten.*

Jeg vil blot sige ganske kort, at det er rigtigt, at kameraet ser det samme som denne her udmærkede betjent, men så kan man sige, at kameraet husker på en helt anden måde end den udmærkede betjent sandsynligvis husker. Det er så et af problemerne.

Det andet er, kan man sige, det er jo ofte diskuteret - og man har jo selv oplevelsen, når man er netop i Sydeuropa og sådan nogle steder - at det, at der står en vagt eller to, som måske er en privat vagt, det er ikke nødvendigvis politiet, med diverse synlige våben ofte jo i den slags lande, på en måde giver det tryghed.

På den anden side så giver det måske også det modsatte, og selv om jeg gerne vil se - det er der jo andre, der gerne vil - mere synligt politi, som man jo taler om, så er man måske heller ikke interesseret i at se politi overalt. Altså der er jo stadig hele tiden sådan en afvejning af, hvad vi er interesseret i, og hvor langt vi vil gå.

**Knud Erik Hansen** (SF):

*Hvilke modtræk laver forbrydere mod politiets overvågning?*

Ja, det var en opfølgning på den kommentar, Peter Christensen havde - og som er et spørgsmål til Troels Jørgensen, fordi det, der var budskabet i Peter Christensens spørgsmål, det var, at vi oplever, at hvis vi laver de her foranstaltninger, at så dem, der vil lave forbrydelser, har jo modtræk. Så jeg vil godt spørge dig: Hvad oplever du af modtræk, som gør, at jeres forfølgelse efter elektroniske spor eller lignende bliver

besværlige og måske i nogle tilfælde umuligt? Kan du give nogle eksempler på, ud over det Peter Christensen nævnte, hvor det bliver besværligt for jer, fordi man laver modtræk?

**Troels Ørting Jørgensen:**

*Nemmest af fange de dummeste forbrydere. De rigtig smarte tager modtræk og er langt sværere at fange. Måske vil politiet bede om nye muligheder for at løse de besværligheder.*

Internettet er som skabt til anonymitet, og den globale verden og de meget forskellige retsregler, der er, gør, at det er ufatteligt nemt at skjule sig på Internettet. Og der er jo også en vis kvalifikation. Og man kan sige, at hvis man kigger på kriminaliteten sådan generelt, så er det jo altid nemmest at fange de dummeste, og det er jo det, vi ofte er bedst til - om jeg så må sige.

Men produktudviklingen – sofistikeringen inden for kriminaliteten - er jo også til stede, både blandt dem, man kan sige, der er de mere traditionelle organiserede kriminelle, altså dem der skjuler mennesker, narko, kvinder eller andet. De kommunikerer jo. Det gør de via Internettet, via ip-telefoni. Jeg kan jo på ét sekund oprette et telefonnummer i New York via Internettet, hvor man kan indtale en besked til mig elektronisk, som jeg så kan shuffle fire gange rundt om jorden, inden jeg aflytter den et andet sted. Det er ikke noget problem. Der er hele problematikken, altså hele den der med, hvor man udgiver sig for at være en anden, og så findes der en masse proxy-modeller, der gør, at det næsten er umuligt.

Men fordi det er vanskeligt, skal det jo ikke få os til som samfund ikke at reagere over for alvorlig kriminalitet, og politiet har jo også en forpligtigelse til selv at udvikle sig og blive dygtigere og så gøre opmærksom på nye tiltag eller nye muligheder, der måtte være. Og alt afhænger jo af, hvad outputtet skal være. Hvad er et acceptabelt kriminalitetsniveau i det her land her? Og det er jo igen en politisk beslutning. Hvor mange skal vi fange, og hvor mange skal ryge igennem nettet?

Men der er ingen tvivl om, at netop udviklingen omkring Internettet og hele kommunikationen - eller hele krypteringsdelen - gør, at man altså er nødt til at være mere vaks ved havelågen. Men vi kommer måske også til på længere sigt at bede om nogle andre indgreb for at omgå de besværligheder, der er.

Det vil jeg da ikke afvise kan blive løsningen på det, hvis man vil. Men det er jo jer, der bestemmer i virkeligheden, hvor meget vi skal opklare. Og hvem er det egentlig, hvilke forbrydelser er det egentlig, vi skal opklare? Altså er det ham heroppe, vi skal fange? Eller er det bare ham dummernikken, som render rundt og så en eller anden narkoman henne på hjørnet, som skal have til sit næste fix, ham kan vi sgu sagtens fange, ikke?

Han er jo sådan relativ eksponeret. Eller er det andre i det kriminelle hierarki? Og det er jo den afvejning, I skal komme med.

Men jeg kan sige, vi gør, hvad vi kan for at blive dygtige nok, og indimellem er det bare ikke nok, så kræver det, at vi kommer til jer og beder om nogle reguleringer af retsplejeloven, og det håber vi så på, vi kan gøre så velunderbygget, så I synes, det er en god idé. Men det er jo en politisk afvejning til syvende og sidst, men det er rigtigt, hvad Peter siger: Der er gode muligheder.

**Eva Smith:**

*Overvågning overalt vil nok føre til en del opklarede forbrydelser. Men der skal trækkes en grænse.*

Jeg vil bare sige til det der, Helge Adam Møller spurgte om, hvad er egentlig forskellen på i og uden for banken. Altså forskellen er jo, at du kan selv bestemme, om du vil gå ind i banken eller ej, ellers så går du bare på fortovet tilfældigvis forbi en bank.

Og det er jo jeres valg, hvor I vil sætte grænsen, fordi man kan også sige: Vi kan sætte videokameraer op over hele byen, så ville vi nok kunne opklare en hel del vold og sådan noget. Men jeg tror nok, de fleste ville synes, det var at gå for vidt, ikke? Så et eller andet sted skal der trækkes en grænse, og det kan jo nemt blive en glidebane, hvis vi først begynder at sige: ”Jamen lad os lukke op”.

## Overvågning med et efterretningssigte

**Ordstyrer:**
Ja, så går vi i gang igen med den sidste blok her inden frokost, og det er overvågning med et efterretningssigte. Og den første, jeg her skal give ordet, det er politimester i Glostrup, Jørn Bro, værsgo.

**Jørn Bro**, Politimester i Glostrup, tidligere souschef i Politiets Efterretnings Tjeneste

*PET's interesse og målområder bestemmes af ministeriet og i sidste instans regeringen. PET's registre er fortegnelser over de personer, organisationer og emner, som forekommer i PET-sager.*

Tak for det. Jeg beklager, at jeg må først skuffe forsamlingen. Vore to meget beskedne efterretningstjenester beskæftiger sig ikke med - som det siges - at overvåge borgerne. Det har de hverken direktiver til, og de har heller ikke ressourcer til det. PET, som det her drejer sig om, har til opgave at overvåge, forebygge, modvirke og forhindre foretagender og handlinger, der må antages at rumme en fare for rigets selvstændighed og sikkerhed og den lovlige samfundsordning.

Som sine virkemidler har man nøjagtig de samme virkemidler som det øvrige politi, og det vil sige, at PET også er omfattet af retsplejeloven. Særlig er der i den givne sammenhæng grund til at pege på bestemmelserne i retsplejelovens kapitel 71 og indgreb i meddelelseshemmelighed og observation.

Her er der mulighed for at indhente kendelser til aflytning af rum, telefon samt det man kalder teleoplysninger samt til brevåbning og brevstandsning, og der er givet regler for observation, hvis man skal observere inden for et område, der ikke er frit tilgængeligt og ved hjælp af særlige virkemidler. Alle disse muligheder kræver retskendelse, som igen skal hvile på nogle ganske sådan kvalificerede krav.

Retsplejelovens indgående regelstyring er udtryk for den store vægt, man i det danske samfund lægger på den enkelte borgers retssikkerhed. På årsbasis meddeler retterne i hele landet ca. 1.700 kendelser om indgreb i meddelelseshemmeligheden. Heraf er ca. 800 telefonaflytningskendelser og ca. 900 kendelser om det, man kalder teleoplysning.

Ca. 900 af disse kendelser af både den ene og den anden kategori relaterer sig til narkosager, og i denne sags kategori er der hyppigt tale om bandeforbrydelser, hvor den enkelte efterforskning let fordrer 5-10 kendelser. Det samme gør sig gældende i øvrige grove sager, hvor man overhovedet anvender disse virkemidler. Da telefonaflytning og efterfølgende bearbejdning af disse teleoplysninger er overordentlig ressourcekrævende,

siger det sig selv, at politiet - herunder PET - kun i meget begrænset omfang gør brug af disse virkemidler.

Og når man sammenholder antallet af kendelser om indgreb i meddelelses-hemmeligheden med antallet af både faste telefoner og de mobile telefoner og den umådelig mængde samtaler, der daglig føres over disse apparater, med antallet af på den anden side kendelser, så synes jeg, der somme tider er tale om en vis proportions-forvrængning, når man bruger begrebet »overvågning« i forbindelse med politiets - herunder PET's - muligheder for at bruge disse virkemidler.

PET's interesse og målområder bestemmes af ministeriet og i sidste instans regeringen, idet man kan sige, at PET beskæftiger sig kort og godt med de områder, som regeringen og de øverste statsmyndigheder har et nødvendigt og legitimt krav på at være ordentligt informeret om, således at der kan træffes de fornødne foranstaltninger til beskyttelse af borgerne og samfundet.

PET's registre, som det hyppigt drejer sig om, er fortegnelser over de personer og organisationer og emner, som forekommer i PET-sager. Tidsperspektivet er langt i den slags sager, derfor er de undertiden mere omfattende end i andre sager. Men jeg vil lige nævne, at det, man kalder »navneregisteret« i en middelstor drabssag let løber op i en 2.000-3.000 navne.

Borgernes retssikkerhed sikres dels igennem tjenestens instrukser, ministeriets tilsyn og igennem det såkaldte Wamberg-tilsyns opgave og endelig igennem, hvad er meget vigtigt, det parlamentariske tilsynsudvalg. PET beskæftiger sig ikke med at foretage overvågning af borgerne. Det ville kræve ganske andre rammer, ganske andre regler, og et meget, meget større personale.

Elektronisk indhentning har jo været kendt siden første verdenskrig. ECHELON er muligvis en af de måder, det gøres på, men det er vigtigt at lægge mærke til, at kinesisk, russisk, iransk, irakisk osv. udfører nøjagtig de samme lyttetjenester. Så om man råber ud i verdensrummet, det bliver, og det kan opfanges.

**Ordstyrer:**
Tak til Jørn Bro, og den næste, det er Birgitte Kofod Olsen, Det Danske Center for Menneskerettigheder.

**Birgitte Kofod Olsen**, lic.jur., seniorforsker, Det Danske Center for Menneskerettigheder

*Når Folketinget vedtager en lovgivning, der giver adgang til overvågning, skal menneskerettens krav om klarhed i lovhjemmelen, præcisionen i lovhjemmelen, det lovlige hensyn og nødvendigheden være til stede.*

Jeg har i det skriftlige oplæg, der findes i mappen, redegjort for de principper, der danner grundlag for den menneskeretlige beskyttelse, der er i privatlivet, og de problemer, der særlig knytter sig til overvågning med efterretningssigte.

Derfor vil jeg benytte lejligheden til nu at illustrere den menneskeretlige privatlivs-beskyttelse med en dom fra Menneskerettighedsdomstolen i Strasbourg. Det er en sag, som er afsagt den 16. februar år 2000, og den drejer sig om en svejtsisk forretnings-mand, hr. Armand. Han importerer og sælger apparater til fjernelse af uønsket hårvækst, og de her apparater, dem annoncerer han i svejtsiske blade og aviser, og en dag er der en kvinde, der kontakter ham.

Hun sidder på den dengang sovjetiske ambassade i Bern og ønsker altså at købe et af de her apparater. Telefonsamtalen, den bliver aflyttet af den offentlige anklager, som videregiver oplysningerne til Politiets Efterretningstjeneste i Kanton Zürich. Den offentlige anklager beder efterretningstjenesten om at undersøge sagen nærmere.

Hr. Armand, han bliver derefter registreret i et indeks om national sikkerhed, fordi han bliver betragtet som en person, der har kontakt til den sovjetiske ambassade. Det her sker i 1981. I 1990 var der en offentlig debat i Svejts om det her indeks om national sikkerhed og om det rigtige i og det rimelige i, at en hel masse borgere var registreret der.

Hr. Armand indbringer sin sag forskellige steder i det nationale system, bl.a. til ombudsmanden, og i 1995 indbringer han sagen for Kommissionen i Strasbourg, og den går så videre til Menneskerettighedsdomstolen. Der er to spørgsmål i denne her sag, som er aktuelle for os, når vi taler om overvågning, og det er dels spørgsmålet om telefonaflytning, og så spørgsmålet om registrering af data om hr. Armand og den efterfølgende opbevaring af de oplysninger.

Domstolen udtalte om telefonaflytningen, at det er at betragte som et indgreb i en beskyttet rettighed. Det er et meget alvorligt indgreb i privatlivets fred. Derpå går de videre til at se på, om betingelserne for at foretage sådan et indgreb er til stede. Og de betingelser, dem kan I læse nærmere om i papiret, og jeg kan bare kort sige, det er et krav om lovhjemmel, det er et krav om lovligt hensyn, og det er et krav om nødvendighed.

Og domstolen benytter lejligheden til at konstatere, at lovhjemmelskravet ikke blot er et krav om, at en lovhjemmel skal være til stede. Den skal også opfylde nogle kvalitetskrav. De kvalitetskrav de består af kravet om tilgængelighed. Hjemmelen skal være tilgængelig for den berørte person, og effekten af anvendelsen af den lovhjemmel skal være forudsigelig for den person, der berøres af indgrebet. Det betyder, at en lovhjemmel skal være formuleret med tilstrækkelig klarhed og præcision, sådan at enhver borger kan indrette sin adfærd efter lovreglen.

I den her konkrete sag der fastslår dommen derudover, at loven skal sikre, at borgeren beskyttes mod vilkårlige indgreb. Når man rejser spørgsmålet om vilkårlige indgreb i en efterretningsmæssig sammenhæng, så er det, fordi at risikoen selvfølgelig er særlig stor, fordi vi har et krav om hemmelighedsholdelse af nogle af de efterforskningsskridt, som efterretningstjenesten foretager. Og det er nødvendigt, for ellers vil formålet forspildes. Og det er anerkendt af domstolene.

Men på grund af den her øgede risiko for vilkårlighed så stiller man altså ekstra strenge krav til beskyttelse af borgeren. Man siger, at lovhjemmelen skal følge nogle fast angivne mål. Og det skøn, der udøves på baggrund af lovgrenen, det skal være styret af faktorer, som også er åbenbare for borgeren. Domstolens konklusion i den her sag det er, at den schweiziske lovhjemmel ikke er tilstrækkelig klar, og at det ikke er tilstrækkeligt klart at se, hvordan skønnet udøves og hvad effekten af det er.

De konkluderer også, at registreringen af Armand - der står blot om hans navn, at han driver den her forretningsvirksomhed og har haft en kontakt til ambassaden. Det er også en krænkelse af hans privatliv, ligesom den efterfølgende opbevaring er. Og lovhjemmelen anses heller ikke i den sammenhæng for tilstrækkelig klar.

Så det, jeg lige kan slutte med at sige, det er, at det, der er relevant at se af den her dom, det er, at vi har altså et generelt krav til lovgivningen, som I skal være opmærksom på som politikere, nemlig at når I vedtager en lovgivning, der giver adgang til overvågning, så skal menneskerettens krav om klarhed i lovhjemmelen, præcisionen i lovhjemmelen, det lovlige hensyn og nødvendigheden være til stede.

Derudover så skal man også være opmærksom på, at når man anvender den her bestemmelse, som I vedtager den bliver anvendt af politi og efterretningstjeneste, så skal de samme krav være opfyldt i den konkrete situation. Og det betyder så især, og det har jeg skrevet mere om i papiret, at kravet om nødvendighed og proportionalitet i den konkrete situation skal være opfyldt.

**Ordstyrer:**
Ja, tak til Birgitte Kofod Olsen. Og værsgo til Peter Christensen.

**Peter Christensen**, CNDO, Co-operative Network and Data Operation

*Krypteringsværktøjer er et forsøg på at skjule den kommunikation, vi foretager frem og tilbage mellem to parter. I dag bruger man kryptering i almindelige samhandelsfunktioner inden for Internettet, og til at skjule de meddelelser, som man ikke synes, at andre skal læse. Men meget amerikansk software er forberedt på at kunne snakke med amerikanske efterretningsvæsner.*

Ja, jeg skal koncentrere mig lidt om de overvågninger i efterretningssammenhæng, som ikke er sket på baggrund af en retskendelse. Og det går selvfølgelig typisk fra overvågning foretaget fra, kan man sige, ikke dansk grund.

Det bedste eksempel, vi har, det er sådan set Echelon, som EU jo i en rapport i 1999 trak frem som et af de eksempler på overvågning af vores satellitkommunikation, som eksisterer. Og det er rigtigt, som det er sagt tidligere, at det var ikke kun er den engelsk-talende version, nemlig Echelon, som er blevet ramt i den rapport, det var selvfølgelig også Tyskland og Frankrig, som har forsøgt at lave de samme systemer, men på baggrund af deres dækning geografisk selvfølgelig ikke har kunnet opnå samme effektivitet.

Og den netop udgivne rapport fra EU-Kommissionen, som tager udgangspunkt i den rapport i 1999, har netop også konkluderet, at EU-landene ikke bør indgå i det samarbejde, som Echelon er udtryk for, og det gælder selvfølgelig alle EU-lande, og at eneste svar på Echelon og andre er krypteringsværktøjer.

Krypteringsværktøjer er et forsøg på at skjule den kommunikation, vi foretager frem og tilbage mellem to parter. I dag bruges det på Internettet. Hvert eneste køb. Der er ikke nogen, der vil købe en Folkevogn over nettet, hvis ikke man er sikker på, hvem der har sendt meddelelsen, hvad der stod i meddelelsen, eller hvem det jo egentlig er, der modtager den. Og derfor bruger man kryptering i almindelig samhandelsfunktioner inden for Internettet.

Det, der sker også nu, det er så, at man bruger kryptering, som er at skjule de meddelelser, som man ikke synes, at andre skal læse. Og det kan være alt fra, kan man sige, personlige ting til andre personer, eller det kan være meddelelser, som man af en anden årsag ikke synes, at offentligheden skal have kendskab til.

Der er ingen tvivl om i dag, at alle meddelelser, der går specielt via satellittransmission, og det vil sige typisk over Atlanten, det vil blive opsamlet, og man vil kunne mønster-genkende ting. Og når jeg siger mønstergenkende, så er det selvfølgelig, fordi at man kan jo ikke, selv om man har store systemer, læse alle de her meddelelser igennem uden at have et eller andet at gå efter, men på et tidspunkt var det sådan, at amerikanske National Security Agency havde den datakraft, der svarer reelt til selve Internettet for netop at kunne mønstergenkende i de her e-mails.

Så der er ingen tvivl om, at den bliver opsamlet. Det, der er problemstillingen, det er selvfølgelig, hvorfor de bliver opsamlet. Og det har man så selv fra amerikansk side sagt, at det var for at lave, kan man sige, efterretningsvirksomhed, delvis på grund af selvfølgelig almindelig efterretningsvirksomhed, men delvis også på grund af industrispionage.

Argumentet var, at den europæiske industri generelt brugte en form for system, så man fik nogle opgaver, som amerikanerne fik en næse forbi. Så konklusionen på det det er sådan grundlæggende, at hvis man skal sørge for ikke at blive efterretningsovervåget i denne her sammenhæng, så må man indføre nogle værktøjer, som gør, at man kan vælge ikke at blive det, og det vil være krypteringsværktøjer.
Det ville være smart at bruge de samme krypteringsværktøjer, som man bruger i almindelig e-handel, så der er transparens her. Der er så et enkelt problem. Det er, at meget amerikansk software, i hvert fald de store, har en tendens til også, kan man sige, at have forbindelser til NSA i dag, som gør, at man ikke altid kan være sikker på, hvad det er, der kommer ud af det.

Faktisk har både og IBM og Microsoft erkendt, at de har ting i deres software, som på forhånd er forberedt på at kunne snakke med NSA. Og det gør selvfølgelig, at man på europæisk plan burde overveje at lave sit eget system eller sine egne værktøjer, så man er sikker på, hvad man får ud af det, når man krypterer.

**Ordstyrer:**
Ja, tak til ekspertpanelet. Og den første, der har bedt om ordet, det er Knud Erik Hansen.

## Spørgsmål fra Folketingets spørgepanel

**Knud Erik Hansen** (SF):

*Gør digital teknik det ikke langt nemmere at overvåge?*
*Er menneskeretskonventioner tidssvarende på dette område?*
*Kan Open Source software hjælpe på sikkerheden?*

Jeg har ét spørgsmål til hver af jer. Først til Jørn Bro:
Jeg forstod på dig, at I ikke har ressourcer til at aflytte generelt. Og det kan jeg sådan set godt forstå. Altså hvis I skal have det samme, som NSA har, så er det ganske store ressourcer, I skal have, hvis jeg være lidt polemisk, ikke? Men det kan jeg sagtens acceptere.

Men det, jeg godt vil spørge dig efter, det er: Er det ikke rigtigt, at nu man går fra analog kommunikation til digital kommunikation, faktisk gør det meget mere muligt for

jer at skanne? Altså I kan faktisk med meget færre ressourcer gå ind og skanne den kommunikation, der foregår, og bruger I ikke det, altså at det faktisk er mindre ressourcekrævende at skanne elektronisk kommunikation, når den er digital?
Og til Birgitte Kofod Olsen: Jeg vil godt spørge efter, når vi snakker om menneske-rettigheder og de konventioner, vi har - nu nævnte du nogle eksempler på, hvorledes man kunne bruge dem - er de i virkeligheden tidssvarende? Altså i forhold til den teknologi, hvor vi oplever en teknologi, hvor vi sender åbne postkort, vi har en teknologi, hvor vi har persondata gemt i nogle store systemer, som er svære at kontrollere, er der ikke brug for en anden type konventioner eller aftaler landene imellem, som sikrer, at man kan beskytte sig? Altså er de eksisterende regler er de gode nok til i virkeligheden - internationale regler - til at sikre, at landene laver noget effektivt for at beskytte os?
Og til Peter Christensen: Du snakker om kryptering til at beskytte os. Altså min fornemmelse er, hvis man skal beskytte os, der er egentlig to svar til det, og du nævner selv det ene: Det er kryptering. Det andet det er, hvis man skal beskytte sig mod de bagdøre, så må man kræve, at man har systemer med åben kildekode, så man kan se det.

Men det, jeg synes, jeg oplever, når jeg ser på hele IT-udviklingen, det er, at den bliver hæmmet. Krypteringen er ikke kommet. Altså vi har fået alle mulige faciliteter på nettet, men af en eller anden grund så er krypteringen der ikke. Men det eksisterer teknologisk, men det er ikke udbredt. Så spørgsmålet er egentlig: Hvad skal der til for at få de her ting udbredt, sådan at de reelt bliver brugt, og hvad er det der hæmmer deres udbredelse?

**Jørn Bro**:

*PET har ikke udstyr mandskab eller ønske om at samle store mængder elektronisk data. 99 procent af befolkningen kan i bund og grund også være ligeglade med, om nogen lytter.*

PET har ikke hjemmel til og skal heller ikke have hjemmel til at foretage skanning eller det, man kan kalde elektronisk fisketur. Det ligger fuldstændigt uden for opgavesættet. Og man har overhovedet ikke kræfter at have udstyr til det, har heller ikke noget ønske om at få det. Hvis der skal være mening i det arbejde, der udføres af politiet og herunder PET, så gælder det i høj grad om at være selektiv og præcis i sin måludpegning og det, man arbejder med.

Det, der er det store problem nu om dage, det er, at hvis man skal ind på et givet område for at foretage en nærmere undersøgelse af nogle helt specifikke ting, så kan man inden for det elektroniske område let blive kvalt af en utrolig mængde data, og det samme som blandt en kæmpe fiskestime skal man finde en enkelt lille fisk. Jeg ser ikke nogen fare i det.

Derimod synes jeg nok, der er grund til at sige, at hvad der råbes ud i verdensrummet over mobiltelefoner og lignende, det bliver aflyttet masser af steder. Og jeg tror ikke rigtigt, at det kan forebygges, for hvis man finder en eller anden kode, så kan koden knækkes. Det har masser af lande arbejdet med siden Første Verdenskrig.

Så det giver falsk tryghed. Og 99,99 pct. af befolkningen kan være revnende ligeglad med i virkeligheden, om nogen lytter. Men vores beslutningstagere bør måske være en smule forsigtige med, hvad de råber ud over mobiltelefonerne i lidt for klart sprog.

**Birgitte Kofod Olsen:**

*Konventioner omfatter beskyttelse mod enhver form for dataindsamling og – anvendelse. Konventionerne er under stadig udvikling.*

Dit spørgsmål om, om konventionerne, menneskerettighedskonventionerne er tidssvarende: Altså så det er meget klart fra retspraksis fra Menneskerettigheds-domstolen fra Strasbourg , som arbejder med den europæiske menneske-rettighedskonvention, at det ligger, det er iboende i menneskeretten, at den er dynamisk. At konventionen, den europæiske menneskerettighedskonvention er tænkt som et levende instrument, har de udtalt, sådan så den kan tilpasses de behov, der er til enhver tid.

Så det betyder, at den privatlivsbeskyttelse, vi har i den europæiske menneske-rettighedskonvention, den er under stadig udvikling. Så der er ikke noget i vejen for, at vi anvender den på de problemstillinger, som er rejst her i relation til overvågning, selv om der er tale om anvendelse af midler, som man ikke kendte på det tidspunkt, da konventionen blev til. Så det ser jeg ikke som noget problem. Tværtimod kan man sige, at den måske er mere "up to date" og mere anvendelig i dag, end meget national lovgivning er.

Og dertil kommer, kan man også sige, at selv om man kan sige, at privatlivs-beskyttelsen, som den står i artikel 8 i den europæiske menneskerettighedskonvention, den kun omfatter privatliv, familieliv, korrespondance og hjemmet, så omfatter den altså også, har vi set fra praksis, personoplysninger. Så du har en beskyttelse af enhver form for dataindsamling og -anvendelse dér - en grundlæggende beskyttelse.

Så har du så særkonventioner om persondata fra Europarådet, og du har hele den EU-retlige regulering på persondatabeskyttelsesområdet, som skal ses i forlængelse af den grundlæggende beskyttelse af privatlivet. Så jeg synes ikke, der er behov for ny international regulering på det her område.

**Peter Christensen:**

*Problemer med udbredelse af individuel kryptering.*

Ja, kryptering. Jeg vil sige, jeg vil dele op i to dele, fordi at der er noget, der hedder gruppekryptering, kan man sige, og der er noget, der er individuel på kryptering. Gruppekryptering det er typisk det, som vi oplever, hvis f.eks. en a-kasse i dag skal kommunikere med sine afdelinger rundt omkring i landet. Så vil man typisk bygge det, der hedder et VPN-net, hvor man krypterer en tunnel over Internettet, så andre på Internettet ikke kan aflæse, hvad der foregår. Det gør man selvfølgelig af hensyn til medlemsoplysninger, men simpelt hen, fordi det er et krav fra myndighederne også. Man kan sige, alle andre organisationer kunne gøre det samme, og det viser jo også, at den dag, at politiet får midler til at kunne skanne den slags ting, så vil de organisationer, som de måske bekæmper, have lavet de samme tunneler. Det er bokse, der koster meget billigt eller meget lidt - 10.000 kr. stykket cirka - og det vil sige, dem kan man bare sætte op, så har man krypteret sin vej over Internettet, uden at man kan gå ned at kigge på, hvad det er.

Den anden side det er så den individuelle. Og der tror jeg helt klart, at vi har et problem med udbredelsen af krypteringen, både fordi at der er et vist rent brugermæssigt stort problem at bruge krypteringsværktøjer i dag. Der er også ikke altid en forståelse for, hvorfor man skal gøre det. Og det er klart, Maren i Kæret, der skriver til et eller andet familiemedlem har ikke behov for at kryptere. Det er der mange andre, der har - måske af hensyn til, at der er forretningsforbindelser eller andre ting, som gør, at man ikke synes, at hvem som helst andre skal kunne følge med.

Men i dag har vi ikke de fornuftige interfaces til, at det er udbredt. Og man kan så sige, at man har måske heller ikke altid tillid til de værktøjer, vi har. Og det er så et andet problem. Der kan man sige, at der havde vi måske en opgave i at stille nogle bedre værktøjer til rådighed og måske gøre noget mere pædagogisk for at motivere folk til at bruge det, hvis det er nødvendigt. For man skal også være opmærksom på, at det at bruge kryptering i privat sammenhæng er jo en reaktion mod noget. Så det kunne jo være, man skulle starte dér i stedet for.

**Knud Erik Hansen** (SF):

*Kan alle krypteringsprogrammer brydes - eller er der nogle, der er sikre?*

Jamen det var til Jørn Bro, altså du siger, at man kan bryde krypteringer altså, og også til Peter Christensen. Jeg vil godt spørge efter, i hvilket omfang kan man bryde kryptering - som det ene.

Og det andet synes jeg er der også et spørgsmål, det er: Det er klart, hvis man får et brev og har 10 dage til at bryde koden, så kan man, men hvis man skal bryde online, så er det vel en anden situation. Altså det at kryptere forhindrer i virkeligheden måske i praksis at man kan skanne. Det kan godt være, at man kan bryde den enkelte efter 10 eller 30 dage, men krypteringen må vel bryde det, at man kan skanne.

**Jørn Bro:**

*Tror ikke på, at der findes kryptering, der ikke kan brydes.*

Man har siden Første Verdenskrig arbejdet med problemet kodebrydning elektronisk. Og der er udgivet en meget stor litteratur om, hvad der foregik under Anden Verdenskrig. Jeg gætter på, der kommer en omfattende litteratur om, hvad der foregik under det, vi kalder den kolde krig.

Jeg tror, at man skal være varsom med at knytte alt for store forhåbninger til, at der findes krypteringsprogrammer, der ikke kan brydes. Det giver en falsk tryghed. De fleste brevkoder vil formentlig i dag kunne knækkes på et par timer. Det er muligt, at det vil tage lidt længere tid, hvis den er online, men det finder man ud af på en eller anden måde.

Der er et ganske klart behov for store statsforetagender og for regeringen og for store firmaer måske at kunne kode sin kommunikation. Men jeg har meget svært ved at se, at der for landets private borgere og for almindelige firmaer er nævneværdigt behov for at kunne foretage kodning, også fordi de vil kun være i stand til at kunne lave kodning, der vil kunne knækkes, hvis det er det, man ønsker. Det vil kun gøre opklaringsarbejdet vanskeligere.

Og så skal man lige være opmærksom på, at der, hvor man virkelig henter efterretninger ind, det er såmænd ved at rette sine lytteapparater imod den dagligdags trafik. Jeg gætter på, at i øjeblikket lytter amerikanerne intensivt imod alt, hvad der siges i taxaer, ambulancer, politi osv. inde i Kabul. Og jeg er helt sikker på, at når man overhovedet er i stand til at kunne udpege med nogen sikkerhed, hvem der var gerningsmanden til den store terrorhandling, så var det faktisk signalopklaring baseret på det, vi kalder masteoplysninger.

Så det er et virkemiddel, man ikke får nogen stat til at give fra sig. Men man bliver nødt til at indrette sig på, at det foregår, og træffe rimelige foranstaltninger imod, at særligt sårbare områder udsættes for aflytning. Og det gælder ikke mindst regering osv.

**Peter Christensen:**

*Meget af den kryptering vi bruger i dag er simpel at knække. Men det vil tage tid alligevel og det kan gøre det uinteressant at overvåge.*

Den krypteringsform, vi bruger f.eks. på mobiltelefoni i dag, den er forholdsvis simpel at knække. Den krypteringsform, som generelt anvendes af private i dag, den kan i hvert fald forsinke og måske helt afvise en dekryptering, men langt hen ad vejen vil den i hvert fald gøre den så uinteressant det, der kommer ud af det, fordi det ofte er »real time«, der er interessant. Det vil sige, forsinkelsen i sig selv gør, at man ikke får noget ud af det.

Og så er der selvfølgelig den kryptering, som i hvert fald i dag med de maskiner, vi har i dag, ikke kan knækkes, men selvfølgelig ad åre vil kunne gøre det, og det gør jo også, at man hele tiden forbedrer systemerne.

**Peter Landrock**, prof., adm. dir., Cryptomathic:

*Der findes koder, der anses for ubrydelige i praksis.*

Ja, nu er jeg jo med som krypteringsekspert. Så synes jeg, jeg var nødt til lige at sige nogle få ord. Jeg kommer ind på det praktiske i mit indlæg i eftermiddag, hvorfor det måske er sværere. Og jeg er enig med meget af det, Peter Christensen siger. Men jeg synes lige, jeg må slå fast, at der findes koder i dag, som er anset for praktisk ubrydelige. Det er ikke nemt at vise, at de ikke kan brydes. Fordi hvis man har ubegrænset beregningskraft, så kan de brydes.
Men vi benytter os f.eks. af metoder af rent matematisk karakter, som gør, at vi kan afgøre, vi kan slutte, at hvis man kan bryde den og den kode, så kan man løse et matematisk problem, som matematikere ikke har kunnet løse nogen sinde. Så derfor er det min ekspertvurdering, at der findes masser af praktisk ubrydelige koder i dag.

Jeg vil også i mit indlæg komme ind på det der med bagdøre. Men jeg vil lige sige, at i USA har det altid været tilladt at bruge stærk kryptering. Og Netscape kommer med source-kode, frigørelse af krypteringsalgoritmer, så det er muligt også for den almindelige borger at kryptere, stærkt kryptere, men der er nogle praktiske vanskeligheder, som jeg kommer ind på.

**Kristian Jensen** (V):

*Er det acceptabelt, at man skal kryptere for at have privat kommunikation?*

Det var sådan mere, når det praktiske er på plads, et moralsk spørgsmål om, det fra et menneskerettighedssynspunkt er tilfredsstillende, at man som borger skal bruge

kryptering f.eks., hvis man havde venner i Saudi-Arabien, i Afghanistan, i et af de lande, der er under overvågning nu, hvis man skulle kommunikere privat med vedkommende, så skulle være nødt til at bruge krypteringsværktøj.

Fordi jeg kan godt følge Jørn Bro i, at den almindelige dansker, der sidder og sender fødselsdagskort til moster Gerda over Internettet, har ikke den store grund for at kryptere. Men vi har jo en globaliseret verden, hvor man har kontakter i mange andre lande med mange andre forskellige indgangsvinkler, også til overvågningen, så er det ud fra et menneskerettighedssynspunkt tilfredsstillende, at kryptering er blevet så stor en del af debatten?

**Birgitte Kofod Olsen:**

*Borgene har ret til at kryptere deres kommunikation, men ikke ret til at kunne kommunikere uden kryptering.*

Jeg er nødt til at svare på det på en anden måde, fordi det er ikke sådan, så vi kan sige, at vi har en ret til kommunikere uden brug af kryptering, altså at vi skal have sikker kommunikation på den måde. Fordi overvågning er et redskab til også at sikre vores rettigheder, altså vi har en ret til effektiv efterforskning fra politiets side, og derfor skal der også være overvågning. Og det var det, jeg sagde før, at den overvågning skal så leve op til nogle forskellige krav. Det behøver jeg ikke at gentage.

Men noget andet er, om man kan vende spørgsmålet lidt om og så sige, om vi ikke har en ret til at kryptere vores kommunikation, og det synes jeg nok, man må sige, at vi har. Altså det kan ikke nytte noget, at man laver for mange begrænsninger i adgangen til at kryptere for private borgere, for selvfølgelig skal vi have lov til at sende vores kommunikation og sikre den sådan, så den er privat, så andre ikke kan bryde ind i den. Men det er så en lidt anden diskussion og en anden vinkel på det.

**Per Helge Sørensen:**

*Almindelige borgere har i høj grad behov for at kryptere. Og behovet vil stige.*

Jeg vil bare sige, at jeg er helt uenig i, at almindelige borgere ikke har behov for at kryptere. Jeg tror faktisk, almindelige borgerne er nogle af dem, der krypterer allermest for tiden, når de bruger deres homebanking-system, for der er jo netop krypteret, og der er jo helt tydeligt behov for at beskytte de informationer. Og Internettet er og bliver også meget andet end fødselsdagskort.

Vi vil se i de kommende år, at folk kommunikerer med deres læger, deres psykologer måske, de vil kommunikere i forhold til deres religiøse overbevisning, en hel masse ting, hvor at det er helt tydeligt, at der er behov for at beskytte kommunikationen for, at

andre ikke kan følge med i, hvad der foregår, at internetudbyderen eller arbejdsgiveren eller hvem, der nu kan lytte med, ikke har en chance for at se, hvad jeg skriver en mail til min læge om.

Og der har jeg som privatperson et klart behov for at kryptere, og jeg må indrømme, at jeg er ikke i tvivl om, at vi vil se mere og mere kryptering derude, fordi der er det behov for at beskytte vores kommunikation efterhånden, som brugen af Internettet bliver mere og mere udbredt også til andet end ligegyldige e-mails.

**Jon Stokholm**, advokat, fmd. for Advokatrådet:

*Digitalisering af forvaltningen rejser krypteringsspørgsmål.*

Jeg vil bare i tilslutning til det, som lige blev sagt, pege på den betænkning, der lige er kommet om digital forvaltning, hvor tanken jo faktisk er at digitalisere alt, hvad der overhovedet kan digitaliseres både i den kommunale og amtskommunale og den statslige forvaltning. Det kan ikke undgå at sætte fokus på et krypteringsproblem.

**Jørn Bro:**

*Falsk sikkerhed, hvis man tror, kryptering beskytter mod, at andre lytter med. Den eneste beskyttelse er omtanke med, hvad man skriver.*

Ganske kort: Man har i mange, mange år kunne foretage telefonaflytning af folks samtaler med deres læge og psykolog og bank, hvis det var det, man ville og havde hjemmel til. Jeg synes for så vidt, det er et dårligt billede. Det, der er grund til, og det er det, jeg har talt om, det er: Hvad har almindelige mennesker brug for af koder, scrambling, kryptering osv. Og det har jeg faktisk i det danske samfund, som det ser ud i dag, svært ved at se noget nævneværdigt behov for at kunne foretage en sådan kodning osv.

Og jeg tror, at det rummer en falsk sikkerhed, også hvis man forestiller sig, at man foretager en eller anden form for en korrespondance med sin gode ven, der lever i et lukket samfund. Der skal myndighederne såmænd nok finde ud af at komme ind til den maskine, der modtager den besked og få sat det element ind, der gør, at det går ud i klart sprog. Det, der er farligt i virkeligheden, det er, at man bilder folk ind, at der kan skabes en masse sikker kommunikation.

Den bedste beskyttelse det er trods alt omtanke - for der lyttes, hvad enten vi kan lide det eller ej. Og det meste af det, der bliver aflyttet, det ryger ned i den store brokkasse, for det er uinteressant. Men der filtreres visse oplysninger ud, og det er meget svært at sige, hvor det ligger henne, som anvendes efterretningsmæssigt og måske siden kan anvendes i nogle aktive tiltag. Så det, jeg bare vil sige, det er: Lad være med at tro, at

man kan skabe et eller andet sikkert rum, hvor man kan plapre fuldstændig uhæmmet, skriftligt eller mundtligt.

**Per Helge Sørensen:**

*Efterforskningsmyndighederne var bekymrede for kryptering og ønskede at tilrette teknologien, så man sikrede en aflytningsmulighed.*

Jeg bliver nødt til at respondere mod det. Altså jeg tror, at rigtig mange mennesker er enige om, at trusselsbilledet på Internettet er anderledes end i forhold til telefon-systemer. Og det er jo derfor, at bankerne har lavet kryptering i deres homebanking-system. Det er derfor, Datatilsynet stiller krav om, at kommunikation er krypteret, hvis der bare skal overføres et CPR. nr.

Så jeg mener ikke, at man kan foretage denne sammenligning at sige, at når vi har kunnet snakke med vores bank i telefonen, så kan vi også lave homebanking uden kryptering, fordi trusselsbilledet er et andet på Internettet, og de ting, vi foretager os på Internettet, er nogle helt andre end det, vi snakker i telefon om.

Der ligger tre glimrende rapporter på Forskningsministeriets hjemmeside om kryptering, som diskuterer hele det her forhold, og hvad mulighederne er for at forbyde det eller bremse det, som dokumenterer nogle af de her ting. Og en af de ting, som var meget klart, det var, at efterforskningsmyndighederne både i Danmark og USA var ret bekymrede for kryptering, og man ønskede at tilrette teknologien, så man sikrer en aflytningsmulighed.

Og det må jeg sige, at det viser i hvert fald for mig, at det er ikke rigtigt at sige, at politiet altid vil kunne finde en måde af aflytte folk, hvis de krypterer. Det mente folk i hvert fald ikke, dengang vi diskuterede kryptering. De var faktisk bekymrede over, at de moderne krypteringssystemer ikke kunne aflyttes. Og det tror jeg er rigtigt, jeg er helt enig med Peter: Der findes software, som krypterer så godt, at det er utrolig vanskeligt at bryde koderne, og det er software, der ligger på nettet frit tilgængeligt.

**Helge Adam Møller** (KF):

*Eksemplet fra Schweiz er utænkeligt i Danmark.*

Birgitte Kofod Olsen nævnte i sit indlæg sagen fra Schweiz med monsieur Armand, som både blev aflyttet og registreret af de schweiziske myndigheder, og hvor på et eller anden tidspunkt, så Den Europæiske Menneskerettighedsdomstol var det vel, frikendte ham og dermed bebrejdede de schweiziske myndigheder. Og det synes jeg, sådan som sagen blev fremstillet, det lød fuldstændig rigtigt og fornuftigt, det var jo groft overgreb.

Nu kunne der jo være nogle, der var her til stede, der måske ikke troede, at den sag kunne eksistere i Danmark, og derfor vil jeg godt have, at du og politimester Jørn Bro bekræfter, at det vil være fuldstændig utænkeligt, medmindre man klart brød de danske retsregler. For der er jo ingen muligheder for hverken at aflytte ham i den situation, som er beskrevet og endsige at registrere ham.
Og som det også blev fastslået meget klart, så de regler, som Politiets Efterretningstjeneste har her i Danmark, det er nøjagtig de samme retsregler, de skal følge som alle andre, altså de skal have ifølge retsplejeloven.

Jeg kan ikke huske, hvad det er for en paragraf, det er der andre, der kan, særlige forbrydelser typisk med en straframme på seks år eller mere, og de skal til en dommer, og særlig bestyrket mistanke og proportionalitet osv. osv., og så kan de få tilladelse til at gøre det. Og intet af det var jo tilsyneladende sagen i Schweiz. Så derfor, at det vil være fuldstændig utænkeligt i Danmark, kan du bekræfte det, medmindre der selvfølgelig var en, der brød loven, og det kan man jo aldrig gardere sig imod.

**Birgitte Kofod Olsen:**

*De schweiziske regler ligner de danske.*

Nej, nu fører det for vidt at gå ind i en detaljeret gennemgang af de schweiziske regler. De schweiziske regler på aflytning ligner i virkeligheden meget dem, som vi har i den danske retsplejelov. Det, der var problemet her, det var, at denne her Armand ikke var en mistænkt. Han var heller ikke en tredje person, som var relevant for opklaring af denne her sag. Han var en, som tilfældigt havde en telefonsamtale med en, der var på ambassaden.

Og lige præcis det tilfælde, at en tilfældig person bliver aflyttet, var der ikke hjemmel til, og det vil jeg heller ikke tro, der er, hvis man tager den danske retsplejelov. Så vil der heller ikke være hjemmel i den situation, så det var det, der var problemet her, og det var derfor, domstolen gik så meget ind i selve hjemmelsgrundlaget. For hjemmelen ser pæn nok ud, ligesom vore egen gør, men det er derfor, man skal være opmærksom på, at der kan altså være situationer - også i Danmark - hvor at den hjemmel, vi har, ikke kan anvendes i en konkret sag, og så er det, at myndighederne må afstå fra en aflytning og afstå fra en registrering.

**Jørn Bro:**

*Schweiziske regler tolkes mere lempeligt end danske. Oplysningerne fra en efterforskning står skrevet op, indtil sagen er færdigbehandlet.*

Ganske kort: Schweiziske regler er noget mere lempelige end de danske og den måde, så vidt jeg er informeret om det, de er i årenes løb også blevet forvaltet noget mere

lempeligt. Vi har nogle meget strikte krav i vores retsplejelov om, hvornår der kan opnås telefonaflytning, og de følges striks.

Noget andet er, at de oplysninger, der indgår over en telefonaflytning, eller som skabes igennem anden efterforskning, f.eks. hvis vi går fra dør til dør og spørger folk, om de var på et givet sted inden for et givet tidsrum, de vil stå skrevet op et stykke tid, indtil sagen er færdigbehandlet. Ellers er det jo meningsløst at gå ud og samle oplysningerne ind.

Spørgsmålet er bare, hvor længe og på hvilken baggrund, de kan samles sammen, registreres. Så jeg forstår i nogen grad ikke den schweiziske sag, før jeg har læst den nærmere, men der er meget skrappe regler for, hvad vi må indhente, og hvad vi må opbevare efter dansk ret.

**Søren Søndergaard** (EL):

*Underminerer ny teknologi mulighederne for kontrol med efterretningstjenesten?*

En del af diskussionen om overvågning, det er jo også en diskussionen om kontrollen med overvågningen. Og der har jeg så et spørgsmål til Jørn Bro, fordi i forhold til overvågning af Politiets Efterretningstjenestes registrering af personer, der har man jo Wamberg-udvalget. Og Politiets Efterretningstjeneste har dels en registrering af personer, men så har Politiets Efterretningstjeneste selvfølgelig også generelle sagsmapper og generelle arkiver liggende.

Er der ikke sket en underminering af Wamberg-udvalgets muligheder for at føre kontrol i og med den nye teknologi. Fordi man efterhånden som det hele bliver lagt på computere, så kan man simpelt hen ved et søgeord gå ind og plukke ud og sådan set lynhurtigt oprette en sagsmappe på en person og så øjeblikket efter, når man har tjekket de oplysninger, man ønskede, så lade den gå væk igen. Er der ikke sket en ændring på det punkt, i og med at PET har fået lagt tingene på computere?

**Jørn Bro:**

*Det er rigtigt, at ny teknik giver større muligheder for at bearbejde stort datamateriale. Men PET er den politiafdeling i landet, der er under strengest kontrol.*

I og med at man får edb-behandling af sine oplysninger, så får man væsentligt større muligheder for hurtigt at finde frem til relevante hændelser, navne, organisationer og lignende. En af grundene til, at engelsk politi brugte mange penge på hurtigt at få indført omfattende edb-systemer, var en meget stor seriemordersag, som man ikke

kunne komme til bunds i, før man fik sat det kæmpemæssige navnemateriale, man havde samlet sammen over hele England ind på en computer, og så faldt faktisk de fire-fem hovedmistænkte ud, og blandt dem fandt man gerningsmanden.

Så det er rigtigt, at man er i dag i stand til at håndtere og bearbejde og uddrage mere præcise oplysninger af et stort datamateriale. Jeg vil hævde, at en eller måske den politiafdeling her i landet, der er mest kontrolleret og mest reguleret, det er PET. Det ligger jo i hele den enorme politiske overvågning, der foregår, den enorme politiske debat, der foregår, omkring tjenestens opgavesæt og udførelse af sine opgaver.

Hertil kommer helt specifikke tilsynsudvalg, som jeg ikke har oplevet andet ved, end at de har passet deres tjeneste overordentligt nidkært. Og hvis ikke, man finder det er nok, så må det parlamentariske tilsynsudvalg rykke ind og sige: Hvad foregår der, og hvordan gør I det? Men det er nok den danske politiafdeling, der bliver kigget mest i kortene.

**Troels Ørting Jørgensen:**

*Politiet bekymrede for kryptering.*

Jeg vil bare lige sige til krypteringsdebatten, og muligvis kan jeg komme ind på det senere igen, at i hvert fald i den åbne del af politiet er vi meget bekymrede for kryptering. Det er faktisk sådan, at vi er bekymrede derhen, at vi er meget opsatte på, at man lovgivningsmæssigt tager højde for, at der kan skaffes nøgler til kryptering, for når vi bare er oppe over 256 bite kryptering, så er vi jo på den.

Og det vil så sige, at man rent faktisk kan kommunikere og så gør det det utrolig vanskeligt for ikke at sige umuligt for politiet at se det. For kriminalitet foredrages som en form for kommunikation mellem a og b, og hvis man så ikke på en eller anden måde kan dekryptere den, så skal vi i politiet jo i hvert fald tillægges andre metoder for at kompensere for den manglende mulighed for indgriben i kommunikationen efter rettens kendelse selvfølgelig.

**Søren Søndergaard** (EL):

*Underminerer ny teknologi kontrollen med personregistrering?*

Altså mit spørgsmål gik meget konkret på Wambergudvalget, altså om ikke Wambergudvalgets kontrol med personregistreringen bliver undermineret af muligheden for at anvende den nye teknologi.

Forstået på den måde, at man jo, når man arbejder med en konkret sag, bare kan gå ind gennem at lave et søgeord, der hedder et navn, så kan oprette det, der i virkeligheden er

en sagsmappe på den enkelte person. Og det kan man gøre løbende i forbindelse med sagen, uden at Wambergudvalget overhovedet kommer ind. Altså Wambergudvalget kommer ind på det tidspunkt, hvor man mere permanent opretter en sagsmappe på den enkelte person.

**Jørn Bro:**

*Jeg tror ikke, at PET bruger ny teknologi til at omgå kontrollen.*

Hvis man vil omgå tilsyn og tilsynsmyndigheder, så kan man selvfølgelig gøre det i en vis tid, men festen slutter, og den slutter brat, når det bliver afdækket. Jeg har ikke fantasi til at forestille mig, at man i tjenesten vil forsøge på, om man kan gå under øjnene på Wambergudvalget eller det parlamentariske tilsynsudvalg. Det ligger altså ikke i vores tradition eller vores uddannelse, og det bliver afsløret. Så det nærer jeg ikke nogen betænkelighed ved.

Men hvis det politiske liv ikke føler sig tryg ved den måde, hvorpå tilsynene udføres, så må man jo stille spørgsmålene i den politiske sfære. Men jeg føler mig ganske sikker på, at man ikke anvender de nye teknologiske muligheder til at lave fiflerier - det er jeg ganske sikker på.

**Ordstyrer:**
Ja tak. Tak til ekspertpanelet. Klokken er faldet i slag, den er 12. Det er tid til frokost, og jeg skal sige til tilhørerne, at der er lidt frokost inde ved siden af. Og for mit vedkommende skal jeg også sige tak for nu. Vi skifter over, så det bliver Hanne Severinsen (V), formand for Forskningsudvalget, der overtager efter frokost. Og så skal jeg erindre jer om, at vi starter præcis kl. 13.

## Overvågning på arbejdspladser

**Ordstyrer, Hanne Severinsen** (V), formand for Forskningsudvalget:
Så går vi i gang med eftermiddagens program. Og vi skal i første omgang diskutere overvågning på arbejdspladser, og dér har vi jo så også tre oplægsholdere, og den første, som jeg giver ordet her, er Laurits Rønn.

**Laurits Rønn**, sektionschef, Ansættelsesretlig Sektion, Dansk Handel og Service

*Butikker bruger tv-overvågning for at mindske butikstyverier, og for at beskytte personalet. Både medarbejderne og virksomheden er interesseret i regler om søgning på racistiske og pornografiske sider, og ønsker en åben politik på området.*

Tak for indbydelsen til den her høring. Jeg er blevet bedt om at tale om overvågning på arbejdspladsen, herunder hvordan vi ser på det fra arbejdsgiverside. Jeg vil fremhæve tv-overvågning, og jeg vil fremhæve problemstillingerne vedrørende e-mail og Internet.

Det er sådan, at detailhandelen de bruger tv-overvågning. Det gør vi ikke, fordi vi synes, det er sjovt. Det gør vi ikke for at genere kunder eller medarbejdere, eller fordi vi synes, vi skal have et Big Brother-samfund. Det gør vi, fordi vi har en saglig grund til det. En saglig grund - det er svind i butikkerne. Der er tale om et betydeligt svind i detailhandelen. Vi anslår det til omkring 3-4 mia. kr. om året. Det er mange penge, så vi er nødt til at gøre noget. Så vi gør det altså for at mindske det her svind. Og det, vi kan konstatere, det er, at det virker, altså overvågning virker. Har man video-overvågning eller tv-overvågning, så formindsker man svindet.

Vi gør det også for at øge sikkerheden for medarbejderne. Altså der er færre tyverier, der er færre røverier, det skaber en større tryghed. Medarbejderne er også fri for at holde øje med kunden, om det er kunden, der stjæler noget - det gør kameraet. Når man indfører de her systemer, den her tv-overvågning, så er det selvfølgelig naturligt, at lønmodtageren er utryg, altså: Hvad sker der her nu? Hvorfor gør virksomheden det her?

Derfor er det vigtigt, at man har en dialog og en åbenhed, når man indfører de her systemer - det her tv-overvågning. Man forklarer: Hvorfor gør man det her. Hvad er målet med det. Hvordan installerer man de her apparater osv. Altså man har en dialog og en åbenhed om det. For at mindske den her utryghed, så har vi på DA-/LO-området her i forsommeren lavet en aftale om, at lønmodtagerne skal informeres senest 14 dage, før det iværksættes, altså så de kan vurdere, hvorfor gør man det her, har man en saglig grund til at gøre det.

Og der er jo ingen tvivl om, at når man mindsker svindet i en virksomhed, så er det til fordel både for medarbejdere og for virksomheden. Hvis man kigger på Internettet og e-mail, så er det jo i en fantastisk udvikling. Man bruger jo e-mail i dag, som man brugte post før i tiden. Virksomhederne er helt afhængige af, at IT-systemet virker. Går systemet ned, lukker kontoret. Altså man kan ikke gøre noget. Og det kan være dyrt, og det kan være tidsmæssigt krævende at reetablere et sådant system.

Så derfor er vi nødt til at lave nogle retningslinjer. Vi er simpelt hen nødt til at opstille nogle retningslinjer: Hvordan styrer man det her forbrug af Internet og e-mail? Og i den forbindelse skal virksomheden selvfølgelig overholde den lovgivning, der er. Altså vi har persondataloven, vi har straffeloven, vi har de kollektive regler. Og det er klart, at de skal medtages, når man laver retningslinjer.

Vi har fra Dansk Handel og Service opfordret vores virksomheder til at lave de her retningslinjer og gå i en dialog med lønmodtagerne om de her ting, altså: Hvordan laver man de her regler, de her politikker på området? Der er mange ting, man skal tage stilling til: Hvordan håndterer man e-mail?

Hvem har adgang til medarbejdernes e-mail? Hvad gør man, når medarbejderen ikke er der - hvis kunder skriver, hvordan får man så effektueret den her ordre, når medarbejderen ikke er der? Hvordan gemmer man e-mail? Hvordan registrerer man e-mail? Hvornår downloader man filer? Hvordan sikrer vi os mod virus - det kan være ødelæggende for en virksomhed, hvis der kommer en virus? Hvad registrerer man og hvorfor?

Altså hele den her politik er helt afgørende. Det er helt afgørende, at man har nogle retningslinjer, som overholder lovgivningen. Der er også nogle etiske regler, man skal tage hensyn til. Både medarbejderen og virksomheden er interesseret i en regel om, hvor man søger på racistiske sider, hvor man søger på pornografiske sider, altså man har en politik på området, en åbenhed om det.

Min erfaring siger, at fra virksomhedens side - det er ikke kontrol, der er det bærende - det er sikkerheden, det er driften for virksomheden. Jeg vil give Peter Christensen ret i, at der er også en ledelsesmæssig fokus i det her. Altså laver de ikke noget, jamen så bør man også ledelsesmæssigt gå ind og få sat nogle retningslinjer for den pågældende medarbejder.

Jeg vil sige arbejdstageren bliver også mere fleksibel. Altså man går mere op i produktet end i tiden. Så jeg vil sige, at kontrol det er ikke det bærende, men for nogle virksomheder har det selvfølgelig også betydning. Der findes, som vi allerede har hørt i dag, en masse lovgivning på området: Vi har straffeloven, vi har person-dataloven, vi har kollektive regler. Og det er vores opfattelse, at vi har rigeligt med regler.

Der er efter vores opfattelse en god balance i de regler, vi har nu, mellem medarbejderens rettigheder og de muligheder, som virksomheden skal have for at kunne få en ordentlig drift. Så jeg vil egentlig opfordre til, at man ikke laver flere regler, men at man styrker dialogen ude i virksomhederne.

**Ordstyrer:**
Ja, tak. Og næste er Bjarne Petersen.

**Bjarne Petersen**, faglig sekretær, HK-handel

*Mennesker, der er ansat i en butik, bliver - under dække af at blive beskyttet af tv-overvågning - selv kontrolleret med kamera og mikrofon. Kameraer bliver mindre og kan optage lyd. Det gør overvågningen af de ansatte meget mere omfattende.*

Ikke mindst set i lyset af, at vi selv forsøgte engang her i forsommeren at afholde en konference om nøjagtig det samme tema, hvor vi i den grad manglede folketings-politikernes deltagelse, så er det jo ekstra dejligt, at vi sådan kan få mulighed for her at få luftet vores synspunkter.

Jeg vil godt sige, at jeg i mit indlæg udelukkende vil beskæftige mig med spørgsmål omkring tv-overvågning, hvorimod spørgsmål om e-mails det vil jeg lade ligge, fordi der i øjeblikket foregår nogle forhandlinger, som jeg meget nødig med forkerte eller, ja, andre udtalelser vil kunne komme til at spænde ben for.

Så jeg vil alene koncentrere mit indlæg omkring tv-overvågning. Og dér vil jeg sådan dvæle lidt ved udviklingen siden 1981, fra dengang vi fik den første lov om tv-overvågning, og så frem til i dag, og jeg vil dele den periode op på de der 20 år i to områder: Dels den teknologiske udvikling og dels den holdningsmæssige udvikling.

Hvis vi først og fremmest ser på den teknologiske udvikling, så dengang i 1981, da vi fik den første lov, så var baggrunden for, at man fik loven, at man i et butikscenter i Holstebro, havde meddelt, at man ville indføre tv-overvågning, som kunne beskytte det her butikscenter mod hærværk, når butikscenteret var lukket. Og til det formål da ville man opsætte et antal tv-kameraer, som så kunne fotografere de her uregelmæssigheder, der måtte foregå. Da lød et ramaskrig fra befolkningen.

Men lad mig sige først og fremmest omkring den teknologiske dér: De kameraer, som man havde til sinds at sætte op, og som da også senere blev sat op, ja, det var jo kameraer af en størrelse, næsten ligesom de tv-kameraer, vi ser anvendt her, altså et kamera af en størrelse, som man næsten ikke kunne undgå at få øje på.

Det var så i hvert fald til at forholde sig til, fordi så kunne man måske indrette sin adfærd efter, hvor de her store kameraer de pegede hen. Men der var også den holdningsmæssige side af sagen dengang: Det var, at man rent faktisk i Holstebro, hvor det her foregik, var utroligt bange for, at den overvågning, som man ville indføre, nærmest ville medføre, at man fik Big Brother-samfundet ind ad bagdøren.

Og de diskussioner, der rejste sig i Holstebro, de bredte sig meget hurtigt til det ganske danske land. Hvor nøjagtig de samme holdninger kom til udtryk, og disse holdninger nåede jo også Christiansborg, og man lavede så den første lov om privates forbud mod at anvende tv-overvågning. Siden da så er det gået stærkt, må jeg sige, både med den teknologiske udvikling og også med den holdningsmæssige udvikling.

Vi har i den samme periode oplevet, at man bl.a. i bankerne, som vi også har hørt det tidligere i dag, indførte tv-overvågning for at begrænse det store antal bankrøverier, der var på det tidspunkt. Og det var - vil jeg godt sige - den måde at beskytte medarbejderne på, og for den sags skyld også værdier på, var egentlig rigtig nok. Fordi det, man gjorde, det var, at man alene med udstyret fokuserede på de områder, hvor en formodet røver måtte formodes at ville indfinde sig, således at det var røveren, man fotograferede, således at man i efterforskningsmæssigt arbejde kunne alene bruge de optagelser til det arbejde.

Den succes, hvis man kan kalde det sådan, som bankerne havde på det tidspunkt ved at indføre det her, betød også samtidig, at en lang række røverier blev flyttet fra pengeinstitutterne til bl.a. servicestationer, døgnkiosker og bagerbutikker. Og vi oplevede, at nøjagtig de samme områder også lige pludselig indførte tv-overvågning. Og det var egentlig også helt i overensstemmelse med det, vi synes, der var godt - altså med vores holdning - fordi hvis det kunne medvirke til at beskytte medarbejderne, så var det vældig godt.

Men desværre, må man sige, at det, der samtidig skete, det var, at man ikke nøjedes med at beskytte medarbejderne eller nøjedes med at fotografere de områder, hvor de formodede røvere måtte indfinde sig, næh, man begyndte systematisk også at tv-overvåge medarbejderne. Og det er måske nok dér, vi skal se, at det største holdningsskred er sket fra dengang i 1981 og så til i dag, hvor at vi måske dengang havde en oplevelse af det Big Brother-samfund, som vi ikke ville have.

Det var et Big Brother-samfund, som i den grad var baseret på nogle opfattelser af, at vi blev kontrolleret, adfærdsmæssigt kontrolleret og sindelagsmæssigt kontrolleret, og det ville vi ikke acceptere. Den beskyttelse, som der også er ført med - som jeg nævnte før i forbindelse med tv-overvågning - den har hele tiden været accepteret, og det er, som om at det er alene den beskyttelse, som tv-overvågning kan føre med sig, er den side af sagen, vi taler om i dag, når vi taler om tv-overvågning. Altså, at

medarbejderne er beskyttet mod røverier, mod overfald, at de værdier, som der er i butikkerne, at de er beskyttet på samme måde.

Men vi glemmer i samme instans så at sige: Jamen de mange, mange kameraer, som så den teknologiske udvikling også har ført med sig, og den øvrige udvikling, der er sket, har ført med sig, at vi i dag i meget større udstrækning, end vi ville acceptere, oplever en kontrol af medarbejderne. Kameraerne, der altså i 1981 havde en størrelse som dem, vi ser her i dag, næsten da, er i dag nogle ganske, ganske bitte små kameraer på størrelse med halv tændstikæske, med objektiver på størrelse med et tændstikhoved og endda oven i købet en gang imellem tilført mikrofoner. Og som vi hørte i dag, så kan man også til disse systemer lave noget mønstergenkendelse i forbindelse med de her kameraer.

Det vil sige, at man hele vejen igennem har muligheder for at kontrollere både billedmæssigt og lydmæssigt medarbejdere med nogle ganske små og for den sags skyld også meget billige kameraer. Og det er det, vi oplever desværre i dag, at der i meget stor udstrækning bliver opstillet mange, mange, mange små kameraer, og kun nogle ganske få, skal vi sige, synlige kameraer i butikkerne.

Alle butikker har så at sige i dag tv-overvågning i en eller anden udstrækning. Og jeg vil godt præcisere, at den form for skiltning, som der i dag er påbud om, at der skal være i butikkerne, når man har tv-overvågning, den er ikke tilstrækkelig. Vi diskuterede bl.a. med juristerne i Justitsministeriet i forbindelse med den lovrevision, der førte til lovændring i 1998, om begrebet skjult overvågning. Og for juristerne da er der ingen tvivl om, at hvis man skilter - hvis man bare har et skilt med, at der tv-overvåges - jamen så er der ikke længere tale om skjult overvågning.

Hvorimod det er vores opfattelse af skjult overvågning det er altså alle de kameraer, som man i øvrigt kan opsætte, uden at medarbejderne er vidende om, at kameraerne er der. Fordi det vi ser de fleste steder, det er, at der sidder et enkelt skilt på døren, men ikke nogen skilte i øvrigt og ingen information om, hvor kameraerne i øvrigt er placeret.

Og når vi ser på, at meningen med skiltningen jo dybest set er at give medarbejderne mulighed for, at de kan indrette deres adfærd efter, at der foregår tv-overvågning, så er der ikke rigtig nogen overensstemmelse mellem skiltningen på døren og de mange kameraer, der er placeret i butikken.

**Aflytning af medarbejdere**

Og lad mig så lige igen tilføje, at de der små kameraer, som også kan suppleres med mikrofoner, som der er sat op mange steder, gør altså også, at der foretages aflytning, og det synes jeg også er en dimension, man skal have med. Altså vi har diskuteret aflytning i forbindelse med andre handlinger her i dag, og hvor politiet i forbindelse

med deres efterforskning af hård kriminalitet skal have en dommerkendelse for at kunne foretage aflytning og overvågning af kriminelle borgere.

Vi er altså i den situation, at mennesker, der er beskæftiget i den butik, under dække af, at de måske bliver beskyttet af noget tv-overvågning, tværtimod bliver kontrolleret både visuelt og auditivt, altså at man ved hjælp af de her små mikrofoner også aflytter, hvad det er, de siger.

Og jeg kan godt sige, at vi har flere eksempler på, at det er foregået, og når vi så har rejst spørgsmålet og sagt, det er ulovligt, så er der blevet sagt: "Jamen vi skal bare have samtykke for at måtte foretage denne her aflytning, og der er altså blevet givet samtykke af min nærmeste arbejdsleder", og så er vi altså nærmest på herrens mark.

Og det er altså et skisma - en forskel mellem den kriminelle verden og så nogle mennesker, beskæftiget i butiksverdenen, som er til at føle på. Og det mener jeg i hvert fald også er en dimension, man skal se på. Slutteligt her i mit indlæg skal jeg lige pege på det, som der også er blevet sagt tidligere i dag, det er, at persondata-loven, som jo blev vedtaget efter tv-overvågningsloven, også i hvert fald har nogle dimensioner, som man bør have med ind i en revision af tv-overvågningsloven, således at i hvert fald dette omkring skiltekravet ikke mindst bliver bragt up to date.

Altså der skal være et klart formål med, at man må indsamle de her persondata. Og man må sige, at tv-overvågning på den måde, som det foregår i dag, er også person-dataindsamling, og så skal der også være et klart formål med det. Og så må man også, når det er, at der skal skiltes med det, skilte med, hvad formålet er med at foretage denne tv-overvågning. Det vil altså sige, at det vil ikke længere være tilstrækkeligt bare at sige: Her foretages der tv-overvågning. Næh, tværtimod, der skal stå på skiltet: Her foretages tv-overvågning, fordi vi tror, personalet og kunderne de stjæler.

**Ordstyrer:**
Og den sidste i den her række, det er så Janne Glæsel. Værsgo.

**Janne Glæsel**, advokat, næstformand for Datarådet

*Overvågning, logning og kontrol af medarbejderes brug af e-mail og Internet skal ske ud fra hensyn til virksomhedens drift og sikkerhed og internt fastsatte regler. Og medarbejderne skal have klar og entydig information. Lovgivningen på området er i orden. Men der er nok brug for aftaler på arbejdspladserne.*

Jeg kan sådan generelt tilslutte mig det, der er blevet sagt i dag om, at det er utrolig vanskeligt at få et fuldstændigt overblik over samtlige former for overvågning, som

vi som danske borgere udsættes for. Og jeg har bemærket, at Peter Blume også i sit oplæg har kastet et forslag på bordet om at igangsætte et udredningsarbejde, og det kan jeg egentlig tilslutte mig. Det vil måske give et godt afsæt for en fortsat dialog. Her taler jeg ikke så meget for Datarådet, men mere for mig selv som advokat, der beskæftiger sig med det her område.
Jeg tror, at det er utrolig vigtigt at finde ud af, om det er rigtigt, at vi er ude på den her glidebane, som man taler om, om vi er i et overvågningssamfund, og hvad er et overvågningssamfund? Er det først, når vi ændrer adfærd som følge af overvågning, eller indtræder det på et tidligere tidspunkt, og hvad ændrer trusselsbilleder på vores opfattelse af de her problemstillinger?

Det, jeg synes, der er vigtigt hele tiden at holde sig for øje, når vi diskuterer også det emne om arbejdsgivere/arbejdstagere, det er, at intuitivt så er de fleste mennesker imod overvågning, hvis man spørger generelt. Men hvis man spørger konkret: Er du for, at man overvåger for at hindre socialt bedrageri? Jamen så vil de fleste svare ja. Og så er mulighederne for at komme ud på en glidebane til stede. Og derfor så er det vigtigt hele tiden at have en dialog og en debat og politisk stillingtagen.

Hvis vi så vender blikket mod arbejdspladsen og forholdet mellem arbejdsgiver og medarbejder, som jeg også er blevet bedt om at komme med et indlæg om, så mener jeg ikke, at problemstillingen er så diffus på det område. Jeg har den opfattelse, at området faktisk er tilpas reguleret, dels med persondataloven, tv-overvågningsloven, straffeloven, hovedaftalen, som netop er blevet indgået - man har også en skærm-bekendtgørelse, man har lov om helbredsoplysninger og diskriminationslove, hvor man også har reguleret de her mere arbejdsrelaterede forhold. Og så findes der også en sikkerhedsbekendtgørelse, der gælder for offentlige myndigheder. Det skal jeg senere komme tilbage til.

Og det ligger helt fast, at overvågning, og herunder logning og kontrol af medarbejderes brug af e-mail og Internet, at det skal være sagligt, og det skal ske ud fra hensyn til virksomhedens drift og sikkerhed og overholdelse af internt fastsatte regler fra virksomhedens side. Det ligger lige så fast, at medarbejderne skal have en klar og entydig information om disse politikker. Så myndigheder og virksomheder de er altså, sådan som reglerne er i dag, forpligtet til at fastsætte politikker omkring tv-overvågning, Internetovervågning og overvågning af e-mail.

Det, jeg mener, der er et behov for at sætte fokus på, det er altså information om de her forhold. Og i Datatilsynet dér har man fokus på det. Man har allerede udsendt én nyhedsmeddelelse, der kommer om ikke så længe, en anden nyhedsmeddelelse i forbindelse med en konkret sag. Og også i IT-Sikkerhedsrådet arbejder man med en publikation omkring disse her forhold, netop fordi vi har reglerne. Men der skal informeres til arbejdsgiverne og arbejdstagerne om, at der skal altså vedtages nogle politikker, der skal forhandles med samarbejdsudvalgene.

Og som jeg skriver i mit skriftlige indlæg, så tror jeg, at det, medarbejderne er bange for, jamen det er dér, hvor de ikke kender formålet. De ved ikke, hvad der sker. Det er det, der skaber usikkerheden. Men har man været inde i en dialog, så er den usikkerhed ikke til stede. Jeg tror, at danske arbejdsgivere ved, at overvågning ikke kan erstatte ledelse. Det mener jeg er helt klart, at det kan det heller ikke i den digitale verden.

Det handler ikke om kontrol for kontrollens skyld, men det handler om at sikre en virksomheds drift. Og reglerne, som de er nu, mener jeg giver en fleksibilitet, der gør, at man kan tilpasse det individuelt på den enkelte arbejdsplads. Så tror jeg heller ikke, at domstolene de vil se med milde øjne på en arbejdsgiver, der bortviser en arbejdstager, fordi han har været inde på en side, som arbejdsgiveren ikke synes om, uden at der er formuleret en politik i virksomheden, uden at der er givet en advarsel. Så også det system tror jeg giver en god sikkerhed.

Og endelig så er krænkelser inden for det her område ganske dårlig markedsføring. Vi er i hvert fald i mange brancher i en situation, hvor man gør meget for medarbejderne, simpelt hen for at tiltrække medarbejdere, så også ud fra det hensyn, så ligger der altså en opgave på arbejdsgiverens side. Jeg tror også, det er vigtigt at se på, hvordan kommer sagerne frem.

Sagerne - mener jeg ikke, med det kendskab, jeg har - de kommer ikke frem ved, at arbejdsgiveren sidder om aftenen og går loggen igennem og kontrollerer systemerne og så fanger de medarbejdere ud, der har gjort noget, som er i strid med politikken. Så vidt jeg er orienteret, så kommer sagerne frem ved, at pornosider videre-distribueres ved, at dårlige racistiske vittigheder videresendes ved, at man kommer tilbage til sin skærm, som man har lånt ud og kan se, at nu ligger der lige pludselig beviser på, at den, der har brugt installationen, har været inde på nogle sider, som man ikke lige synes om.

Det er den måde, det kommer frem på, hvis der er tyveri i en virksomhed, så har man en adgangskontrol, og man kan gå ind og se i loggen, hvem der har været der. Altså jeg tror ikke, arbejdsgiverne vil bruge ressourcer på at sidde og kigge og overvåge på den måde, fordi det har man ledelsessystemerne til at opfange. Endelig så er der jo mange virksomheder, der installerer sladrehanke sådan at forstå, at man installerer nogle værktøjer, der gør, at man simpelt hen ikke kan komme ind på visse sider, og det er jo så en rent teknisk kontrol, kan man sige, hvor selvfølgelig den system-ansvarlige kan gå ned og se.

**Tv-overvågningslov og persondatalov**

Med hensyn til tv-overvågning og persondataloven, der skal jeg lige kort komme med nogle bemærkninger. Jeg mener egentlig ikke, at der er den store uklarhed mellem de to love. Tv-overvågningsloven den regulerer adgangen til at foretage overvågning, mens persondataloven regulerer, hvordan må man bruge det, til hvilket

formål. Og det er klart, at de oplysninger, hvis man kan identificere en person via en tv-overvågning, jamen så er det omfattet af persondataloven, og så skal såvel de generelle som de specielle regler i persondataloven, være opfyldt. Der skal være et klart formål, og man må ikke opbevare længere end hensynet nødvendiggør.
Det er muligt, at der kan være nogle problemstillinger omkring skiltning, det kan godt lyde sådan. Jeg tror igen, at det handler om at få en debat ude på arbejdspladserne om, jamen hvorfor gør man det her. Hvordan anvender man det, sådan så der skabes en tryghed og sådan så medarbejderne ved, hvor det er, de bliver overvåget.

Til sidst vil jeg lige sige lidt omkring den sikkerhedsbekendtgørelse, der gælder for offentlige myndigheder, fordi jeg synes, den på god måde illustrerer kompleksiteten i området. Det er sådan, at offentlige myndigheder de har faktisk pligt til at foretage logning af visse transaktioner efter den sikkerhedsbekendtgørelse, som er gældende. Og det viser, at det handler ikke kun om medarbejderne over for arbejdsgiveren.

Det handler også om de oplysninger, som virksomheden ligger inde med, oplysninger som kan være følsomme omkring borgerne, at der har virksomheden altså en pligt til at føre kontrol med via en log, hvem der er inde og hente oplysninger, helbredsoplysninger om borgere og andre følsomme oplysninger. Så det handler ikke kun om medarbejderne, det handler også om de oplysninger, der ligger inde i virksomheden, at man altså har et krav om, at man skal logge for at hindre misbrug. Ja, det var hvad jeg havde.

**Ordstyrer:**
Ja, men så siger jeg tak for de oplæg, og fra Folketingets spørgepanel er der allerede tre, der har meldt sig, så det er Thomas Adelskov, der først får ordet.

## Spørgsmål fra Folketingets spørgepanel

**Thomas Adelskov** (S):

| |
|---|
| *Kan vi få konkrete eksempler? Hvad er arbejdsgivernes grænser for overvågning?* |

Jeg vil stille to spørgsmål, først til Bjarne Petersen: Har du nogle konkrete sager, nogle konkrete eksempler på, hvor at tv-overvågningen er blevet brugt eller misbrugt og har virket krænkende, der kan være med til at belyse nogle af de problemstillinger, du anfører og de synspunkter, som HK har. Det var mit ene spørgsmål.

Det andet, det går til Laurits Rønn: Vi har tidligere i dag også hørt, at der er nogle, der har stillet spørgsmålstegn ved tv-overvågningen som sådan, hvad der står på

skilte, hvor mange skilte der skal være, hvad der skal være anført af forskellige ting derpå. Men du angiver, at du ikke mener, at der er behov for ekstra eller fornyet lovgivning.

Hvad siger du til et ønske, et krav om, at der bliver anført på, hvad man overvåger for, og hvor meget man overvåger i lokaler. Det ene til dig, og det andet skulle være at sige: Har I nogle grænser for, hvad for nogle rum, altså omgivelser, I mener, at I som arbejdsgivere har ret til eller bør have ret til at overvåge i?

**Bjarne Petersen:**

*Ansatte bad om tv-overvågning for at stoppe tyverier – og endte med selv at blive udsat for skjult overvågning.*

Ja, nu bliver jeg bedt om et helt konkret eksempel, og det har jeg flere af, men jeg vil godt trække et frem, som er ganske nyt, og som også egentlig er temmelig groft. Jeg skal ikke nævne virksomhedens navn, det er jo uinteressant, men sige, at det er en af de største detailhandelskoncerner i Danmark og det største medlem af Dansk Handel og Service. De har en lang række butikker, også bl.a. nogle tøjbutikker, som hedder Tøj og Sko. Og her for ganske nylig, der skete det, at vi fik en henvendelse fra nogle medarbejdere beskæftiget i sådan en Tøj og Skobutik her på Nørrebro i København.

De medarbejdere, de var startet i butikken, i den samme butik for ni måneder siden, hvor der var et afsindigt rod, og hvor der var utrolig stort svind. De tre medarbejdere, som var to miniansatte og en butiksbestyrer, de var alle tre enige om, at den butik ville de have op og stå. Men butikken lå altså i et område, hvor der var utrolig meget svind. Og for ikke ret lang tid siden, en uges tid før at vi fik en henvendelse fra dem, der er der en dag en kunde, der siger til en af de ansatte: ”Bemærkede du den kunde, der var herinde lige før, som tog en bluse og stak ned i sin taske?”

Det sagde den ansatte til den pågældende kunde, at det havde hun godt bemærket, og at de i øvrigt tit havde talt om tv-overvågning. Men den der episode fik de tre medarbejdere til igen over for deres distriktschef, at rejse et ønske om, at de fik noget tv-overvågning i butikken, således at de kunne undgå de her butikstyverier. Det blev affærdiget og afvist med, at det var der ikke penge til.

Få dage efter denne her episode dukker der et brev op i deres postkasse fra Falck-Securitas. Falck-Securitas sender en faktura, fordi Falck-Securitas to gange, to nætter har været ude og lukke butikken op. Og det forstår butiksbestyreren ikke, hvad det er for noget, så han ringer til Falck-Securitas og spørger, hvad det er, og får så at vide, at det er koncernens interne revision, der har været ude og få butikken lukket op med henblik på kontrol.

Og det får de her tre medarbejdere til at reagere temmelig voldsomt. De går igennem butikken for at se, om der er et eller andet synligt bevis på, at der har været nogen, og de finder så nede i kælderetagen en boks sat op på væggen, som de aldrig har set før. En boks hvorfra der stikker tre ledninger ud, og de tre ledninger prøver de på at følge.

Den ene ledning kan de se, at den slutter i et rør, hvor der også er et lille hul, og når de kigger ind i det lille hul, så sidder der et kamera, som peger hen imod der, hvor de klæder om. Og den ene af de ansatte klæder sig altså om næsten fra inderst til yderst hver dag. De to andre ledninger kan de ikke rigtig se, hvor de fører hen, men da de ser, at det første her er til et lille kamera, så er de ikke i tvivl om, at de to andre ledninger, det sikkert også fører til nogle kameraer, hvis ikke den ene af dem måske fører til et eller andet transmissionsanlæg.

Den reaktion, der er fra de tre medarbejdere, er meget voldsom. De føler sig dybt, dybt krænkede. Både fordi den der mistillid, som de er blevet vist efter selv at have forsøgt at rette en butik op, og efter selv at have rejst spørgsmålet om, hvorvidt man kunne få tv-overvågning til at kunne beskytte varer og værdier, nu i stedet bliver brugt til at kontrollere dem selv, sådan oplever de det.

Og det må jeg sige, at det er meget analog med den reaktion, vi oplever fra mange, mange medlemmer. Det er, at de medlemmer, der henvender sig til os, de henvender sig til os, fordi de ved en tilfældighed har opdaget, at de også har været genstand for noget overvågning, som mere har haft karakter af kontrol, end det har haft karakter af at beskytte varer, værdier, kunder og personale og hvad ved jeg.

Og det er typisk - nu hørte jeg engang her i weekenden i radioavisen, at der er en meget lille lyst til for voldtægtsramte kvinder til at gå videre end en anmeldelse, fordi man oplever, at man er blevet så krænket, som man har været i forbindelse med en voldtægt. Den oplevelse, som medlemmerne har, og ofte - vil jeg godt sige - for det meste kvindelige medlemmer har i forbindelse med det, at de bliver opdaget ved sådan en tv-overvågning, det har karakter af åndelig voldtægt. Men reaktionen er nøjagtig den samme. Man vil godt ringe til os og sige: Jeg har været udsat for det og det, men man tør ikke gå videre.

Og det er måske lige netop det, der så kendetegner den pågældende sag fra Nørrebro, det er, at den ene af de tre var butiksbestyreren, og man derfor stod sammen. Men det jeg også godt vil slå en fed streg under, det er, den der loyalitet, som man fra medarbejderens side har oplevet er blevet brudt, den gør utrolig ondt. Og det er det, vi også skal være opmærksomme på.

Det er i hvert fald det, som vi siger, at ud over, det der er modbydeligt, der kan ligge i overvågningen, så også den loyalitet, som man i den grad bryder over for medarbejderen. Den skal vi også tænke på, og det er den, arbejdsgiverne desværre

måske med baggrund i, at det er så billigt at anskaffe sig det overvågningsudstyr, altså for ofte ser bort fra.

Og der kan altså sættes overvågningsudstyr op af alskens slags til meget, meget små penge i dag, og der bliver det også. Eksemplet med, at man kan rekvirere en virksomhed som Falck-Securitas til i nattens mulm og mørke og komme ud og sætte den op, understreger for os, at det her, det er nok ikke et enestående eksempel, det er nok en vare, man tilbyder andre virksomheder også.

**Laurits Rønn:**

*Kender ikke den konkrete sag, men det lyder som et brud på loven. Det giver sig selv, hvad formålet er med overvågning, så der er ikke brug for særlig skiltning. Man skal kun overvåge, hvor der er et sagligt formål.*

I relation til den konkrete sag, Bjarne Petersen, så kender jeg den ikke, men det er klart, hvis en virksomhed ikke har skiltet med det så gør de noget, der er i strid med loven, og det må de ikke. Sådan er det. Med hensyn til skiltning, så er det jo sådan, at man skal skilte, hvis man laver videoovervågning.

Og man kan sige, hvor meget skal man skilte? Skal man skrive, hvad formålet er? For mig at se, så giver det sig selv. Altså formålet det er, at man vil mindske svind i virksomheden. Og er der grænser for, hvor man skal overvåge henne? Ja, men der skal man have for øje, det skal have et sagligt formål det her. Altså ved kantinen der kan jeg ikke se, at der umiddelbart skulle være et sagligt formål med at lave overvågning.

Det med om man skal sige, hvor kameraerne er, vil jeg sige, at det generelt er en meget god ide, at man har en dialog med medarbejderne også i: Vi har de her politikker, vi gør på den her måde. Jeg mener, det er sjældent, at man retter kameraet direkte mod medarbejderne, og hvis man har det, så er det, fordi man har en konkret mistanke om, at der er tyveri, at der bliver taget nogle penge fra kassen. Hvis man sagde det, så duer det ikke, for så får man ikke opdaget det. Så det er bare ordene herfor.

**Knud Erik Hansen** (SF):

*Hvorfor er e-mails et problem at håndtere, når straffeloven og reglerne om brevhemmelighed siger, at man ikke må bryde post, herunder e-mails, som har privat karakter?*

Jeg vil godt stille nogle spørgsmål til e-mails i virksomhederne. Nu sagde du godt nok Bjarne, at du ikke ville ind på det, men jeg har lidt svært ved at forstå, hvad problemet egentlig er. Altså hvorfor det skal være et problem.

Altså hvis vi har almindelig brevpost, så har man typisk en tradition på en virksomhed, hvis der kommer noget, der står privat på, jamen så er det klart, så er det et privat brev, så det er et personligt brev. Man har også typisk en tradition for, at medarbejderne vil snakke sammen i telefonen eller i krogene og går til hinandens kontor, så lytter man ikke på det. Og hvorfor laver man så ikke e-mails på den måde, sådan at man siger, at hvis man har en officiel adresse udadtil, hvis der kommer breve på den, så er det til virksomheden, selv om det så er til personen, men hvis det er den officielle adresse, så er det den.

Så kunne man have en adresse til en person på virksomheden, hvor der stod et lille p på også, så signalerede det, at den adresse var et privat brev, mail, og så kunne man så til intern post typisk sagtens teknisk lave det således, at det var intern post. Så havde man tre kategorier, og så kunne man behandle det på nøjagtig samme måde, som man egentlig behandler skriftlig post. Kan man ikke gøre det, og hvor er problemet så henne?

**Bjarne Petersen:**

| |
|---|
| *HK har en privat og en firmamail til hver medarbejder. Men vores modpart mener, at alle mails skal kunne åbnes.* |

Jeg vil godt sige, at internt i HK, der har vi den politik, nøjagtig som du der skitserer. Altså at man har en adresse, som er til firmaet, om jeg så må sige, og den post, der kommer dertil, den er tilgængelig, den er fra det her firmapost. Ligesom hvis det var papirpost, hvor der kom brev og stod: HK-Handel, att.: Bjarne Petersen, så er brevet altså til HK, så er brevet ikke til mig.

Derimod hvis der er noget, der er privat, så er det altså til Bjarne Petersen, og den mulighed er der, den tekniske mulighed er der, og det kan sagtens lade sig gøre, i hvert fald så vidt jeg ved. Det, der er problemet, det er altså hos vores kære modparter, der mener, at de altså har behov for at kunne lukke posten op, når det er elektronisk post. Et behov, som de ikke har haft tidligere, da det bare var almindelig papirpost, så du må næsten spørge Laurits hvorfor.

**Laurits Rønn:**

| |
|---|
| *Vi ønsker ikke at åbne post, der er markeret som privat.* |

Tak skal du have Bjarne.

Man kan sige, vi anser jo e-mails som almindelig post, og det er således, at hvis man kommunikerer med andre virksomheder via e-mail, og derfor har vi et behov for at se de her e-mail, i hvert fald at vi har en adgang til at have dem. Men det er også sådan, at hvis der står privat på e-mailen, altså så åbner vi den jo ikke. Vi følger den praksis, Datatilsynet har tilkendegivet. Så hvis lønmodtageren skriver det her er privat eller modtageren er privat, jamen så åbner vi den ikke. Altså det har et klart driftsmæssigt formål.

**Knud Erik Hansen** (SF):
Det, I svarer mig, det er, at der ikke er noget problem. Er det rigtigt?

**Bjarne Petersen:**
Jeg ser ikke noget problem. Det kan teknisk løses.

**Janne Glæsel:**

| |
|---|
| *Mange virksomheder ønsker ikke to e-mailadresser, fordi det kan være svært at skelne, hvad der er privat.* |

Ja, men der er vel mange virksomheder, der er tilbageholdende med at tildele både officielle adresser og så private adresser, fordi det måske kan være vanskeligt at skelne mellem, hvad der er privat, og hvad der er virksomhedsrelateret.

Jeg kunne forestille mig, at det var noget sådant. Men det er klart, at vi har jo også straffeloven og brevhemmeligheden, som klart siger, at man ikke må bryde post, herunder e-mails, som har privat karakter. Men jeg ved også, at der er virksomheder, som definerer al post - også selv det, der står privat på - som virksomhedsrelateret ud fra driftsmæssige hensyn, sikkerhedsmæssige hensyn, og hvor det så også er klart kommunikeret ud til virksomhederne. Det er der virksomheder, der gør.

**Ordstyrer:**
Ja, Kristian Jensen, det er måske en anden boldgade?

**Kristian Jensen** (V):

| |
|---|
| *Er det oplysning, der mangler?* |

Ja, og dog. Allerførst det, jeg hører jer sige, det er, at lovene er gode nok, eller reglerne er gode nok, men informationen om, at man skal ud og have lavet aftaler og få lavet de konkrete aftaler, at der er der stadig et stykke arbejde at lægge.

Men noget, jeg også hører både Janne sige, men også andre af indlederne i dag, det er, at der mangler oplysning om den overvågning, der finder sted. At hvis folk får at

vide, hvorfor, hvordan, hvem, hvornår og hvor længe, så skifter folk holdning til overvågningen. Og det må nok så være til Bjarne: Er du enig i det scenario, som i hvert fald i noget af det skriftlige materiale er et par af indlederne, der har lagt op til, og som jeg også lidt hører Janne sige nu her.

**Bjarne Petersen:**

*Problemerne opstår, når folk ikke er klar over, hvad der foregår. Kæden knækker, hvis man føler sig unødigt kontrolleret.*

Jeg er enig langt hen ad vejen og i hvert fald enig, at hvis det er, folk er informeret, så de ved, hvordan de skal forholde sig, hvordan de kan indrette deres adfærd, og at det er foranstaltninger, der er lavet for at beskytte dem, ikke for at kontrollere dem, så er de meget langt hen ad vejen dus med de her ting og vil gerne være med til tingene. Det, der er problemet, det er, at lige så snart de ikke er klar over, det foregår, lige så snart man føler sig kontrolleret og unødigt kontrolleret, så knækker kæden.

Må jeg lige sige også til Kristian, du spurgte i formiddag, om der var forskel på folks adfærd, hvis de vidste sig overvåget eller ej. Jeg kom til at tænke efterfølgende på en episode for et par år siden, hvor en skolelærer nede i Solrød blev overvåget af en forældrekreds gennem hele undervisningen, og hvor denne skolelærer blev temmelig alvorligt syg af den overvågning - det var altså ikke en elektronisk overvågning, det var en manuel eller en personlig overvågning - men den skolelærer blev altså meget alvorligt syg, psykisk syg, af den her overvågning.

Og jeg tror ikke, der er nogen forskel på, om overvågning den foregår maskinelt eller teknologisk, eller om det foregår via mennesker. Altså hvis man føler sig kontrolleret, hvis man føler sig overvåget, og hvis man også er det, jamen så er man begrænset så meget i sine udfoldelsesmuligheder, at det kan ikke undgå at sætte sig spor også rent helbredsmæssigt.

**Thomas Adelskov** (S):

*Hvordan beskyttes privatlivets fred og den personlige integritet på arbejdsmarkedet?*

Ja, jeg vil godt følge lidt op på Knud Eriks spørgsmål omkring e-mails og Internetbrug og logning. Det var jo sådan, at tidligere på året blev der rejst et par sager og var en del pressepolemik netop omkring det her og et par fyringer som konsekvens af folks enten e-mails eller Internetkiggeri.

I den forbindelse sådan lidt polemisk så tænkte jeg på, at da Internettet i sine fødselsår jo skulle implementeres i virksomhederne, der gjorde man jo mange steder

egentlig noget ud af at få medarbejderne til at sidde og skrive lidt privat, så de vænnede sig til det her nye medie og gå ind på Internettet og kigge lidt rundt, så de også vænnede sig til den der arbejdsform.

Nu er vi måske kommet i en situation, hvor virksomhederne i nogle situationer i hvert fald føler, at det er blevet for meget, og denne her frivillighed og denne her tilskyndelse til at gøre det det har vendt sig om, til at man ønsker at begrænse det, og deri opstår måske så nogle af de problemer, som vi løber ind i i dag.

Men mit spørgsmål det kunne være at sige, er der behov for, at vi som lovgivere skal ind her, eller er det noget, jeg forstår, I har nogle forhandlinger i gang, eller hvad var det, der lå en antydning af i starten fra Bjarne Petersen?, Fordi kan man løse det arbejdstager/arbejdsgiver imellem, så tror jeg, vi som lovgivere ville være mere lykkelige.

**Laurits Rønn:**

*Information er vigtig, og vi overvejer at lave et sæt retningslinjer til vores medlemmer.*

Jeg tror, at vi er meget enige om, at det her handler om information, det er meget vigtigt, at medarbejderne får at vide, hvad er det, vi kontrollerer, hvad må du gøre, hvad må du logge ned osv. Og derfor så har vi gennem tid overvejet, om man kunne lave nogle anbefalinger, nogle retningslinjer, hvad er det for nogle ting, vi skal oplyse om, og de pågår p.t.

Vi lagde nogle anbefalinger ud på vores hjemmeside for omkring 3 år siden, og vi kan se på de besøgstal, vi har, at det er noget af det mest besøgte, altså det er noget, der interesserer virksomhederne. Der er ingen tvivl om, at de er implementerede i mange virksomheder i dag, man har nogle konkrete retningslinjer, og det skal man også i henhold til lovgivningen. Så jeg synes, der er en god udvikling.

**Bjarne Petersen:**

*Vi kan måske godt få brug for hjælp fra Folketinget på dette område.*

Men jeg vil bare supplere med at sige, jamen altså de tekniske muligheder de er til stede, og muligheden for at kunne lave nogle politiske løsninger også på arbejds-markedet er også til stede, hvis viljen er til stede.
Men jeg vil ikke sidde her og afvise, at der godt kan være brug for måske at få hjælp fra Folketinget også til at få løftet den her diskussion op, således at de aftaler, der skal laves på arbejdsmarkedet, måske får en anden dimension. Og det er det, som jeg

godt vil undlade at gå ind i nogen bemærkninger omkring, fordi jeg ved ikke præcis, hvor det er henne, man er på det sæt.

**Ordstyrer:**
Og her vil Peter Blume godt ind.

**Peter Blume:**

*Eksempler viser, at regulering er nødvendig. En stor del af arbejdsmarkedet vil falde uden for det, som arbejdsmarkedet parter kan blive enige om, og deres foreløbige aftaler er ikke imponerende.*

Jeg vil godt sige to ting. For det første er det her jo et godt eksempel på det, vi også drøftede i formiddag, at der kommer en ny teknologi, som skaber en ny form for overvågning, som formodentlig ikke er ret meget anderledes, kan man sige, end den gamle. Men dette at man nu overvåger korridorsnakken, som man jo gør, Internettets interne anvendelse i virksomheden. Altså den gode eller mindre gode vittighed om chefen, som hviskede et andet sted, og så blev man så fyret, som der er eksempler på. Det er sådan øget overvågning, som gør en regulering nødvendig.

Om man drøfter, om det nu er bedst at holde sig til de sådan relativt generelle retningslinjer, som man kan udlede af Datatilsynets brug af persondataloven og så overlade det til arbejdsmarkedets parter eller ej, ja, så opstår selvfølgelig spørgsmålet: Hvis man overlader det til arbejdsmarkedets parter, hvad så med det store uorganiserede arbejdsmarked, som ikke er omfattet af de aftaler.

Hvis jeg skulle tilføje for helt egen regning, så vil jeg sige, at det protokollat, som LO og DA præsterede her i april, ikke er særlig imponerende. O.k. det nye er måske de 14 dage, resten er der intet nyt i. Men i hvert fald kan man sige, at en stor del af arbejdsmarkedet falder fuldstændig uden for det, som arbejdsmarkedets parter måtte kunne blive enige om. For mig at se drejer det sig om så grundlæggende værdier som privatlivets fred, personlig integritet på arbejdsmarkedet. Her i det her tilfælde, at det er en lovgivningsopgave og ikke en aftaleopgave.

**Kristian Jensen** (V):

*Kan aftalerne ikke fungere som rettesnor for de andre?*

Jamen aftalen ligger jo ikke blot mellem LO og DA, den ligger jo også mellem den konkrete arbejdsgiver og den konkrete arbejdstager. De regler, som Datatilsynet har lavet for overvågning på arbejdspladsen, er jo ikke nogen, som er LO-, DA-relateret, så kunne man ikke lige så vel forestille sig, at man også på det uorganiserede arbejdsmarked gik ind og sagde, vi vil altså følge de retningslinjer, der nu engang

ligger og tog den diskussion op, sådan at det ikke er fra Folketinget, men fra dem, der sidder i situationen, at man aftaler: Hvad er det, vi gør her hos os.

**Peter Blume:**

*Uorganiserede arbejdsgivere har ingen pligt til at følge LO og DA's aftaler.*

Altså det er klart, de retningslinjer, som Datatilsynet har stillet op i forbindelse med nogle konkrete afgørelser, de er jo baseret, kan man sige, på lovgivning, nemlig persondataloven, og det er det, som Datatilsynet kan gøre. Datatilsynet kan jo ikke gå ind og prøve at gøre sig klog på, hvad man kan udlede af arbejdsretten, det er der ingen kompetence til, det er klart. Og lovgivningen gælder jo for alle, så det gælder selvfølgelig også for det uorganiserede arbejdsmarked.

Hvis man ønsker at lave mere præcise retningslinjer og måske finder, at det, som Datatilsynet er nået frem til - det er der nogle, der gør - er for arbejdsgivervenligt, ja, så ender bolden eller aben tilbage på jeres bord. Fordi den vil ikke kunne ende hos LO, DA eller andre organiserede organisationer, om man så må sige, fordi deres aftaler har ingen betydning for resten af arbejdsmarkedet, og der er ingen pligt for uorganiserede arbejdsgivere til at interessere sig overhovedet for, hvad LO og DA kan finde på at aftale. Men det her handler jo grundlæggende som på mange områder om spørgsmål om, hvordan skal vi se på den berømte eller forkætrede danske aftalemodel i forhold til brug af lovgivning.

**Janne Glæsel:**

*Persondataloven er et godt grundlag for lokale aftaler.*

Jeg har den holdning, at jeg tror, det bliver alt for stift, hvis man går ind og rådgiver om sådanne detaljerede, helt individuelle forhold, som kan gøre sig gældende på forskellige virksomheder. Jeg tror, at vi har et godt grundlag med persondataloven og med den praksis, som Datatilsynet har udstukket kombineret med alle de andre regler, som vi har på det her område. Og det er da rigtigt, at det uorganiserede arbejdsmarked ikke er bundet af hovedaftalen.

Men i virkeligheden så reflekterer hovedaftalen jo grundprincipperne i person-dataloven og har så konkretiseret denne her 14-dages-frist. Om det skal være 14 dage, 1 uge eller 3 uger, inden man igangsætter en overvågning, det kan være individuelt. Men altså jeg tror i virkeligheden også, at man i tilsynspraksis vil komme til, at man skal informere inden. Og inden det er typisk 1 uge - 14 dage. Så altså jeg tror, det er farligt at indføre snærende regler på det her område.

**Ordstyrer, Hanne Severinsen** (V):

*Er der brug for yderligere regulering, hvis det diskuterede eksempel er ulovligt?*

Man kunne måske stille det tillægsspørgsmål om det eksempel, som Bjarne Petersen nævnte. Det er måske i virkeligheden ulovligt? Men du siger, der måske stadig væk er brug for noget lovgivning?

**Peter Blume:**

*Eksemplet var klart ulovligt, men er reguleringen tilfredsstillende?*

Det var det eksempel med skoforretningen, ikke. Ja, det er jo klart ulovligt, det er alle enige om, for der var ikke skiltet. Men det er så den anden del af det her tema, altså omkring hvorvidt den regulering, der er om tv-overvågning, er tilfredsstillende. Det er en lidt anden problemstilling, det er den samme, men det er selvfølgelig en anden teknologi end det med mail og net.

**Lissa Mathiasen** (S):

*Er overvågning med lydoptagelse på arbejdspladser i overensstemmelse med menneskerettighederne?*

Når vi taler om lydoptagelser, og det gør vi jo så uden dommerkendelse af gode grunde i forbindelse med butiksansatte, der kunne jeg godt tænke mig at høre Birgitte Kofod Olsen, hvordan har dette det egentlig i forhold til proportionalitets-princippet, set i relation til overtrædelse af menneskerettighederne? Fordi der er vi jo i hvert fald langt væk fra spørgsmålet om svind. Det er i hvert fald ikke det, der typisk kan komme ind i den sammenhæng.

**Birgitte Kofod Olsen:**

*Det må komme an på en konkret vurdering i hvert tilfælde.*

Altså nu er det ikke sådan ganske oplagt lige at bruge menneskerettigheds-, privatlivsbeskyttelsen i denne her sammenhæng, når vi taler om overvågning på arbejdspladser. Det kan man godt gøre, og i det tilfælde at man gør det, vælger at gøre det og sige, at nu er der en standard her, som vi også mener, at arbejdspladser skal leve op til, ja, så vil det, som jeg sagde før, være et spørgsmål, om man kan sige, at indgrebet er proportionalt i forhold til det formål, som det er iværksat med henblik på at opnå.

Og det kommer jo an på situationen, hvis det er, der har været så meget svind i en forretning, så man mener, at et egnet middel til at undersøge det, det er at sætte video-kameraer op, ja, så må man sige, så kan det være proportionalt, men det kommer helt an på den konkrete situation.

Jeg vil sige, den der konkrete situation vil jeg ikke udtale mig om, det synes jeg ikke, jeg kender nok til den til. Men altså der lyder det, som om at - også hvis man skulle anlægge en menneskeretlig vinkel - at det vil være den samme konklusion, at det var en krænkelse af deres privatliv.

**Bjarne Petersen:**
Blot lige omkring det med lyd. Jeg ved ikke, om der var lydoptagelser også i forbindelse med den der Tøj & Sko butik.

**Laurits Rønn:**
Det var der ikke. Det tror jeg ikke.

**Bjarne Petersen:**

| |
|---|
| *Skjult aflytning foregår på arbejdspladser.* |

Det kan jeg godt forstå, du ikke tror. Men jeg ved konkret, at en bestemt leverandør af overvågningsudstyr til bagerbutikker har solgt tv-overvågningsudstyr med indbygget mikrofon, og det så at sige er blevet leveret til samtlige bagermestre, der er medlemmer af en bager- og konditormesterforening i Danmark.

Og der må jeg sige, at i og med man sælger det som sådan en serievare nærmest til en bestemt kæde eller en bestemt type butikker, så tror jeg ikke, der ligger bestemte grunde eller noget bestemt svind til grund for de der overvejelser for at anskaffe et udstyr.

**Laurits Rønn:**

| |
|---|
| *Jeg har ikke mødt en eneste sag om lydoptagelse.* |

Jeg skulle måske lige nævne, at med hensyn til lydoptagelse, så er det som udgangs-punkt ulovligt. Altså man må ikke optage lyd, og jeg har ikke mødt en eneste sag i min tid i Dansk Handel og Service, hvor vi har optaget med lyd, og hvad skulle det saglige formål også have været?

**Peter Christensen:**

*I hvilke situationer bør man bruge overvågning på arbejdspladser?*

Jeg synes, at vi nu hører, at arbejdsgiversiden siger, man skal have et godt formål for at installere videoovervågning og anden form for overvågning, og HK siger ligesom lidt defensivt, at så skal vi bare have noget information.

Det, jeg synes, der er behov for i det her forum, det er også at sige, vil man gå aktivt ud og for det første lave noget omkring de regler. Og for det andet, hvad er egentlig rådgivningen til arbejdsgiveren, fordi det kan ikke være rigtigt, at al den video-overvågning, vi sidder med i dag, at der er så stort et behov og for den sags skyld også med e-mail-overvågning. Så hvad er egentlig budskabet, i hvilken situation skal vi have det, og i hvilken situation skal vi ikke have det?

**Laurits Rønn:**

*Man overvåger, hvor der er en saglig grund til det.*

Det er jo sådan, at når man etablerer de her ting, så skal de have et sagligt formål. Altså man skulle jo sige, hvorfor investerer man de her penge. Der er nogle, der siger, at det nærmest er gratis, altså det er ikke tilfældet, altså det koster stadig en masse penge at lave videoovervågning.

Altså arbejdsgiveren gør det, fordi han mener, det er nødvendigt at gøre det i den konkrete sag her for at mindske det her svind. Der er ikke nogen, der gør det bare for at få videoovervågning i butikken.

**Bjarne Petersen:**

*Vi har siden 1994 forsøgt at få en aftale. Nu er der behov for en revision af loven.*

Jeg vil godt supplere og sige, at vi har faktisk siden 1994 forsøgt at få nogle aftaler igennem med Dansk Handel og Service om, hvordan og hvor man kunne bruge det her tv-overvågningsudstyr. Og det er ikke lykkedes overhovedet, og derfor så vi os også tvunget til efter overenskomstforhandlingerne i 1997 at gå til politikerne her i huset og sige: Nu må der ganske simpelt ændres på den lov, der er fra 1981, fordi udviklingen er ændret på alle måder, og vi kan altså ikke komme igennem med vores sædvanlige part på arbejdsgiversiden med at få lavet nogle aftaler om det område.

Og jeg vil godt sige, at selv om vi har fået revideret den lov, også på en måde, som vi i hvert fald dengang, den blev revideret, var tilfreds med, så må vi sige, så er udviklingen altså fortsat med galopperende hastighed siden da, og vi må sige, der trænger i den grad allerede nu til en revision af loven.

Og vi må også sige, at når vi får loven revideret, så kan det være, at vi også vil være i stand til at sætte os ned og lave nogle aftaler med arbejdsgiverne, men det skal være med udgangspunkt i en revideret lov, som tager udgangspunkt i bl.a. nogle af de ting, som vi har talt om her i dag. Hvor det er, at de overvågningsmuligheder, de kontrolmuligheder, de virkelig er tænkt ind i lovgivningen på en anden måde, end tilfældet er i dag.

Det er en forudsætning for, at vi overhovedet kan komme nogen steder med arbejdsgiverne, fordi de vil alene hele tiden pege på deres ledelsesret og også anvendelse af overvågningsudstyr som en del af deres ledelsesret. Og det er vi altså nødt til komme lidt videre væk fra.

**Janne Glæsel:**

*Måske formålstjenligt at få nogle sager om overvågning af ansatte på bordet, og få fastsat nogle retningslinjer efter persondataloven.*

Det, der kan undre mig, det er, at der ikke har været nogle sager i Registertilsynet og Datatilsynet for nylig omkring de her forhold. Fordi det lader til, at en del af den videoovervågning, der foregår, faktisk er ulovlig og på kanten af det, som de lovgivningsmæssige rammer opstiller. Og det kan man jo ikke ændre ved ny lovgivning.

Altså det kan man måske godt, men jeg synes, det ville være mere formålstjenligt så at få nogle sager på bordet og så fastsat nogle retningslinjer. Fordi vi har jo persondataloven, der har alle de her generelle kriterier om saglighed og formålsbestemthed og proportionalitet osv., så jeg synes egentlig, redskaberne er der, og det kan undre mig, at der ikke har været nogle sager.

**Kristian Jensen** (V):

*Hvor udbredt er videoovervågning i butikker?*

Nu hørte vi Bjarne Petersen sige, at der var en galopperende hastighed i udviklingen. Og det er jo lige før, man skal til at rede håret, inden man går ind i butikkerne, fordi man bliver overvåget og filmet. Kan I ikke prøve at fortælle, hvor udbredt er videoovervågning? Hvor stor en del af Dansk Handel og Services medlemskreds

bruger det her, fordi som det lyder nu, så lyder det, som om at det nærmest er en selvfølgelighed.

**Bjarne Petersen:**

*Krænkede ansatte ønsker ikke at rejse sag. Næsten alle butikker har i dag videoovervågning.*

Jeg vil godt lige tage fat i det først, som Janne rejser. Når ikke der er nogen sager, så vil jeg godt sige, at så skyldes det, som jeg sagde i mit indlæg, at de medlemmer, der henvender sig til os, de henvender sig, når det er, de ved en tilfældighed har opdaget, at de imod deres viden er blevet optaget - og ofte er blevet optaget i nogle situationer, som har været meget krænkende.

Og i den situation der reagerer de, som man åbenbart også gør i meget store tilfælde som voldtægtsofre. At man måske har lyst nok til at anmelde det og fortælle, men man har ikke lyst til at gå videre i en efterforskning. Man føler sig så dybt krænket, at man ganske simpelt ikke har overskud til at gå videre.

Og det er jo sådan, at vi kan altså ikke rejser sager, uden at medlemmet har sagt ja til, at vi kan rejse sagen for medlemmet, fordi det er jo medlemmet, som vi repræsenterer. Så vi kan ikke bare, desværre - og vi håber nu, vil jeg godt sige, at vi med den der sag fra den der Tøj og Skobutik rent faktisk får den sag, som måske kan være med til at sætte dagsordenen også fremover.

Men til det sidste, Kristian, med den der udvikling, der er, når jeg siger, at den er galopperende, så er det, fordi det er vores oplevelse fra næsten alle de butikker, vi besøger i dag, så er der et skilt på døren, at her foretages der tv-overvågning. Men det skilt om, at der foretages tv-overvågning siger måske godt nok, at der er tv-overvågning, men de fortæller ikke noget om omfanget af den tv-overvågning, der foregår.

Fordi det er jo det, vi bl.a. så får at vide, både af nogle flinke arbejdsgivere og også af vores medlemmer, det er, at der er sat kameraer op mange steder i butikkerne. Og der ved vi også, at med nogle af de desværre uheldige elementer, der også findes fra arbejdsgivers side, at der er der også nogle, der fristes til at sætte et kamera op, som er skjult for medarbejderne. Og det er måske de kameraer, som er de allerværste.

Der, hvor informationen foregår, jamen så er der ikke nogen problemer, det har jeg også sagt. Altså når man oplever kameraerne som værende en beskyttelse, så er det godt nok. Det er i det øjeblik, man oplever det som en kontrol, at tingene de bliver krænkende. Og det er, når det bliver sat op, uden at man er informeret om det. Og derfor må vi sige, at vi skal heller ikke gå og vente på, at sagerne kommer.

Vi skal ind og have forberedt og have lavet et holdningsskift eller få nogle diskussioner om, hvad er det for nogle konsekvenser, denne her overvågning den fører med sig. Hvad er det for nogle ting, der kan risikere at udvikle sig til sager. Men hvorfor skal vi have sagerne? Hvorfor kan vi ikke ligeså godt få stoppet tingene først?

Og der ser jeg i dag, at man kan prismærke på en måde, så i hvert fald nogle af værdierne de ikke behøver at forsvinde, fordi man med prismærkerne kan have noget tyverialarm, så hvis ikke varerne bliver deaktiveret, ja, så er det en alarm, der lyder, så værdierne behøver jo ikke at forsvinde. Og man kan i forhold til de der uheldige elementer også omkring dem, der opsætter udstyret, måske indføre en autorisations-ordning, så alene dem, der har rent mel i posen, også opsætter dette.
Fordi der er også nogle pirater, var jeg lige ved at sige, der tilbyder at opsætte de her ting for små populære penge, og det bliver ofte sat op i nattens mulm og mørke uden de ansattes viden.

**Ordstyrer:**
Det er sådan set skrappe sager, for i virkeligheden så siger du jo, at der er ikke nogen sager – men at det er fordi, at man føler sig så kraftigt krænket, at man ikke kommer frem med det.

**Laurits Rønn:**

| |
|---|
| *Vi har ingen interesse i dårlige forhold til vores medarbejdere. Men vi må erkende, at nogle medarbejdere stjæler.* |

Jeg kan ikke nikke genkendende til det, Bjarne siger. Jeg mener virksomhederne de er meget seriøse, når de opstiller det her overvågning, og de skilter også med det, når de opsætter disse kameraer. Der er stor seriøsitet. Vi har ingen interesse i at have dårlige forhold til vores medarbejdere, tværtimod. Altså vi lever af at have dygtige medarbejdere. Sure medarbejdere sælger ikke nogle varer.

Der, hvor jeg tror, at Bjarne og mine veje skilles, det er jo, at vi må erkende, at der er også nogle medarbejdere, der stjæler. Der er et svind på grund af medarbejdertyveri. Og der, hvor man har en konkret mistanke, der vil vi have en adgang til at opstille nogle kameraer, altså hvis der er skiltning oppe.

**Kristian Jensen** (V):
Men Laurits, er du enig i Bjarnes beskrivelse af omfanget. At det er alle steder?

**Laurits Rønn:**
Nej, det er ikke alle steder, på ingen måde. Jeg kan ikke sige, om det er 60 procent eller 70 procent, men det er ikke nær alle steder.

**Bjarne Petersen:**

| |
|---|
| *Vi holder ikke hånden over nogen, der stjæler.* |

Må jeg ikke godt lige sige omkring det, nu bliver ordet tyveri nævnt. Altså vi kunne ikke drømme om at holde hånden over nogle, der stjæler. Det kunne vi ikke drømme om. Men jeg vil godt, når vi nu så taler om tyveri, så prøve igen at fremvise sådan et lille dilemma, kunne man måske kalde det for. Altså den medarbejder, der stjæler for 9,95 bliver bortvist øjeblikkelig - ingen tvivl om det - selv om det bliver opdaget via optagelser på et kamera, som er skjult for medarbejderen, som medarbejderen ikke er informeret om eksisterer.

Altså der er sådan en lille smule skisma i, at man kan godt, den der ulovlighed ved at opsætte det her kamera eller ikke informere om det her kamera, det går man bare let hen over, men ham, der stjæler for 9,95 - ud af vagten, ikke.

**Laurits Rønn:**
Jeg kan kun konstatere, at vi overholder reglerne.

**Bjarne Petersen:**

| |
|---|
| *I overholder ikke altid reglerne.* |

Lad mig lige sige til det: Altså det er ikke i alle tilfælde, Laurits, så bare det der lille eksempel med skiltning. Den samme store koncern, jeg nævnte lige før, har en tendens til, at der skriver man ikke, at her er tv-overvågning. Her står der på skiltene, i hvert fald de steder hvor medarbejderne færdes: Her foretages vedvarende eller regelmæssig tv-overvågning. Det er teksten, skilteteksten, og det vil altså sige, at medarbejderne har ikke skyggen af chance for at kunne indrette deres adfærd, om hvorvidt der foretages tv-overvågning.

Og det er altså på områder, som altså ikke er kundeområder, men de områder, hvor medarbejderne måske opfører sig lidt anderledes end de områder, hvor der er kunder. Men der kan de ikke engang vide sig sikre på, om der så foretages overvågning.

## Hvor er Folketingets indsats påkrævet?

**Ordstyrer, Hanne Severinsen** (V), formand for Forskningsudvalget:
Vi starter igen, og vi skal jo så i gang med en debat om, hvor er Folketingets indsats påkrævet. Vi har strejfet det mange gange, det kan vi jo ikke undgå, vi er jo her. Men nu vil vi prøve at få en samlet debat, og så har vi fire oplæg først, og det er Jon Stokholm, der er den første.

**Jon Stokholm**, advokat, Formand for Advokatrådet

> *Når det teknologisk iler så stærkt, at en lovgivning er forældet fra det tidspunkt, hvor den træder i kraft, bør man måske finde et samspil mellem nogle grundlæggende standarder i lovgivningen og noget aftalemæssigt. Pas på med forhastet lovgivning. Der er ingen hurtige løsninger.*

Jeg vil dels sige noget om, hvor er Folketingets indsats nødvendig og påkrævet, og hvor er den ikke nødvendig og måske også lidt om, hvordan. Det var jo som Stalin sagde, at tillid er godt, kontrol er bedre. Det er måske det, der rammer, hvad det drejer sig om.

Men når man spørger: Hvordan er Folketingets indsats blevet nødvendig, så tror jeg, at det her møde afslører med al ønskelig tydelighed behovet for kvalitet i lovtilblivelsen og behovet for at undgå hurtige løsninger, for der er ingen hurtige løsninger. Det synes jeg er krystalklart i den debat, som vi har haft dagen i dag.

Det er jo paradoksalt, at en lov som vedrører fem, bliver genstand for den mest grundige behandling, man kan forestille sig herhjemme, nemlig lov om tredje generations mobilauktionen, som blev forberedt meget grundigt af ministeriet med høring af de berørte parter meget grundigt på ministeriet, Forskningsministeriets hjemmeside og med et forum, hvor de berørte parter kunne stille spørgsmål, og hvor man kunne debattere og med fornyet fremlæggelse af lovforslaget for de berørte parter.

Og da så bekendtgørelsen skal udmøntes om denne auktion, så sker det på samme måde igen i en meget, meget tæt dialog med branchen og brancherne og de berørte parter. Og der er slet ingen diskussion om, at den lovgivning, som blev forberedt på den måde, har en helt anden kvalitet end så megen anden lovgivning. Det er hævet over enhver tvivl, og det er jo også tankevækkende, at en sådan lovgivning, som måtte opfattes som kontroversiel af dem, den rettede sig til, til syvende og sidst endte med at få almindelig accept af alle, også af modstanderne, og høstede almindelig anerkendelse.

Og der blev også taget hensyn til de synspunkter, der kom i processen, og hvis der ikke blev taget hensyn til dem, så blev der givet en god begrundelse for dem. Og på

samme måde må jeg sige, at de lovgivningsinitiativer, der eventuelt skal tages her, bør tages i en bred offentlig debat, og de moderne hjælpemidler, som eksisterer bør at tages i brug på de her sæt.

Den lovgivning, som man i givet fald har, skal have en bred accept af dem, den retter sig til. Hvis den ikke har det, så har den sådan set ingen mening. Så jeg synes i virkeligheden, at den proces, som blev tilrettelagt for et ganske ringe antal aktører i det danske samfund, at den proces må være endnu mere relevant for det her, der vedrører os alle.

Jeg tror, at man skal diskutere måske noget sektorvis. Noget kan løses i en sektor og de reelle hensyn, der gør sig gældende, er forskellige fra sektor til sektor. Jeg tror også, at man skal se lidt på overvågning i det perspektiv, som også var fremme i morges lidt, omkring logning. Er det særlig acceptabelt og tilfredsstillende, at private firmaer, Klaus Riskjærs Cyberspace, skal fungere som opsamling, central oplagrings-central for dybt personlig kommunikation. Er det det, vi gerne vil have?

Normalt ville man vel sige, at det gjaldt om at få slettet så meget som muligt fra private firmaer af den karakter så hurtigt som muligt. Jeg tror også, at vi skal se på samspillet mellem de civilretlige regulatoriske muligheder og de offentligt retlige, det kan være de strafferetlige, det kan være de retsplejemæssige, det kan være de forvaltningsmæssige. Om meget i virkeligheden ikke lader sig løse i en kombination af noget civilretlig lovgivning, noget aftaleretlig lovgivning med nogle minimums-standarder og så aftaler.

Eksempelvis nogle mennesker har ikke noget imod, at deres dankortbetaling bliver registreret og fulgt, tværtimod er de interesseret i det. Andre ser det som pesten. Hvorfor ikke give folk et valg, et informeret valg. Men ser man civilretligt på det, så er det selvfølgelig en modernisering af aftaleloven, der måske skal til, nogle helt andre ting, der skal reguleres end dem, vi har i dag.

Det er måske også "Forbudsinstituttet", der skal tages op og "Retsværnetings-instituttet" må påkalde sig opmærksomhed i en international alder. Hvad er de økonomiske muligheder for at foretage retshåndhævelse for forbrydelser navnlig på nettet individuelt, får vi brug for "class-actions", altså for gruppesøgsmål, er det særlig relevant her? Det kan det meget vel være.

Hvordan sikrer man sig bevis og bevismidler i en sådan sag? Og der kan den drøftelse, der var om bevissikringen i en række retstvister, måske tjene til inspiration. Men når det bliver sagt, og det er med rette, at det her teknologisk iler så stærkt, så en lovgivning er forældet fra det tidspunkt, hvor den træder i kraft, så bør man måske finde et samspil mellem nogle grundlæggende standarder i lovgivningen og noget mere aftalemæssigt. Det tror jeg er frugtbart.

**Ordstyrer:**
Og næste er Anne-Sofie Dideriksen, værsgo.

**Anne-Sofie Dideriksen**, medlem af Teknologirådets Borgerpanel om overvågning

*Den rivende teknologiske udvikling medfører et behov for en tæt opdækning af lovgivning og retssikkerhed. Den enkelte borger må sikres stor medbestemmelse over, hvornår hun overvåges. Problem at børn ikke beskyttes mod overvågning af lovgivningen.*

I november sidste år gennemførte Teknologirådet en konsensuskonference om emnet elektronisk overvågning også her på Christiansborg. Og i den forbindelse blev et borgerpanel på elleve kvinder og mænd nedsat af Teknologirådet til at udarbejde en række anbefalinger på området. Og min opgave er her kort at gøre rede for de centrale vurderinger og anbefalinger, som vi i borgerpanelet i november år 2000 kunne danne konsensus om.

Anbefalingerne vedrører dels overvågningens konsekvenser for det enkelte mennesker og for samfundet, dels lovgivning og retssikkerhed. Og endelig har panelet givet anbefalinger vedrørende overvågning på arbejdspladsen.

I sit udgangspunkt lagde borgerpanelet vægt på, at den enkeltes beskyttelse mod overdreven kontrol og overvågning står i centrum. Panelet satte selvbestemmelsen højt, retten til at have indflydelse på, hvilken overvågning man udsættes for. I den sammenhæng understregede panelet også, at den enkelte dermed har et ansvar for at sige fra, når den enkeltes grænse er nået.

Går vi derefter ind på borgerpanelets første emneområde, de menneskelige konsekvenser af elektronisk overvågning, så lød den overordnede anbefaling, at overvågning ikke må erstatte den sociale kontrol. Desuden så panelet et problem i, at der ikke findes nogen lovgivning, som tager specielt hensyn til børns rettigheder. Panelet anbefalede, at der rådes bod på dette, så børn kan beskyttes mod overvågning, der ofte - det var i hvert fald panelets indtryk - opfylder voksnes behov for kontrol.

Borgerpanelet behandlede også overvågningens konsekvenser for samfundet og for fællesskabet. Og på det område var det panelets anbefaling, at omsorg og opdragelse skulle prioriteres højere end kontrol og overvågning. Man skal med andre ord ikke stjæle i en videoovervåget butik, fordi det kan opdages, men fordi man skal respektere den private ejendomsret. Det skal man opdrages til at forstå. Det skal man ikke trues til at lade være med. En løbende etisk debat om, hvordan vi f.eks. takler spændingsfeltet mellem den krænkende og den forebyggende overvågning, blev desuden efterlyst af panelet.

Det var dengang borgernes indtryk, at den rivende teknologiske udvikling medfører et behov for en særdeles tæt opdækning af lovgivning og retssikkerhed. Borgerpanelet vurderede f.eks., at persondataloven, som regulerer brugen og samkøringen af registrerede kundeoplysninger, kan sættes under pres, når telemedie-, forsikrings-, bank- og kreditvirksomheder samles i store enheder, der har en praktisk interesse i at sammenkøre registrerede kundeoplysninger.

Man kan ligeledes forvente, at forsikringsselskaber ønsker at gøre brug af helbredsoplysninger og dna-materiale i forbindelse med risikovurdering. Panelet anbefalede i den forbindelse, at persondataloven og andre love vedrørende overvågning til stadighed bør holdes øje med og revideres, så den kan blive ved med at beskytte den enkelte borgers kontrol over sine persondata.

Hvad angår den enkeltes retssikkerhed, vurderede panelet, at den retssikkerhed i forbindelse med overvågning med præventive formål, potentielt kunne krænkes. Overvågningsteknologi gør det muligt at fastslå ens blotte tilstedeværelse i nærheden af et gerningssted. Hvad hvis en omvendt bevisbyrde kunne komme til at gælde, så man ville være skyldig i en forbrydelse begået på stedet, indtil det modsatte var bevist?

Ud fra den antagelse at den enkeltes retssikkerhed i sådanne situationer ville kunne krænkes, anbefalede panelet, at gevinsten ved opsætningen af overvågningsudstyr nøje bør afvejes i forhold til den potentielle krænkelse af retssikkerheden. Og panelet efterlyste mere debat på området.

Overvågning på arbejdspladsen var det sidste område, panelet gav anbefalinger på. At medarbejderindflydelse skal prioriteres, og at der skal herske åbenhed og klare retningslinjer på den enkelte arbejdsplads, stod her øverst på listen. Helt overordnet anbefalede panelet for at styrke åbenheden og klarheden på den enkelte arbejdsplads, at arbejdsmarkedets parter udarbejder et sæt regler for indførelse og regulering af elektronisk overvågning, som ophæves til lov af Folketinget.

Panelet var også af den opfattelse, at medarbejderinddragelse er central for håndteringen af overvågningsproblematikken og f.eks. betydningen af overvågningsfri zoner, håndtering af data og placering af kamera osv. nøje overvejes i samarbejde med de ansatte.

Og som afslutning: Hvad alle 11 borgere således kunne blive enige om i november 2000 vil jeg her til slut sammenfatte i følgende nøgleord: Beskyttelse af børn, vægtning af omsorg og opdragelse frem for overvågning og kontrol, skarp opdækning af lovgivningen og klare spilleregler for overvågning på arbejdspladsen gennem dialog og samarbejde.

**Per Helge Sørensen**, forfatter, bestyrelsesmedlem i Digital Rights

*Der er sket et skred mod øget overvågning. På mange områder drejer man på teknologien for at muliggøre overvågning, ud fra en grundholdning om, at kommunikationsteknologi er noget, der kan overvåges. Ud over, at teknologien i sig selv giver en overvågningsmulighed, så tilretter vi også teknologien med henblik på overvågning.*

Jeg har haft den opfattelse, at en del af målet med denne her høring var at få et overblik over, hvad det er for en udvikling, der er sket på overvågningsområdet de sidste 10 år, kan man sige. Og derfor har jeg så i mit skriftlige oplæg forsøgt at beskrive den udvikling, og med frygt for at blive kaldt overvågningsparanoid, så kunne jeg ikke finde et bedre ord end et skred mod øget overvågning.

Jeg trækker i mit oplæg tre ting frem, som giver det skred. Dels den teknologiske udvikling, det forhold at vi bruger dankort i stedet for kontanter, læser aviser på nettet i stedet for fysisk, at vi overvåger med kamera i stedet for med personer gør, at der bliver registreret en masse oplysninger, som bliver brugt i forbindelse med efterforskning af kriminalitet. Og det giver i sig selv en øget overvågningsmulighed og forrykker balancen mellem staten på den ene side og borgeren på den anden side.

Der er i dag folk, der har forsøgt at negligere det problem med at sige, at der bliver skabt så mange data, og det forsvinder i mængden, men det må jeg sige, at det kan jeg ikke se noget tegn på. Der er ingen tvivl om, at der bliver skabt utrolig mange data via de her mobiltelefoner i alle de her master rundt omkring, men det har jo tilsyneladende ikke været noget som helst problem at finde de data, der tilhører ham her Kurt Thorsen. Det har heller ikke været noget problem at finde de data, der tilhører Rasmus Trads, at bruge dem i forbindelse med efterforskningen af den sag.

Og jeg synes, at man må simpelt hen konstatere, at for 10 år siden havde de data ikke fandtes, og de findes nu, og de bliver brugt. Og det er det samme, vi ser på en række andre teknologiske områder. Det er ikke det eneste, der giver en øget overvågnings-mulighed, fordi ud over at teknologien i sig selv giver en overvågningsmulighed, så tilretter vi også teknologien med henblik på overvågning.

Og der syntes jeg, at vi faktisk hørte noget af det mest interessante, der er blevet sagt i dag - jeg tror, at det var Troels Ørting Jørgensen, der sagde, at Internettet giver utrolig mange muligheder for anonymitet. Det er altså ikke Internettet i sig selv, der gør, at vi kan blive overvåget mere. Man kan sagtens drive Internet uden at give overvågnings-mulighed. Det er der tilsyneladende et antal Internetudbydere, der gør.

Når vi får en øget overvågning, så er det, fordi vi tilretter Internettet f.eks. med krav om at lagre oplysninger tilbage i tiden, fordi vi ønsker, at den overvågningsmulighed skal være til stede. Og Internettet er ikke de eneste eksempler på det. Diskussionen af

kryptering og tilsvarende diskussion, der har været diskussion om anonyme taletidskort, som i hvert fald visse lande har forsøgt at bremse udbredelsen af. Og man ser på en masse andre områder, at man rent faktisk drejer lidt på teknologien for at muliggøre overvågning, som teknologien ikke af sig selv havde givet.

Det sker tilsyneladende ud fra sådan en grundholdning om, at kommunikations-teknologi det er noget, der kan overvåges. Men sådan behøvede det jo ikke at være. Jeg synes, jeg underholdt nogle af jer i pausen med det her kørselsafgiftssystem. De folk, der laver kørselsafgiftssystemer, de ved godt, at overvågning det er en død sild, hvis man vil lave kørselsafgifter. Så de har faktisk lavet et kørselsafgiftssystem, som ikke kan overvåges, hvor der ikke er en central server, der ved, hvor alle bilerne er, men hvor det kun er den enkelte bil selv, der ved, hvor den er og opkræver penge på et taletidskort.

Sådan kunne man også have lavet mobiltelefonsystemer. Sådan kunne man måske også have lavet Internet, men det har vi ikke ønsket, og det er ikke et tilfælde, at det ikke er blevet sådan. Det er jo eksplicit besluttet, bl.a. ved at efterretningstjenester og politiet deltager i standardiseringsarbejdet, at vores kommunikationsteknologier bliver anderledes indrettet.

Jeg synes også, at man kan måske kan sammenligne Internettet med vores traditionelle postsystem og sige, jamen er det guds givet, at vi skal kunne dokumentere kommunikation på Internettet et antal måneder tilbage i tiden. Man kan jo, som jeg hørte i dag, begå alvorlige forbrydelser via Internettet.

Man kan fremkomme med trusler, man kan sprede racisme, og man kan sprede børneporno. Men så vidt jeg ved, så kan man ikke sprede miltbrand, og det kan man altså ved det traditionelle postsystem. Så hvorfor skal vi ikke have små kameraer på postkasserne, så vi kan se, hvem der er den anonyme afsender af brevene. Hvorfor er det virkelig guds givet, at vi i et kommunikationssystem, der skal vi kunne spole tilbage og se, hvem der har kommunikeret med hvem.

Det sidste fakta, jeg trækker frem i mit oplæg, det er så jeres ansvar, om jeg så må sige. Det er det politiske skred, der er sket i og med, at man bl.a. har undtaget en række forbrydelser fra det her straframmekrav på seks år. Man gjorde det med spredning af børneporno, man er så vidt jeg ved, ved at gøre det med kvindehandel, og mon ikke også der kommer noget om finansiering af terrorisme, som vil ligne.

Og man ser fra gang til gang, fra enkeltsag til enkeltsag, der ser man åbenbart, at forbrydelserne, på trods af at de ikke har så høj en straframme, alligevel er så alvorlige, så vi ønsker aflytning. Jeg synes, L 194 giver også et eksempel. Der har man gjort op med det grundlæggende krav, at det kun er folk under mistanke, som kan udsættes for overvågning i og med, at man går ind og kigger på lister over alle de folk, der kommer forbi et gerningssted. Man orienterer dem ikke bagefter. Igen, man skruer lidt ned for

betingelserne for at bruge denne her overvågning, på trods af at overvågningen jo faktisk er blevet mere indgribende på grund af teknologien.

**Efterforskningsmidler og den elektroniske overvågning**
Og der er også ting i udlandet, som peger på, at der er mere på vej af samme slags. Man har Europarådets konvention om IT-kriminalitet, hvor man tænker sig, at adgang til trafikoplysninger, altså f.eks. positionsoplysningerne for mobiltelefonen, jamen det skal kunne ske i forbindelse med enhver forbrydelse begået via en computer, altså helt udnytte alvorlighedskrav.

Og det er de tre ting, jeg trækker frem. Jeg ved ikke, om man kan være uenige i, at det har givet et skred, og det har forrykket balancen mellem staten og borgeren. Man kan selvfølgelig overveje, om man ønsker det skred. Men man må sige, at der er ingen tvivl om, at det skred vil fortsætte, hvis man ikke gør noget. Teknologien vil blive mere og mere præcis, mobiltelefoner vil kunne give oplysninger om positioner helt ned til ti-fem-tre meters nøjagtighed. Vi vil bruge Internettet mere og mere, så skredet vil fortsætte, hvis der ikke bliver grebet ind.

Og jeg synes måske, at det var værd at træde et skridt tilbage og sige: Jamen hvis vi nu kunne beslutte det, ønskede vi så et samfund, hvor at man kan stedbestemme samtlige borgere med få minutters tidsinterval med fem meters nøjagtig, ønsker vi et samfund, hvor man til enhver tid kan spole et halvt år tilbage og dokumentere en given borgers kommunikationsmønster.

Der er ingen tvivl om, at sådan et samfund vil være utrolig effektivt til at bekæmpe kriminalitet. Men der er måske så nogle andre ting, der er gået tabt i sådan et samfund. Hvis vi ikke ønsker det samfund, så skal I gøre noget, eller så skal I holde op med at gøre det, I gør, eller hvad det nu er. Jeg peger i mit oplæg på to punkter, man kan gribe ind. Jeg tror ikke, at man kan forhindre den teknologiske udvikling, og jeg tror heller ikke, at vi kan stå imod, at når oplysningerne ligger der, når mobiltelefonerne er blevet mere præcise, så vil vi selvfølgelig også bruge det i efterforskningen.

Men man kan godt lave kørselsafgifter, der ikke kan overvåges eller kørselsafgifts-systemer. Og det vil sige, at man også lave kommunikationssystemer, som ikke kan overvåges. Det vil sige, man kan godt lade være med at gå ind og påvirke den udvikling. I det mindste kunne man lade den flyde af sig selv i stedet for at påvirke den til at sikre overvågning.

Og jeg mener også, at man kan lade være med at give efter for det skred i enkeltsagerne og mindske barriererne for at benytte de efterforskningsmidler, som den elektroniske overvågning giver mulighed for. Og det var sådan set min kommentar.

**Peter Landrock**, professor, administrerende direktør i Cryptomathic

*Hvorfor er kryptering ikke mere udbredt, hvilke barrierer er der, og hvem er de væsentlige aktører? Får man fat i et certifikat, kan man kommunikere sammen og kryptere, uden besvær. Problemet er, at den infrastruktur, der skal til, mangler.*

Jeg er blevet bedt om at tale om kryptering med udgangspunkt i diskussionen om det såkaldte Echelon overvågningsnetværk. Mit indlæg har måske en lidt teknisk karakter, men jeg skal prøve at lade være med at gøre det for teknisk. Nogle af de ting, vi debatterer her i dag, har vi også debatteret i regeringens IT-Sikkerhedsråd, og da vi først hørte om Echelon, diskuterede vi selvfølgelig også det.

Der var så en, der sagde," at det er også utroligt, altså jeg er efterhånden meget påpasselig, når jeg taler i telefon. Jeg siger slet ikke noget vigtigt", hvortil jeg sagde: Jeg er meget mere forsigtig. Man ved aldrig, hvem der lytter, så jeg siger principielt aldrig noget vigtigt. Så det kan I have i baghovedet, når jeg nu går videre. De spørgsmål, jeg vil adressere, det er: Hvorfor er kryptering ikke mere udbredt, end det er? Hvilke barrierer er der for en mere udbredt kryptering, og hvem er de væsentlige aktører?

Der er en række betingelser af praktisk karakter, der skal være opfyldt, for at det kan lade sig gøre at kryptere. Som minimum skal man have en Softwarepakke. Det er faktisk sådan, at stort set alle brugere har en sådan softwarepakke, for det ligger nemlig i den browser, man bruger. Der ligger både Microsoft, der ligger i Netscape, og det er i og for sig i princippet ret nemt at bruge. F.eks. i Microsoft Outlook Express kan man under tools klikke på encrypt og i Netscape er det under options. Og hvis I går hjem og undersøger jeres browser og klikker jer igennem, så vil I kunne se, at I kan komme til at kryptere.

Det, der bare er problemet, det er, at den teknik, man benytter, det er den såkaldte public-key teknik, hvor man har et par af nøgler. Man får genereret sig et par af nøgler, der passer sammen ligesom et par ordbøger. Man har en offentlig nøgle og en hemmelig nøgle. Og for at jeg skal kunne modtage noget, kryptere en information fra f.eks. Per, så skal han have fat i min offentlige nøgle. Ligesom hvis han skal ringe til mig, så skal han have fat i mit telefonnummer.

Måden, man løser det på, det er ved hjælp af det, der hedder et certifikat, så man har nogle såkaldte certificeringscentre, som uheldigvis i dansk lovgivning er kommet til at hedde nøglecentre, men det er altså et certificeringscenter, som udsteder et certifikat, der knytter en bestemt person og hans eller hendes e-mailadresse til denne her nøgle, man skal have fat i.

Og når man kommunikerer med en person, som har fået udstedt et sådant certifikat, så bliver den nøgle, der skal bruges, den bliver automatisk lagret. Så hvis man bare får fat i sådan et certifikat, så kan man faktisk kommunikere sammen og kryptere, uden at det er særlig besværligt.

Hvordan får man så fat i sådan et certifikat? Ja, det er jo derfor, vi har certificerings-centre, vi har i hvert fald to offentlige aktører på det område i Danmark, nemlig Kommunedata og TeleDanmark, og nu hedder det jo ikke det mere. Og jeg vil også lige sige, man skal igennem en større proces for at få sådan et certifikat, fordi man skal selvfølgelig identificeres. Og jeg kan ikke lade være med at fortælle - med fare for, at det bliver misfortolket - at vi har i over et år på vores egen webside haft et certificeringscenter, hvor man kan få udstedt sådan et certifikat for sjov.

Med det mener jeg, at vi går ikke igennem en identifikationsproces, men I kan få, I kan generere jeres nøgler, I kan få et certifikat, og så kan I kommunikere med en hvilken som helst anden, som har fået udstedt et sådant certifikat. Så jeg vil i og for sig opfordre jer til at prøve det.

Og så er spørgsmålet bare: Hvor let er det? Jamen det er nøjagtig lige så let eller endnu lettere end at lære, at en fransk hest hedder "cheval", og sådan er det bare hele vejen igennem. Man skal klikke måske en ti forskellige steder, og det betyder så, at hvis man ikke man får klikket rigtigt, så er der 1.023 muligheder for at være gået galt i byen. Og det er faktisk det i sig selv, der gør, at det bliver lidt kompliceret.

Finanstilsynet har på sin hjemmeside en vejledning liggende i sikker e-mail. Og den burde egentlig ikke være på mere end tre sider. Det burde kunne lade sig gøre at lave en sådan løsning, men den er på 91 sider. Og det er faktisk problemet, vi har. I princippet er det let, det er bare ikke tilstrækkeligt brugervenligt. Men alle har så mulighed for at lave kryptering.

Hvilke alternativer er der? Jamen altså browsere og e-mail bruger en speciel syntaks. Der er også en anden syntaks, altså syntaks har så noget at gøre med i hvilken rækkefølge, tingene kommer osv. Og der er en anden syntaks, der hedder PGP, og der findes stand alone, som er baseret på PGP, så man også kan downloade.

Jeg kender masser, der bruger det, så hver gang jeg får noget fra dem, så er det både signeret og krypteret, og jeg er i og for sig ikke særlig interesseret i at bruge tid på det. Det er det, jeg kalder for sikkerhedsforurening. Det kan også lade sig gøre fra en række firmaer at købe plug-ins og hvad ved jeg, så det egentlig kunne blive brugervenligt.

Men problemet er altså, at vi har ikke den infrastruktur, der skal til. Vi mangler telefonbøgerne. Det svarer egentlig lidt til, at vi alle sammen havde en telefon, men alle numrene var hemmelige, alle. Så hvis vi skulle telefonere til hinanden, så skulle vi mødes og udveksle vores telefonnumre. Det er den situation, vi står i.

**Den amerikanske forbindelse**
Regeringens Sikkerhedsråd holdt i foråret 2000 en høring med forskellige firmaer, som leverede Software til kryptering, og der blev det slået fast, at der findes masser af firmaer, der tilbyder stærk kryptering, altså kryptering, som i princippet ikke kan brydes. Og når jeg nu har nævnt amerikanske produkter, så er det jo, fordi uheldigvis er der kun udbredte amerikanske browsere, og i dem er der som sagt krypterings-faciliteter.

Så er spørgsmålet bare: Kan vi nu stole på de her amerikanere? Dertil vil jeg sige, at det er vigtigt at gøre sig klart, hvem er fjenden? Hvis det er således, at man er bange for National Security Agency, NSA, i USA, så bør man måske tænke sig om en ekstra gang, men det er vel ikke det, de fleste er bange for. Og jeg tvivler på, at NSA er interesseret i den typiske danske borgers e-mailkommunikation.

Men jeg er af den personlige overbevisning, at i de løsninger, vi i dag ser fra USA, der er der ingen såkaldt bagdør. Det ville jeg egentlig håbe, at der var, fordi så ville vi have meget nemmere ved at sælge vores produkter, for der er jo ingen bagdør. Men når jeg siger det, så skal det ses på baggrund af den udvikling, vi har set de sidste 8-10 år. Der har tidligere været det, man kaldte for kommerciel kryptering, og det var, fordi krypteringsværktøjer i USA er klassificeret som våben af anden karat, og det betyder, at de dengang ikke måtte eksporteres.

Våben af første karat, altså håndvåben og sådan noget, det er ikke noget problem, men krypteringer, det er noget farligt stads. Og derfor kunne man kun eksportere de løsninger, hvor 16 af de 56 bits blev stillet til rådighed til National Security Agency. Det betyder altså ikke, at det blev nemmere for os andre at bryde det, for vi andre havde heller ikke adgang til de 16 bits, vi skulle igennem samtlige 56. Men for et par år siden ophævede den amerikanske regering eksportrestriktionerne, så i dag er der stærk kryptering i de løsninger, som kommer fra USA.

Der er så nogle, der vil hævde, at der ligger nok stadig væk noget, NSA kan bruge. Jeg tror ikke på det, jeg har arbejdet sammen med IBM og Microsoft i mange år, og jeg tror simpelt hen ikke på det. Men hvis det er det, I er bange for, så er det altså kun NSA, der kan aflytte jeres kommunikation, det er ikke alle de andre. Så konkluderende må man sige, der er mulighed for at kryptere, hvis man er interesseret i det. Det, vi mangler, det er en infrastruktur, altså vi mangler telefonbogen.

## Spørgsmål fra Folketingets spørgepanel og afsluttende debat

**Ordstyrer:**
Jeg har allerede et par markeringer. Den første er Kristian Jensen.

**Kristian Jensen** (V):

*Kan social kontrol erstatte teknisk kontrol?*

Anne-Sofie Dideriksen du var inde på at sige, at opdragelse er bedre end kontrol. Og det tror jeg ikke, der er nogle, der kan være uenige i - i det omfang, at opdragelse kan klare opgaven. Var I også inde og diskutere i borgerpanelet, i hvor stort et omfang, at opdragelse kan klare opgaven? Altså i hvor stort omfang, I tror på, at opdragelse kan erstatte en vis form for kontrol?

**Anne-Sofie Dideriksen:**

*Social kontrol er at foretrække, men kan ikke stå alene.*

Nej, vi har jo netop diskuteret, at det ikke handlede om enten det ene eller det andet. Der er social kontrol, og så er der også mere håndfast kontrol. Og selvfølgelig er social kontrol det, som man på mange måder kommer længst med. Men vi er jo kontrollerede i vores samfund på alle mulige måder, så selvfølgelig kan vi ikke klare os med den sociale kontrol alene.

Så vi har ikke diskuteret det på den måde, at vi foretrak det ene frem for det andet. Vi har sagt, at man kan afveje, og man kan foretrække, at den sociale kontrol overvejende regulerer vores adfærd og ikke en kontant teknisk kontrol.

**Thomas Adelskov** (S):

*Hvordan kan vi sikre børnenes rettigheder?*

Nu sad jeg lidt langt fra en mikrofon i formiddag, men der blev det bragt op og nu igen her i eftermiddag omkring børns retssikkerhed. Det er jeg egentlig lidt optaget af, og den diskussion der er omkring overvågning i forhold til børn i daginstitutioner.

Er der nogen af jer, der kan give nogle bud på, hvad kan vi som politikere gøre for at sikre børnenes rettigheder i denne her sammenhæng. Og der blev også rejst et spørgsmål tidligere i dag om, hvordan det hang sammen i forhold til Børne-konventionen, altså den overvågning som finder sted i visse daginstitutioner i dag.

Min umiddelbare rygmarvsreaktion er, at det synes jeg faktisk, at vi skulle gå ind og kigge alvorligt på, for det virker på mig som et overgreb, men hvordan er retsstillingen, og har I nogle bud på, hvad man kunne gøre i den situation?

**Anne-Sofie Dideriksen:**

*Vi anbefaler lovgivning.*

Ja, i borgerpanelet har vi konkret anbefalet en lovgivning på området, for der er ikke nogen lovgivning, der beskytter børns rettigheder. Hvordan den konkret skal udformes, og hvilke hensyn der skal tages, og hvor langt man kan gå, har vi ikke diskuteret i detaljer. Det er også jeres arbejde langt hen ad vejen.

**Birgitte Kofod Olsen:**

*I de situationer, hvor der er videoovervågning i vuggestue og børnehave, må børns privatliv anses som krænket - men der er ikke nogen lovgivning, der beskytter børns rettigheder.*

Ja, jeg har en kommentar til det. Det er sådan, så børnekonventionen bygger jo på det helt grundlæggende princip, at børn er ligeværdige parter i forhold til voksne. De har rettigheder fuldstændig, som vi har rettigheder. Børn har også en ret til privatliv. Og jeg har ikke arbejdet særligt med børns rettigheder på det her område, men det er min umiddelbare betragtning, at børns privatliv i de her situationer i vuggestue og børnehave må anses som krænket.

Det blev også rejst tidligere af Tove Videbæk, om man kunne forvente eller stille et krav om, at børn skulle høres i de her sammenhænge. Det kan man ikke bygge på børnekonventionen, børnene er for små til, at det er noget, der er relevant. Men der er helt klart behov for, synes jeg, i Danmark, at man går ind og ser på, hvordan vi kan implementere børnekonventionen også på det her område og få sat nogle regler op for, hvordan vi behandler børnene her, og hvordan vi varetager deres rettigheder.

**Thomas Adelskov** (S):

*Er overvågning i institutioner også en krænkelse af pædagogerne?*

Det synes jeg lyder meget tilfredsstillende i forhold til, hvordan jeg selv reagerede. Altså jeg kommer også uvægerligt til at tænke på en anden sag. Nu har vi jo siddet og hørt på arbejdsgiver- og arbejdstagerdiskussionen i forhold til handels- og serviceområdet.

Men jeg tænker også på de pædagogmedhjælpere, de pædagoger, som arbejder i daginstitutionerne, at det må siges at være en overvågning, der i hvert fald overskrider den overvågning, der direkte finder sted i en butik, hvor det måske er butikschefen, der sidder og kigger efter.

Så der må et eller andet sted her også være en overskridelse, i hvert fald af nogle ansatte, altså nogle personalegruppers rettigheder, eller i hvert fald den norm, som tidligere har eksisteret på deres arbejdsplads.

**Per Helge Sørensen:**

*Nye teknikker er på vej til at overvåge større børn.*

Bare en enkelt kommentar. Jeg tror, at det er et vigtigt område, fordi jeg tror, vi vil også for de lidt større børn se en udvikling her. Man kan allerede se, f.eks. et tysk firma, der tilbyder en tjeneste om overvågning via mobiltelefon, hvor forældrene så kan få en SMS i det øjeblik, at det her barn går længere end en eller anden radius fra nogle givne områder fra hjemmet eller skolen. Eller kan logge sig ind på en tjeneste og se, hvor barnet befinder sig.

Der er også folk, der er ivrige for at sælge forældre software, så de kan følge med i, hvad børnene har sagt i en chat på nettet, hvor de er surfet hen. Og det er selvfølgelig alt sammen for børnenes skyld, det er der ingen tvivl om, for at beskytte børnene mod pædofile, eller mod hvad der ellers kan ske. Men jeg tror, at man kan finde en afvejning, eller jeg tror, at der er behov for en afvejning i forhold til børnenes privatliv, også i forhold til de lidt større børn og den type teknologi.

**Jon Stokholm:**

*Hvordan vil vores børns holdninger blive præget af overvågningen?*

Man kan i hvert fald konstatere, at børnene ikke er repræsenteret ved høringen i dag, så vi må jo prøve at improvisere for dem så godt, vi kan. Men jeg tror, Peter Blume havde fat i noget centralt i morges, da han pegede på, at holdningerne måske er forskellige over generationerne og udvikler sig med generationerne.

Og det giver vel anledning til at fokusere navnlig på børnene og den kommende generation. Og hvad bliver deres holdning og bevidsthed omkring det her, og hvad er det for nogle oplevelser, de får, og hvordan bliver deres holdninger egentlig præget til det her fremover? Det tror jeg må gøre, at vi skal sætte fokus på børnene.

Men det gør vel også, at vi skal sørge for, at de modeller, de reguleringsmodeller, vi udvikler, skal være moderne og måske anderledes end dem, vi hidtil har brugt. Og

have en vis fleksibilitet, så der er plads til legitime holdninger, som yngre har, og som vi andre, der sidder her, ikke har.

**Ordstyrer:**
Skal vi forlade det emne? Så går vi videre til Knud Erik Hansen.

**Knud Erik Hansen** (SF):

*Hvem kan hjælpe med til, at kryptering bliver mere udbredt?*

Jo, tak. Jeg vil godt spørge Peter Landrock: Når du siger, at kryptering, altså vi mangler den der telefonbog, og når vi samtidig har oplevet gennem mange år nu, at forskellige interesser har gjort, at vi ikke har fået adgang til kryptering, så det ikke fungerer - der er stadig væk det der lille led, der mangler, til at det skal fungere, og markedet ikke har klaret det.

Hvilke aktører skal så faktisk træde ind, for at det kommer til at fungere? Er det det offentlige, der har en rolle i at sige: Nu skal vi gå ind og sørge for, at det her fungerer? For det er vel sådan, at hvis det ikke er udbredt, så er det lidt ligegyldigt. Hvis det kun er en tiendedel af mine venner eller hvem, jeg skal kommunikere med, der har det, så er det jo lidt ligegyldigt, fordi så bruges det ikke. Det kræver ligesom et vejnet, som vi alle sammen er på. Hvem er de aktører, der mangler, som skal træde ind, for at kryptering kommer til at fungere?

Så sagde du omkring bagdør, at du tror det ikke. Men er sandheden ikke, at hvis vi skal have et samfund, og specielt et samfund, hvor vi bliver mere og mere afhængige af at have al den her elektroniske kommunikation, så må det være ultimativt, at de programmer, vi får, at der var nogle, der skal tjekke det, og det kan du kun, hvis du har kildekoden - at du kan se kildekoden. Ellers har du ikke en jordisk chance for at tjekke det.

Det er også et af de krav, vi er nødt til at stille, hvis vi skal være helt sikre på, at der ikke er bagdøre. Og som det sidste, og det er så en til jer alle lidt, fordi jeg oplever, at det, vi snakker om nu, er nogle data, der er meget forskellige fra, hvis man har et stykke papir, der ligger på et kontor. Altså det er egentlig forholdsvis svært at flytte. Nu kan man ganske vist fotokopiere, men det er svært at flytte - men det, der kendetegner det, vi snakker om her nu, det er elektroniske data, som er utrolig lette at flytte, og som svæver alle mulige steder hen.

Og hvis vi så også tager nogle systemer, som det, vi har opbygget omkring Schengen-samarbejdet, der er kæmpe dataer. Så kan det godt være, at vi laver sikkerhedssystemer og alt mulig andet, men ved godt, at der er mennesker, der bruger det, og at der meget let ligesom kan være nogle forskellige kulturer, som gør, at de bliver misbrugt.

Tilsvarende også, hvis ISP-udbyderne skal til at logge data, hvordan kan vi reelt sikre, at de her data ikke bliver misbrugt, fordi de her data netop er flygtige? Og kan det ikke få den konsekvens, at vi siger, at hvis vi virkelig skal forhindre overvågningssamfundet og misbrug, så må konsekvensen være, at vi mest mulig som et hovedprincip skal begrænse lagringen af de her data? Ellers er vi ude på et skråplan, som vi ikke kan kontrollere. Eller kan vi stole på de systemer med alle de regler, vi kan lave herinde i Folketinget?

**Peter Landrock:**

*Hvis man interesserer sig for at give den enkelte borger adgang til kryptering, er det i stort omfang et spørgsmål om at lave det mere brugervenligt. Det er svært at forestille sig, at det vil blive videre udbredt, medmindre staten går foran.*

Det første, du spørger om, det er, hvad der mangler. Det er i stort omfang et spørgsmål om at lave det mere brugervenligt. Og hvem der skal betale? Fordi det er svært at se, hvordan et certificeringscenter, som altså skal til for at udstede de her certifikater, hvad det nu end er. Det er svært at se, hvordan de skal kunne leve af det.

Og i det omfang, at man interesserer sig for at give den enkelte borger adgang til kryptering, så har jeg svært ved at forestille mig, at det vil blive videre udbredt, medmindre staten går foran. Jeg tror, at det ellers vil blive noget, som man bruger i virksomheder, og det bruger man jo allerede på nuværende tidspunkt i en række virksomheder.
Det er meget typisk for en virksomhed med flere afdelinger, at man har sat et såkaldt VPN op - jeg tror, det var Peter, der var inde på det tidligere i dag - Virtual Private Network, hvor de har bokse mellem afdelinger, som automatisk krypterer alt, hvad der er imellem afdelingerne.

Det har vi selvfølgelig også i vores firma mellem vores afdelinger i udlandet. Så i det omfang er vi beskyttet. Men det er altså et praktisk problem. I fredags var jeg på Mercedes museum i Stuttgart og så de gamle biler dér og blev mindet om, at da de første biler kørte, da skulle der gå en mand foran og svinge med en lygte. Altså selvom om vi har algoritmerne osv., så på det rent brugermæssige område dér er vi ikke nået meget længere, end dengang i bilens barndom. Og det er i og for sig dét, der er problemet mere end noget andet, det er ikke det at lave algoritmerne. Det er brugervenligheden.

Og hvis borgeren skal have almindelig adgang til kryptering, så er jeg bange for, at staten bliver nødt til at tage en aktiv rolle og måske bære nogle udgifter. Med hensyn til bagdøre og kildetekst - det er jo ikke sådan, at fordi den enkelte borger får en kildetekst, at han så kan afgøre, om der er bagdøre i eller ej. Det er faktisk de allerfærreste, der kan afgøre det. Så dér tror jeg i og for sig nok, at man bliver nødt til at bero sig på nøjagtig

samme principper, som når man køber en bil og får at vide, at den har ABS-bremser, og så regner man med, at de virker hver gang. Altså det er et spørgsmål om tillid til den virksomhed, som leverer varen.

Og jeg vil stadig væk sige med hensyn til amerikanske produkter: Altså det er kendte algoritmer med en meget stor nøglestørrelse, så fjenden i den sammenhæng, hvis du er nervøs, det er National Security Agency. Og personlig vil jeg ikke være nervøs for, om NSA kan gå ind at læse mine private e-mails.

**Per Helge Sørensen:**

*Kan Folketinget modstå fristelsen til at overvåge?*

Ja, det var i forhold til det her med adgang til data. Nu har jeg jo primært forholdt mig til forholdene mellem staten og individet, og dvs. i praksis politiet, efterretningstjenesterne og borgeren. Og da må jeg sige, at i det forhold er jeg egentlig ikke så bekymret for misbrug. Altså jeg har faktisk stor tiltro til, at politiet og PET overholder retsplejeloven og ikke misbruger de data.

Der, hvor misbruget desværre sker, og hvor man må forudse et misbrug, hvis vi registrerer, det er jo faktisk ovre hos jer. Jeg tror ikke, at I kan lade være med, hvis vi forestiller os f.eks., at vi lavede et kørselsafgiftssystem, hvor der var en central server, som registrerede, hvor alle bilerne var. I det øjeblik, der er nogen, der er blevet voldtaget ude i Vestskoven, og der har været kørt en bil forbi, så tror jeg ikke, at I kan holde til at lade være med, at give lov til at bruge de data.
Og det er derfor, at jeg tror - som jeg også skriver i mit skriftlige indlæg - hvis man skal gøre noget ved den her udvikling, jamen så skal man nok kigge på teknologierne og sige: Jamen i hvilken udstrækning vil vi tillade eller fremme teknologier, hvor der ikke registreres data, og i hvilken udstrækning vil vi kræve, at der gemmes data, der muliggør en overvågning?

For jeg tror ikke, at der er nogen, der politisk - og når vi hører den sag i dag her med børneporno - der er vel ikke nogen i det her rum, der ikke ærgrer sig over, at du ikke kunne få den IP-adresse. Det tror jeg ikke, at der er. Så i det øjeblik data er der, ligesom med masteoplysningerne, idet data var i de master og vi vidste, at man faktisk kunne se, hvem der er i nærheden af et gerningssted via de masteoplysninger, så kan vi ikke holde til at sige: Jamen det skal vi ikke bruge, vel. Fordi vi kan opklare alvorlige forbrydelser.

Og derfor tror jeg, at hvis man skal gøre noget ved denne her problemstilling, så er teknologien, det er et vigtigt sted. Det er vigtigt at vurdere, jamen skal vi gøre som forskerne på DTU, der laver kørselsafgift. TeleDanmark ringede jo til dem og sagde: Det dér det kan vi godt lave. Vi skal bare lægge en mobiltelefon i hver bil. Det vil være langt billigere, det vil være langt nemmere. Det kan implementeres i morgen. Men de

forskere deroppe de sagde: Nej, det kan vi ikke leve med, for det kan overvåges. Er det sådan, vi vil have, at vores teknologier skal være, eller skal de være ligesom dem her? Og dér er en vigtig beslutning.

**Jon Stokholm:**

| |
|---|
| *Misbrugsmuligheder er blevet meget større. Vigtigt at kunne revidere love jævnligt.* |

Jamen jeg tror, at Knud Erik Hansen da har helt ret i det, du påpeger, at misbrugsmulighederne er blevet meget, meget større, end de var for papir- og hulkortmediet. Og hvad kan vi så bruge det til? Ja, vi kan bruge det til at konstatere, at der er nogle love - der står i de love, I giver - nemlig naturlovene, havde jeg nær sagt. Det kan vi jo ikke lave om på.

Det, vi så kan, det er jo så at sige: Så må vi indrette den lovgivning, vi har, på ryggen af de naturlove, der nu er, og måske gøre det med en vis ydmyghed og en vis forsigtighed. Og det er derfor, jeg peger på, at det civilretlige element måske ikke er noget dumt sted at starte.

For dit spørgsmål er jo båret af en eller anden tanke om, at når vi nu så har alle disse misbrugs- og omgåelsesmuligheder, så vil de også blive brugt, altså. Den altovervejende hovedregel i det her samfund er jo ikke civilretlig ulydighed, det er civilretlig lydighed. Og måske skal man basere sig sådan set på det kernetilfælde og ikke på det marginale, det sygelige tilfælde. Men så nøjes med at fastslå, hvad man ikke vil acceptere, og så måske nogle retsmidler mod det, som man ikke vil acceptere, og så se, hvordan dét virker.
Jeg tror i det hele taget, at revisionsbestemmelser på det her område er en god ting. Sådan at den lovgivning, man end går ind og laver, at man følger den op hurtigt og ser, hvordan virkede så det her, som vi nu lavede, for vi kan ikke overskue alle konsekvenser af det, vi laver. Og måske også i den lovgivning, vi laver, har noget, jeg vil kalde overvågning, at Folketinget og berørte parter jævnligt overvåger: Hvordan fungerer den lov om overvågning, som vi nu har lavet?

**Ordstyrer:**
Birte Weiss, vil du have ordet nu?

**Birte Weiss** (S):
Jeg vil gerne spørge Landrock: Kunne man forstå dig på den måde, at du reelt mener, at det er prisen for en digital signatur, der er den egentlige barriere?

**Peter Landrock:**

*Det koster penge at gøre kryptering og elektronisk signatur mere brugervenligt.*

Jeg vil lige sige, at selvfølgelig er der, selv om det er de samme teknikker, vi bruger til digitale signaturer og kryptering, så er det selvfølgelig to aspekter af samme sag. Men altså digital signatur er selvfølgelig ikke kryptering, men det er i og for sig den samme principielle problemstilling. Ja, jeg mener, at medmindre vi får det gjort meget mere brugervenligt, så får vi det aldrig udbredt, og det koster altså penge at gøre det mere brugervenligt, ja.

**Knud Erik Hansen** (SF):

*Offentlig kildekode kan kritiseres.*

Det var bare lige en kort kommentar til Peter Landrock: Når du siger det der med, at det er klart, at ingen af os kan kontrollere sådan en kildekode, hvis vi får den altså. Men der er jo den der tredje option, ved at den er offentlig, om jeg kan se det, så er den til offentlig gennemskuelse, og dvs., at eksperter som du og andre kan gå ind og rejse kritik af den. Og det er jo det, der vil ske - altså hvis man har sådan en offentlig kildekode.

**Peter Landrock:**

*Tror ikke, at offentlig kildekode vil løse problemet.*

Ja, men skal jo selvfølgelig kompileres. Og spørgsmålet er så, hvor man henter den kildekode, og hvordan kan man være sikker på, at man downloader den rigtige kildekode? Og hvis man bruger et chipkort, så er det jo ikke sådan, at man kan downloade en kildekode og lægge det ind i chipkortet.

Det er ikke helt så enkelt. Men noget, man kan gøre, det er jo, når man sælger sådan et produkt, så kan man lade det blive vurderet af en uafhængig tredjepart, inden det bliver kompileret, og den tredjepart kan være med til kompileringen. Og hvad der ligger i det, det er, at kompilering gør altså, at koden kan køre på en bestemt platform, og det skal den jo gøre, når det skal kompileres, før den kan bruges.

Så det der med kildekode, det mener jeg er et pseudoproblem. Vi skal i hvert fald kunne afgøre, at den kildekode, jeg har, den er så identisk med den kildekode, som jeg tror, jeg har fået udleveret. Så der skal vi også lægge noget ind, ikke? Jeg tror i og for sig ikke, det i sig selv vil løse problemet. Noget andet er, så skal vi også være sikre på, der ikke er trojanske heste, som omgår kildekoden. Og det er endnu sværere.

**Per Helge Sørensen:**

*Borgerne skal føle, at de får noget for at bruge kryptering.*

Det er til det med udbredelsen af kryptering af digital signatur. Jeg tror ikke, der er nogen vej uden om, at det vil ske langsomt og gradvist i samfundet, og jeg tror, prisen skal betragtelig under nul, før at man kan få folk til at bruge digital signatur. De skal simpelt hen have noget for det, ligesom man får noget for - i overført betydning - at bruge sin homebanking. At det bliver nemmere, livet bliver nemmere. Derfor bruger man homebanking, men man ved jo ikke, at man bruger kryptering, men det gør man jo altså, for ellers var der ikke noget homebanking system.

Og derfor vil jeg tro, at vi vil se kryptering udbrede sig der, hvor man får noget for det: Over for kommunikation med det offentlige, hvis vi får nogle tjenester i det offentlige, som er attraktive og gør vores liv nemmere, i kommunikation mellem virksomheder, hvor der kan spares penge.

Og det sidste sted er nok i virkeligheden i de her private e-mails, hvor vi vel - altså én ud af 100, så er der nok en af de her e-mails, som vi nok egentlig gerne ville have haft krypteret, som måske handler om nogle familiære forhold eller helbredsmæssige forhold. Men det er ikke nok.

Og frygten for NSA er nok for de fleste af os ikke nok til - eller det er vel helt åbenlyst, de her tjenester eksisterer, Peter Landrock har gratis sat mærkater på sin hjemmeside - men frygten for NSA er ikke nok til, at vi vil tage det her til os, selv om det er gratis.

Og der tror jeg, vi vil se en organisk udvikling af det her, det bliver meget svær at fremme. Og det eneste sted, hvor det vil være anderledes, det er de mennesker, der frygter Ørting Jørgensen, og som får noget for at bruge kryptering, nemlig at de ikke længere kan blive aflyttet af politiet, og det er vel et af de steder, hvor man også vil se det udbredt ret hurtigt.

**Jon Stokholm:**

*Virkeligheden har overhalet den digitale signatur.*

Jeg kunne tilslutte mig det, du siger, og et helt klassisk eksempel på det, er jo den udvikling, vi har haft omkring den digitale signatur i Danmark. Hvor nogen har arbejdet med det i meget lang tid på højplan juridisk grundlag, og der er ikke kommet ret meget ud af det endnu. Og at det virkelige liv reelt har overhalet dette højplan juridiske arbejde, der siger: Vi kan ikke vente på, det bliver færdigt, og så må

vi leve med nogle mangler ved det, vi nu får. Og der er sikkert svagheder og bevismæssige svagheder, og hvordan vil domstolene se på det. Den tid den sorg.

Og det er jo det, man gør i Erhvervs- og Selskabsstyrelsen i øjeblikket med deres web-rake, som alle tilslutter sig. Altså vi har i vores medlemskreds købt digital signatur til alle 4.200 advokater, og det sælger vi til dem, og det har vi givet 25 kr. for pr. stk. Og det er dog noget, som Erhvervs- og Selskabsstyrelsen har en interesse i, for så får de pludselig en masse brugere på en gang. Og sådan tror jeg, udviklingen bliver drevet frem af det virkelige liv.

**Kristian Jensen** (V):

*Gør globale forbrydere det ikke nødvendigt med en global efterretnings- og efterforskningsvirksomhed?*

Per Helge, jeg synes, at du har haft ret i, at udviklingen i de sidste 10 år viser, at der er gået et skred i udvikling mod overvågningen, fordi teknikken er til stede. Og jeg tror, du har meget ret i, at når teknikken er til stede, så vil den blive brugt.

Vi kan også se spørgsmålet med roadpricing, vi har meget delte holdninger i Folketinget om roadpricing, men der er også en del af de partier, der er modstandere af roadpricing, der siger: Hvis det kommer, så vil vi også bruge de oplysninger, der er, såfremt der kommer oplysninger, der kan bruges i efterforskningen.

Men jeg synes, dagen har vist, at vi har et meget skarpt dilemma, fordi vi på den ene side har et helt legitimt ønske som borger om ikke at blive overvåget, når vi bevæger os frit, men et lige så legitimt ønske om, at vi også bevæger os trygt og dermed, at der ikke er nogen, der vil os det ondt. At der er en sikkerhed i det samfund, vi har, og i den verden, også den verden som Troels Ørting Jørgensen beskrev.

Der har forbryderne jo fundet ud af at bruge teknikken, Internettet, kommunikations-mulighederne. Du var meget afvisende for at udvide muligheden for aflytning, men er globaliseringen i kriminalitet ikke en faktor, der nødvendiggør en globalisering af efterretningstjeneste- og efterforskningsvirksomhed?

**Jørn Bro:**

*Overvågningen i dagligdagen er langt mere betydningsfuld end efterretningstjenesternes.*

Ja, det er jo en både spændende og væsentlig høring, som faktisk spænder meget vidt fra NSA, der opererer på det store strategiske niveau og over til omklædningsrummet i Bilka. Der er grund til at tage fat på de problemer. Men jeg må sige, jeg er mest

optaget af de nærliggende problemer, som kan ramme den enkelte borger. Og her er vi jo sådan ganske taktfuldt gået uden om nogen af de centrale statslige overvågningssystemer: Automatisk hastighedskontrol, roadpricing, indsamling af alle mulige data vedrørende folks medicinforbrug. Her er jo virkelig overvågning, så det basker noget.

Hvorimod jeg er helt enig med Peter Landrock, at hvem er egentlig fjenden, når vi anskuer det i det store billede? Jeg er et hundrede og femogfirs procent sikker på, at NSA er fuldstændig hamrende ligeglad med 99,999999 pct. af, hvad der siges og gøres og tænkes i det danske samfund på det område. Men det er da rigtigt, at der er et behov for, at enkeltpersoner og virksomheder skal have adgang til at kunne beskytte sig imod måske konkurrenter eller ondskabsfulde naboer, eller hvad ved jeg, der griber ind i deres tilværelse igennem sådan en overvågning.

Jeg vil også gerne sige, at Politiets Efterretningstjeneste interesserer sig ikke for overvågning. Vi interesserer os for at have rimelige efterforskningsmuligheder, svarende til den teknik, eller den teknologi, som vi ved, at de kriminelle bruger. Og de er hele tiden et pænt stykke foran os. Vi halser bagefter. Og det er det, der i virkeligheden bekymrer os.

Vi ved også, at med den kapacitet, vi har i dag, er vi nødt til at være - og det er godt, det er jeg meget tilfreds med - da er vi nødt til at være usandsynlige selektive for ikke at drukne i det rene pladder og vrøvl. Så man skal ikke være så bange for at give myndighederne - så længe vi har det nuværende politiske system - rimelige efterforskningsmuligheder. Og den dag vi får et andet politisk system, så er det ret ligegyldigt, hvad vi synes.

**Per Helge Sørensen:**

*Elektronik giver nye muligheder for overvågning. Er vi sikre på, at vi pr. automatik bør udnytte de muligheder. Er elektronisk kommunikation virkelig så effektivt et middel for f.eks. forbrydere, at vi bliver nødt til at overvåge den?*

Jamen jeg synes det er et godt spørgsmål, om det her med elektronisk kommunikation, er det så effektivt, så vi bliver nødt til at overvåge det? Hvis man laver nogle sammenligninger med den fysiske verden, jeg har allerede draget den til almindelig post, jamen enhver kan sende et brev.

Og når man også ser USA i dag, er det tilsyneladende ret svært at spore, hvor det kom fra, og man kan godt forårsage en del skade via et brev. Man kan også sprede børneporno via et brev. Og der har vi så levet med åbenbart i mange år, at det kan ikke spores.

Altså vi hørte tidligere i dag nogen sige: Jamen bare fordi det er elektronisk, så kalder I det overvågning. Jeg synes faktisk, situationen ofte er omvendt. Bare fordi det er elektronisk, så skal vi kunne overvåge nogle situationer, som den fysiske verden, vi har accepteret, vi ikke kan overvåge.

Jeg må sige, jeg kan gå ind i en bar, og så kan jeg smadre en ølflaske ned i hovedet på en eller anden fyr, og så kan jeg skride igen, og hvis jeg bare ikke har brugt mit dankort, så er det sgu nok svært at finde ud af, at jeg var der, og hvem jeg var.

Flere internetudbydere, Jubii og Teledanmark, eller i fald Jubii, de registrerer deres chatrooms, fordi de vil ikke have, at man bare kan gå ind i et chatroom og fremkomme med trusler mod nogen. Det skal vi registrere 2 måneder tilbage, så vi efterfølgende kan se, hvem der foretog sig hvad.

Jeg kan se måske i børnechatrooms, der er en særlig ting. Men det her handler jo også om voksnes chatrooms. Man kan altså ikke slå nogen ned i et chatroom. Er vi så sikre på, at det her elektroniske kommunikation er så meget anderledes, så meget mere effektivt, at det bliver vi nødt til at overvåge? Eller er det bare, fordi vi kan? Det spørgsmål synes jeg, man må stille.

**Søren Søndergaard** (EL):

| |
|---|
| *Kan der opstå problemer med omvendt bevisførelse?* |

Altså sådan rent personligt så har jeg det meget med denne her overvågning, at det er fint nok, hvis bare det rammer de skyldige, og problemet er jo så lidt, hvem de skyldige er, ikke. Og derfor kunne jeg godt tænke mig i forhold til Anne-Sofie Dideriksen og det, som I har skrevet fra panelet omkring retssikkerhed i forhold til overvågning - hvor I rejser problemstillingen om omvendt bevisbyrde, at det kan blive et resultat af overvågning, at man frembringer en tilstand, hvor man reelt sætter folk i den situation, at de skal bevise, at de ikke har begået en ulovlighed.

Så vil jeg spørge: Er det noget, I vurderer kan ske hen ad vejen, eller er det noget, I bygger på nogen reelle problemer i dag? Og det er måske også lidt til Stokholm, i forhold til om Advokatrådet har nogen erfaringer inden for det område.

**Anne-Sofie Dideriksen:**

| |
|---|
| *Omvendt bevisførelse var også en af vores overvejelser. Handlepligten er også interessant at diskutere.* |

Med den omvendte bevisførelse så var det en vurdering. Det var noget, vi mente måske ville kunne ske - eller vi rejste det som en måske spørgende vurdering, hvad hvis nu, er

retssikkerheden så truet. Altså det er et spørgsmål, man skal arbejde med ind i overvejelserne hele tiden. Vi er ikke jurister, så vi er ikke eksperter på det område. Men vi så det som en problemstilling, som vi synes, man skal medtænke.

Jeg vil gerne lige nævne en anden problemstilling angående retssikkerheden. Vi interesserer os også en del for loven om handlepligt, fordi overvågeren - en, som overvåger en station f.eks. eller lignende - kan sidde meget langt fra det sted, der bliver overvåget og har ingen mulighed for at gribe ind. Der anbefaler vi også, at man skulle medtænke, om der kommer til at gælde noget andet for den overvåger, som muligvis vil komme ud for, at der skete en forbrydelse, som vedkommende ikke kan forhindre eller gribe ind i. Altså dækker loven om handlepligt den nye situation, der er?

For den blev jo lavet med det for øje, at man f.eks. ved en trafikulykke, hvor man står lige ved siden af, har pligt til at gribe ind og handle. Hvad gør man så, når man fysisk er langt væk, men kan se på et kamera, hvad der sker? Det er også et aspekt til retssikkerheden.

**Jon Stokholm:**

*Omvendt bevisførelse er ikke det store problem med dansk retspleje.*

Det sidste skal jeg som ikke kunne sige noget om, men om det første: Omvendt bevisbyrde, det ville jeg tage forholdsvis let, sådan som dansk retspleje fungerer. Som anklagemyndigheden og danske domstole fungerer, er man meget, meget opmærksomme og meget bevidst omkring det her, og jeg kan slet ikke forestille mig, at det her skulle udvikle sig hen i noget, der bare smagte af omvendt bevisbyrde. Så det ville ikke være en fare, jeg ville være særlig bekymret ved.

**Peter Blume:**

*PET og FE er ikke omfattet af persondataloven*

I den forbindelse kan man jo, jeg vil gerne nævne, at en af mine udmærkede kolleger, Mads Bryde Andersen, på et tidspunkt havde den opfattelse, at hvis man nu tillod kryptering og ligesom sagde, at der ikke måtte være, nu siger vi, der heller ikke var, nogen bagdøre, vi havde tilstrækkelig stærk kryptering, så den ikke kunne brydes, ja, så skulle det være således, hvis man så blev udsat for en politimæssig efterforskning og ikke selv ville dekryptere sit program, at det så talte imod en. At det havde det, som vi lidt fint kalder en procesretlig eller processuel skadevirkning, en slags omvendt bevisbyrde, kunne man godt sige.

Vi har jo også, vil jeg lige nævne, omkring vore venner i PET, at det er jo rigtigt, at retsplejeloven gælder jo PET, men det er interessant at konstatere, at persondataloven

f.eks. ikke gælder for PET ej heller FE, hvad den jo godt kunne med visse modifikationer, men det gør den så ikke.

Fordi selv om PET måske ikke overvåger - på en måde er det overraskende for nogle af os, men lad os bare sige, de ikke overvåger - så har de i hvert fald nogle registre, nogle oplysninger, og de er altså ikke omfattet af den lovgivning, der specielt gælder for, hvordan man nu skal behandle personregistre. Men det bliver der sikkert lejlighed for Folketinget på et eller andet tidspunkt, når de der udvalg, man har nedsat omkring efterretningstjenesterne, kommer med deres betænkning.

**Thomas Adelskov** (S):

*Er der positive sider af overvågning med ny teknologi?*

Ja, nu ved jeg ikke, om det har noget at gøre med generationerne, det er der jo blevet talt en del om i dag. Nu er jeg selv en af dem, der har børn i børnehaver. Det kan bekymre mig, jeg vil ikke være en af dem, der aktivt arbejder for en overvågning dér. Men når vi taler om overvågning, så har vi i dag i hvert fald talt meget om den negative side af overvågning, altså fra borgerens synspunkt. Der er sådan set også, og det er der egentlig ikke rigtig nogen, der er kommet på, positive sider af overvågning med den ny teknologi.

Altså jeg tænker på, at Thorsen han er formodentlig i dag rimelig glad over maste-oplysninger, som jo har været med til i hvert fald at gennemhulle nogle af Tradses anklager mod ham omkring datoer og steder. Jeg tænker på, jeg kan kontrollere min bank langt lettere, end jeg kunne først, da jeg fik mit Dankort, hvor jeg var afhængig af min udskrift, og som i øvrigt kom med længere og længere mellemrum, medmindre jeg ville betale formuer for det. Jeg tænker på min mobilkonto, som jeg kan gå ind på, på Internettet og så kan kontrollere dag for dag, time for time, hvis jeg har lyst til det.

Og så tænker jeg også på, at med den ny teknologi får vi også nogle muligheder for at kunne gå ind og se, hvad det offentlige har af informationer på os. Nu tænker jeg på den digitale forvaltning, som jo giver mig som borger nogle muligheder for at se, hvad er det for nogle oplysninger, der ligger omkring mig, og måske også kunne gå ind og se, hvem har sidst hentet oplysninger om mig.

Altså hvilken forvaltning eller institutioner har sidst hentet oplysninger, og hvad er det for nogen oplysninger, de har hentet om mig, sådan at jeg altså som borger kan være med til at overvåge de institutioner, som omgiver mig i langt højere grad og giver mig dermed nogle overvågningsmæssige muligheder.

Og det synes jeg ikke i dag, vi har været inde på, men måske er en af de positive sider - i stedet for at vi bare hele tiden har konstateret her i dag, at teknologien den løber af sted derudaf, så har teknologien for borgerne også positive elementer.

**Jon Stokholm:**

*Nogle borgere opfatter overvågning som en stor fordel.*

Jeg synes, du har helt ret, og det er derfor, jeg synes, at man skal lade det der indgå i den reguleringsmodel, som man udvikler specifikt til den her problemstilling, at der er nogle borgere, som opfatter det som en stor fordel, og som griber disse her ting med stor kyshånd og gerne vil have det.

Og så skal man da tænke sig om at lave en præceptiv lovgivning og sige, dette kan ikke lade sig gøre, dette vil vi ikke have, det er forbudt, hvis der var en betydelig del af befolkningen, som på informeret grundlag siger, vi synes, det er alle tiders, det lever vi helt fint med, og vi synes, fordelene i hvert fald er større end ulemperne.

Og derfor tror jeg måske, at vi skal lave en specifik kombination af noget lovgivning og noget, kan man sige, nogle standarder, som kan indgå i noget civilretligt, med nogle specifikke retsmidler. Så det tror jeg faktisk er vejen frem.

**Per Helge Sørensen:**

*Det er noget dybt i alle mennesker, at man ikke kan lide at blive overvåget.*

Jeg synes også, det var interessant at se, for det var jo både Thorsen og Trads, der var utrolig glade for de masteoplysninger, da de stillede frem. Den ene var gladere end den anden. Man har endnu ikke set Fehår, eller hvad han hedder, han var vist ikke så glad, vel. Men altså jeg ved det ikke rigtig, for det er en del af en større argumentation, man kan sige, hvis vi gennemfører et gennemkontrolleret samfund, så vil vi ikke alene kunne fange alle de skyldige, vi vil også kunne frikende alle de uskyldige.

Med det argument så burde vi, altså der er stadig væk 30 pct. af os, der ikke har en mobiltelefon, vi burde jo give dem en chip, så vi havde positionsoplysningerne på dem, så vi kunne beskytte dem imod at blive uretfærdigt anklaget. Altså det burde vi jo gøre den dag i morgen, ikke sandt. Det er jo et godt og fornuftigt formål at beskytte folk, beskytte borgerne, mod en uretfærdig anklage fra staten osv.

Men der er alligevel et eller andet, der skurrer, ikke, og på en eller anden måde tror jeg, at der er et eller andet dybt menneskeligt i, at man nok helst selv vil bestemme, hvornår man bliver overvåget og selv kunne bestemme, når man bliver mødt med en anklage, hvordan man svarer igen på den anklage. Altså jeg tror heller ikke, de her teenagere, hvis deres forældre forærede dem nogle mobiltelefoner, så de kunne se, hvorfor de kom for sent hjem om natten. Altså de kunne jo også blive frikendt for alle mulige ting, ikke sandt.

Men jeg tror, der er noget grundlæggende menneskeligt, der gør, at vi bryder os ikke om at blive frikendt på den måde. Altså vi vil hellere være uskyldige og så kunne forsvare os på andre måder. Der er i hvert fald noget, der skurrer i baghovedet på mig.

Men hvis man virkelig mener det, så må vi da se at få udbredt overvågning, så lad os gøre det ordentligt, ind i bilerne og ud med nogle chips, og noget DNA-register også, ikke sandt, så vi er helt sikre på, at der i hvert fald ikke er nogen uskyldige, der bliver dømt.

**Peter Landrock:**

*Der er jo registreringer og oplysninger, der er til borgerens fordel. Vi skal passe på, at vi ikke forbyder de gode sider ved overvågning.*

Jamen der er et vigtigt aspekt, som du måske overser dér. I forbindelse med kryptering så taler man om key escrow, når man skal have fat i sessionsnøglen, det vil sige, når der er nogle andre, der skal have fat i den, altså myndighederne - hvorimod du, hvis du selv har tabt den, og du har brug for at dekryptere det, du har adgang til, så taler man om key recovery. Og key recovery det har en positiv klang, og key escrow har en negativ klang.

Og det, du er inde på dér, det er jo registreringer og oplysninger til din egen fordel, og det, du er inde på, det er, du vender det hele tiden om på, hvordan andre får adgang til de oplysninger. Jeg kan kun give dig ret i, at jeg er himmelhenrykt for, når jeg får mine statements fra bank osv., at der er tilstrækkelige oplysninger, til at jeg kan identificere betalingen, og jeg vil også gerne kunne gå mine mobilsamtaler igennem.

Men jeg ønsker ikke, at offentlige myndigheder uden videre kan få adgang til det, det er sådan set problematikken, ikke. Og det er selvfølgelig en kendt problematik, og det må vi forholde os til. Og så det, Stokholm siger, så skal vi passe på ikke at lave en lovgivning, der er så ufleksibel, så vi får forbudt de gode sider af det.

**Anne-Sofie Dideriksen:**

*Vi har et dobbelttydigt forhold til overvågning.*

Det var til, hvad Per Helge Sørensen sagde. Vi formulerede meget i borgerpanelet, at vi nok må lære at leve med, at man via overvågning får kastet en eller anden form for dobbeltsyn på sig. Altså man er potentiel skyldig, men man nyder også godt af de ting, der sker. Når du går ind i supermarkedet, er du en potentiel tyv, fordi du bliver

overvåget som en, der kunne finde på at stjæle. Du har også fordele af det, fordi kameraet registrerer også den, der har haft fingrene nede i kassen og ikke dig.

Og jeg vil bare understrege, at vi diskuterede det ud fra det synspunkt, at det dobbeltsyn er der, og det eksisterer, og man må prøve at holde fast i sig selv. Sådan lidt populært sagt, holde fast i, at det dobbeltsyn er der, men man har sit eget individuelle syn på det også og kan oprette sin egen ukrænkelighedssfære og privatsfære. Man har et ansvar for også at sige fra over for overvågning, man har et ansvar for at tage stilling til den overvågning, der omgiver én og et krav på at blive beskyttet mod den.

**Ordstyrer, Hanne Severinsen** (V):
Jon Stokholm, du har flere gange understreget, at der er også ting, man ikke skal lovgive om. Og nu hedder overskriften jo, »hvor er Folketingets indsats påkrævet«. Hvor er Folketingets indsats ikke påkrævet?

**Jon Stokholm:**

*Vi skal skabe mulighed for, at folk selv definerer en "beskyttelsessfære" mod overvågning.*

Det er jo svært at svare på det. Det er den vel f.eks., hvis man går ind med for generel en regulering, som siger, der er visse ting, som vi simpelt hen ikke vil acceptere, hvis der er en betydelig del af befolkningen, der siger, jamen det lever vi helt fint med, og vi lever helt fint med de risici, så har man valgt en gal reguleringsform.

Og det er måske nok så meget dér, jeg vil hen og sige, vi skal ikke så meget ned og fokusere på en regulering om, hvad man vil have, og man ikke vil have, men finde nogle procesformer, sådan at med tilstrækkelig sikkerhed så får folk det, de gerne vil have. Og får defineret den beskyttelsessfære, som Anne-Sofie i og for sig påpeger fra borgerpanelets side: At hver enkelt selv udvikler og selv definerer og får skabt mulighed for, at hver enkelt selv kan definere den beskyttelsessfære, som vedkommende vil have, men selvfølgelig får den fornødne bistand og gør det på et informeret grundlag.

Men når den så er defineret, så er der tilstrækkelige retsmidler - effektive - sådan at den også skal håndhæves, og sådan at borgerne ved under hvilke betingelser, andre bryder den. Det tror jeg måske er den vej, man skal tænke.

**Troels Ørting Jørgensen:**

*Man kan vende tingene på hovedet og spørge, hvilken sikkerhed har borgerne for, at vigtige oplysninger kommer til politiets kendskab.*

Jeg har lige en enkelt kommentar, fordi det var vel det, som Per Helge sagde med voldtægten i Vestskoven og roadpricing. Der vil jeg give ham ret, fordi jeg tror, at hvis man så en voldtægt af en kvinde, der var blevet voldtaget af tre mænd og blevet molesteret og ydmyget i 4 timer og blevet kylet ud af en bil i Vestskoven, så ville politiet gøre, hvad de kunne for at opklare den sag, det er der ingen tvivl om.

Og hvis det indebar, at vi ville forsøge at få en dommer til at afsige en kendelse om, at vi kunne få adgang til roadpricinglokaliteterne, de positioner, de biler, der har været der på det givne tidspunkt, så vil vi gøre det. Og hvis ikke at der var hjemmel til det i lovgivningen, så ville vi i Justitsministeriet skrive til Folketinget og bede om, at man tog det op. Og så er det jo igen ikke vores afgørelse, men så er det jo Folketingets afgørelse: Hvor ligger balancen henne?

Men jeg var også glad for, at du nævnte, at du var ikke så bange for politiets misbrug, og det tror jeg faktisk heller ikke, at der er nogen grund til. Men jeg vil stadig vende tilbage til det, som jeg nævnte i mit eget indlæg omkring autorisationen: Hvor er det, de fleste hemmeligheder om os ligger henne? De ligger hos ISP'en, er vi ikke enige om det? Det er ham, der har passwordet, det er ham, der shuffler rundt med alle vores mails, det er ham, der har adgangen stort set.

Det er ham, vi skal spørge ad om at udlevere tingene efter kendelse. Hvilken sikkerhed har jeg som borger for, at disse oplysninger i virkeligheden bliver omfattet og opbevaret tilstrækkelig sikkert, og det mener jeg ikke, der er nogen reguleringer om faktisk, sådan som tingenes tilstand er nu. Og igen så mener jeg, man vender tingene på hovedet. Det er myndighederne, man er bange for, men hvem er det egentlig, som sidder med informationer, og hvem er det, der skal reguleres i første omgang.

**Jon Stokholm:**

*Forholdet mellem folk ved computerne og folk hos ISP'en er retsløst.*

Jeg tror, Troels peger på noget centralt, og det må jo aftaleretligt løses i princippet, nemlig forholdet mellem de forskellige folk, der sidder ved deres computere derhjemme og disse centre, det er jo fuldstændig retsløst. Det kunne man jo godt prøve at se lidt på, hvordan skulle det egentlig reguleres på en hensigtsmæssig måde, hvilke rettigheder har man egentlig i den henseende, og hvor er den minimums-beskyttelsessfære, man skal have i en sådan situation som borger. Det synes jeg er meget interessant at kigge på.

**Per Helge Sørensen:**

*Ikke et retsløst område. Lov om autorisation giver kun mulighed for at fange de dumme kriminelle.*

Jeg mener ikke, området er retsløst. De ISP'er de er dækket af persondataloven, og de skal selvfølgelig overholde den persondatalov, og den sige meget præcist - Janne kan forklare det bedre - men at de må lagre de oplysninger, de selv har brug for, og de må gemme dem indtil det øjeblik, hvor de ikke længere har brug for dem.

Og hvis de overtræder det, jamen det er jo ikke meget anderledes end FDB, der har et kontokortsystem, de har også en hel del oplysninger på folk, der har det her kunde-kort, og de er jo ikke autoriseret til at drive brugsforretning, går jeg ud fra, men de overholder forhåbentlig persondataloven.

Jeg ser nok ikke helt det behov for en autorisering af ISP'erne - nu bliver det sådan lidt telepolitik - det er simpelt hen imod den udvikling, vi ser af en decentralisering af hele teleområdet. Jeg tror, at i det øjeblik, hvis der blev vedtaget en lov, der pålagde Internetudbydere at gemme de her data, så har du jo vel meget af det, du skal bruge, for så ville alle de store virksomheder, som har hovedparten af kunderne, de ville selvfølgelig overholde den lov. Og i det øjeblik, I så opdager, der er en ISP, som ikke har de data, som de er forpligtet til at gemme i henhold til den lov, jamen så kan I gøre noget ved det, ikke sandt. Der er vel ikke behov for en autorisation.

Jeg tror, den seneste udvikling, man har set i USA, det er, at sådan nogle private communities de køber trådløse netværk, sætter op rundtomkring på hustagene, og så tilbyder de alle naboerne, at nu kan de komme på nettet via deres ADSL-forbindelse. Og det er sådan en græsrodsting, som jo egentlig er utrolig smuk, og andelstanken og sådan noget, at man deler sin Internetforbindelse.

Og derfor tror jeg ikke, man kommer nogen vegne med autorisation, og desværre, som du også selv var inde på, så kommer man med et lovkrav om at gemme desværre nok heller ikke de aller alvorligste kriminelle til livs, uanset om man havde autorisation eller lovkrav eller kun lovkrav. Fordi de allermest alvorligt kriminelle vil vide, hvordan man laver sin egen ISP eller kobler sig på via sådan et trådløst netværk, der lige står der, eller hvad de ellers kan.

Så vi er i den sædvanlige situation desværre, at vi kan fange de halvalvorlige og de smådumme, og dem er der jo mange af, det erkender jeg, at kriminelle er tilsyneladende ikke blandt de kvikkeste, vel, men de allermest alvorlige, terroristerne måske, dem får vi nok ikke på den konto.

**Kristian Jensen** (V):

*Man kan skifte sit teleselskab ud, men man kan ikke skifte staten ud.*

Troels, det, du siger dér, det er, at de private sidder med oplysningerne, derfor skal vi være varsomme dér. Der er den forskel, at hvis jeg er nervøs for, om mit teleselskab, min Internetudbyder eller FDB misbruger mine oplysninger, så kan jeg skifte dem ud. Det er meget, meget mere vanskeligt at skifte staten ud, og derfor er der jo en forskel, fordi du har en valgmulighed, når det drejer sig omkring de private, der kan logge nogle oplysninger, og så over for det, som offentlige myndigheder logger på.

Og der har Jørn Bro jo meget ret i, at det er mange oplysninger, der bliver logget i det offentlige system - ikke bare af politiet, men af alle mulige andre - som også giver en mulighed for, at man kan sammenkøre, overvåge og kontrollere.

**Troels Ørting Jørgensen:**

*Ønskeligt med større gennemsigtighed på ISP-området.*

Jo, men det, jeg pegede på, det var såmænd bare som almindelig borger en smule større gennemsigtighed på det her område her. Når jeg går ud for at finde mig en internet-udbyder, så går man jo som sædvanlig efter den billigste, ikke, og så tror jeg, at de alle sammen er lige gode, at de alle sammen er TeleDanmark eller Sonofon eller sådan noget.

Og det er jo bare det, at det ved jeg ikke, og der er jo ikke nogen aftaleret. Hvad er det egentlig, de må, når jeg går ind på en hjemmeside. Der er jo masser af de her udbydere, de lokker jo med alt mulig bevægelse og alt muligt andet, så de bagefter præcis kan give mig den side, jeg er mest interesseret, fordi jeg har været henne og dvæle lidt ved både køb og lidt ved jagtudstyr og sådan noget.

Og det er fuldstændig ureguleret den aftale, jeg indgår. Der er altså ikke nogen forbrugermæssig gennemsigtighed, og det er såmænd bare det, jeg peger på, at det var der måske behov for. For det er der på så mange andre områder.

**Søren Søndergaard** (EL):

*Der er brådne kar i alle lejre. Også hos politiet.*

Det var lige til Troels Jørgensen, fordi jeg synes ikke, der er nogen som helst grund til at betvivle, at politiet generelt retter sig efter de retningslinjer, som er skitseret. Men altså problemet er jo, at selvfølgelig er der brodne kar i alle lejre, og jeg er da i

hvert fald sikker på, at en Per Stig Møller har en ganske bestemt opfattelse af, at det ikke er alle politifolk, som lever op til den standard, der burde være normen.

**Jørn Bro:**

| |
|---|
| *Pressen var måske den primære kilde.* |

Det har Søndergaard meget ret i. Men en anden væsentlig ting: Det mest spændende var faktisk, at meget kort efter, at sagen kom frem, der kunne Frederiksberg Bladet uden vanskelighed gå 40 år tilbage og hente den gamle artikel, hvor der stod: Stud. pol. Per Stig Møller blev i går dømt. Så det er måske her, vi finder den primære kilde.

**Søren Søndergaard** (EL):

| |
|---|
| *Ny teknologi øger mulighed for søgning af informationer om borgerne.* |

Jo, men det er jo netop her, at vi ligesom ser forskellen på teknikkerne, fordi selvfølgelig kan man gå ind og bladre Frederiksberg Bladet igennem 40 år tilbage og finde nogle oplysninger frem. Det er der ikke tvivl om, men det er meget besværligt, og det tager lang tid.

Hvorimod man ved hjælp af, var det syv, der var inde på politiets computer, i løbet af nul mikrosekunder kunne finde den oplysning. Og det er jo det, der ligesom er hele humlen i den diskussion, vi fører i dag.

**Janne Glæsel:**
Jeg skulle måske lige konkret sige, at det har man jo løst det problem nu ved at kræve adgangskontrol og password.

**Per Helge Sørensen:**

| |
|---|
| *Man skal passe på med, at tro, at historien er slut, og staten aldrig mere vil misbruge sin magt. Så vi skal være varsomme med at give den mere magt.* |

Jeg ser heller ikke det konkrete misbrug, det er ikke det, der bekymrer mig. Altså det kunne måske være Birgitte, der sagde det her. Men når vi i menneskerettighederne har det her ønske om en balance mellem statens indgrebsmuligheder og individet, ja, så er det vel bl.a., fordi vi så - eller man havde set, lige før man blev enige om de her menneskerettigheder - en stat misbruge sin magt. At misbruge sin viden om borgerne til at foretage sig utrolig grusomme ting.

Og vi sidder måske her - i hvert fald før 11. september kunne man godt have en fornemmelse af, at historien var slut, og det ville aldrig ske i Danmark. Men mens vi på den ene side i øjeblikket vel alle sammen har et ønske om større kontrol, og der er nogle særlig udvalgte mennesker, vi meget gerne vil have fat i, så er der jo altså også på den samme side - det er der i hvert fald inde i mig - også nogle lidt grimme tanker om, hvorvidt det her med at internere folk eller kontrollere folk på baggrund af deres religiøse overbevisning, det ligger ikke så fjernt, som det har gjort.

Og derfor tror jeg, at man skal passe på med at tro, at historien er slut. Man bliver nødt til at sige, jamen der er en grund til, at der skal være en balance mellem staten og individet. Der er en grund til, at vi skal slå en ring om individet og sige: Det er ikke en god ide, at staten ved alt for meget eller kan foretage indgreb, der er alt for indgribende, fordi den magtbalance kan misbruges. Og det er sådan set derfor, at jeg synes, at det var en utrolig god ide at holde denne her høring for at sige, jamen når vi ser børnepornoeksemplet, så er der jo ingen, der kan være uenig i, at det ville være utrolig rart at finde ud af, hvem der havde begået det overfald.

Men vi må også en gang imellem trække os tilbage og kigge lidt bredere på det og sige: Var det egentlig her, vi ville hen med samfundet. Og hvis det ikke var det, så må vi gøre et eller andet, eller også må vi i hvert fald kigge lidt frem og sige, hvor vil vi videre hen. Hvor langt vil vi gå i at flytte den grænse mellem staten og individet. Og så er det ikke så meget det konkrete misbrug, vi skal tænke på. Vi skal tænke lidt bredere og måske lidt mere filosofisk og måske endda lidt følelsesmæssigt over det - at hvor langt vil vi lade staten komme ind på livet af os.

**Knud Erik Hansen** (SF):

*Hvilke alternativer til elektronisk overvågning er der?*

Det er i en lidt anden boldgade. Det er til Anne-Sofie Dideriksen. Nu har vi snakket meget om overvågning og alle de der teknikaliteter og ting, der ligger omkring det. Så jeg tror, jeg vil stille et måske i virkeligheden lidt umuligt spørgsmål. Jeg tror, det er svært at stille, fordi det er sådan meget svært, når vi snakker social kontrol.
Men kan du give det lidt mere kød og blod, hvor er det faktisk, vi kan gå ind og udvikle den der mere sociale kontrol, og hvor er det, I præcis oplever, at den tekniske gennemlysning går ind og overtager social kontrol, hvor vi i virkeligheden kunne satse på den sociale kontrol i stedet for. Og så være fri for den her overvågning, som de fleste af os egentlig helst i mange tilfælde var fri for. Kan du give lidt mere kød og blod? Du nævnte noget om børneområder, er der andre områder?

**Anne-Sofie Dideriksen:**

*Fysisk indretning og menneskelige kontrollører kan erstatte elektronisk overvågning.*

Ja, det lyder nemlig lidt luftigt, men det kan i hvert fald forbindes med vores diskussion af alternativer til elektronisk overvågning. Der findes jo andre former for overvågning end elektronisk, der findes også overvågning, hvor man bruger mennesker, der findes muligheder for at kontrollere - der findes andre muligheder for at kontrollere forskellige ting end elektronik.

Et eksempel er diskussionen om at putte chips i skoene eller om håndled på ældre senile for at kunne blive advaret, hvis de enten er i gang med at forlade plejehjemmet eller kunne følge dem bagefter. I Århus har man indført det på et plejehjem i Tranbjerg, men det er en teknologi, hvor man kun bliver advaret, når den ældre forlader plejehjemmet, men man kan ikke følge den ældre bagefter, altså der er ikke tale om overvågning i den forstand, at den udstrækker sig over tid.

Der kunne man så også diskutere, om der var andre muligheder. Man kan via den fysiske indretning af plejehjemmet gøre det stort set umuligt for en gammel, svagelig ældre at forlade plejehjemmet. Man kan på stationer bemande med mennesker ikke med kameraer - der træder den sociale kontrol i kraft.

Man relaterer sig til det menneske, som sidder og overvåger stationen, som man kan se måske i et glasbur. Der hviler menneskelige øjne og ikke kameraer på én, så der træder den sociale kontrol i kraft. Det var et par eksempler på det. Den med plejehjemmet er lidt mere teknisk, men det var for at belyse, at det handler om at tænke i alternativer, når vi siger social kontrol.

**Per Helge Sørensen:**

*Lad de tekniske muligheder ligge lidt og tal med hinanden.*

Jeg synes også, som vi allerede har hørt i dag, at arbejdspladsen er et godt eksempel. Selv om man gemmer alle de her e-mails af sikkerhedsmæssige årsager og i princippet kan gå ind og se: Hvor mange af dem er private, hvor mange af dem er faglige, så skulle man måske lade være og i stedet for vurdere de ansatte på, hvad de har præsteret, eller hvordan man opfatter dem i det daglige.

Og tilsvarende om de nu går ind på lidt mange sportssider under Tour de France. Jamen det er måske ikke igennem kontrol, man skal undersøge det. Det er måske ved nogle snakke med de ansatte om, hvad er rimeligt at gøre her, og hvor meget kan vi tillade, at produktiviteten falder i juni måned på grund af det her.

Og jeg vil sige, at børn og forældre er for mig det samme. Jeg har ikke nogen børn, men jeg er måske ung nok til at huske, hvordan det var at være ung i hvert fald, og der er det måske også et sted, hvor man skulle sige: Skulle vi nu ikke lige lade være med at udnytte de tekniske muligheder og i stedet for snakke lidt med hinanden.

Jeg er selv personligt i tvivl om kriminalitetsbekæmpelse, det er måske så til gengæld ikke et sted, hvor: Jeg tror ikke, Bin Laden er modtagelig for social kontrol, desværre.

**Jon Stokholm:**

| |
|---|
| *Nabohjælp er et godt alternativ til overvågning.* |

Ja, lad mig pege på ét sted til, altså nabohjælp tror jeg, det er jo også en form for overvågning, som har en meget, tror jeg for de fleste, positiv virkning og opfattes positivt omkring samfundsmæssig solidaritet osv. Så det er da også et sted, hvor man sagtens kan sætte ind.

Jeg tror også, man trods alt skal skrive sig bag øret, at det, som Per siger, at overvågning i mange situationer, vil være at kurere mod symptomer i stedet for at kurere mod selve årsagen til lidelsen. For overvågning er ofte et symptom på, at der er noget galt et helt andet sted.

## Afslutning

**Ordstyrer, Hanne Severinsen** (V), formand for Forskningsudvalget:
Skulle det være de sidste ord, det blev sagt?
Jamen så synes jeg, jeg vil takke alle de mange oplægsholdere og også takke politikerpanelet for spørgsmålene. Vi har fået en masse problemstillinger vendt, og vi har jo hele tiden været klar over, at det her er jo ikke nemt. Der er jo flere og flere muligheder, og det kan blive til "Big Brother is watching you", og der er også meget overvågning, som vi opfatter som positivt. Det er jo godt, at man kan følge med i, om det går godt osv., men sådan er det jo altid, altså.

Fremskridtet har jo sådan et Janushoved, man ser både den ene og den anden vej, og det er jo også måden, vi bruger den teknologi på. Og vi skal jo her i Folketinget drøfte mange ting. Vi skal i gang med en terrorpakke, og der er ingen tvivl om, at 11. september har gjort den her høring endnu mere aktuel, men det er jo aktuelt, kan vi jo se. Vi har fået et overblik over alle mulige problemstillinger, at det er jo noget, som virkelig griber ind i vores samfund, det er også noget, der diskuteres.

Der har været diskussioner. Forskningsministeriet har haft en lignende høring, og Digital Rights har, og der kommer i næste uge høringen »Tænketanken«, og jeg har

hørt, at der er planer om, at man skal uddele årets Big Brother-pris. Det er også lidt interessant.

Jeg tror, at det er godt, at vi diskuterer de her ting, og jeg bed også mærke i udtrykket »at tillid er godt, men kontrol er bedre«. Det skal vi jo passe på, at vi ikke efterhånden synes: At det er bare nemt, og så gør vi det. Så det har været en spændende eftermiddag og formiddag. Og jeg er meget glad for, at så mange kunne deltage. Og først og fremmest vil jeg jo takke dem, der har deltaget her, men jeg synes også, der skal lyde en stor tak til Teknologirådet.

Det er jo sådan, at når Folketinget vedtager at lave sådan en høring, at hvis vi så kan få Teknologirådet med på sagen, så er vi klar over, at så er den i gode hænder, og at rent teknisk får man al mulig hjælp og støtte, men også en afsøgning af, hvem der vil være interessante at lytte til, og det synes jeg, at I har været gode til at udvælge. Det er alle paneldeltagerne et godt eksempel på.

Så vi siger tak i dag fra Forskningsudvalget og fra Retsudvalget, og så er der en lille mulighed for, at man kan få et - jeg er egentlig ikke klar over, hvad det er, man kan få - men i hvert fald man kan gå udenfor - det hedder en reception - hvor man kan få lidt eftersnak. Og det sidste er måske også vigtigt, fordi pauserne er jo også spændende i sådan en høring, de muligheder, man får for at få talt med de forskellige. Så tak for i dag og kom godt hjem.

# Præsentation af oplægsholderne

**Peter Blume**
Professor i retsinformatik, Københavns Universitet
Medlem af Registerlovsudvalget: Betænkning 1345/1997
Forfatter til bl.a. ”Fra tale til data” (disputats 1989), ”Personregistrering” (3. udg. 1996), ”Databeskyttelsesret” (2000), ”Personoplysningsloven” (2000), ”Juridisk Metodelære” (2001) samt artikler om persondatabeskyttelse m.v.
Medlem af Datarådet
Formand for Biblioteksafgiftsnævnet
Institutleder, Retsvidenskabeligt Institut B, Københavns Universitet
Medlem af bestyrelsen for Dansk forening for edb og jura
Medlem af Legal Advisory Board, DGXIII, EU

**Kim Rasmussen**
Mag. Art. i Kultursociologi, Ph.D. i Mediepædagogik
Forsker v. Center for Institutionsforskning, Højvangseminariet
Ansættelser: 1986-1988 Undervisningsassistent på Københavns Universitet, Inst. f. Kultursociologi & Inst. f. Pædagogik
1987-1994 Undervisningsassistent på Danmarks Lærerhøjskole
1990-1992 Ekstern Lektor på Københavns Universitet Inst. f. Statskundskab.
1992-1997 Seminarielærer og planlægger på Hovedstadens Pædagogseminarium
1997-2001 Forsker ved Center for Institutionsforskning, Højvangseminariet.
Udvalgte publikationer:
1999: Overvågningens overvågning (m.S.Smidt) kronik i Politiken 14.1.
2000: Menneskelige konsekvenser af overvågning. In: Teknologirådets rapport 2000/9
2000: Statens børn. m. Søren Smidt In:

**Peter Christensen**
Baggrund:
Startede på Datalogi-studiet i ’73; men fik allerede i ’76 sit første sommerferiejob i IT-industrien. Planlagde og gennemførte på Datalogis overbygning i ’79 kurset: Edb-teknologiens samfundsmæssige konsekvenser i 2 semestre.

Arbejdsområder:
Har arbejdet som programmør/planlægger først hos Regnecentralen og siden Falck. Siden ’83 har arbejdsområdet været orienteret mod databaser og netværk hos KP, Alka, Hafnia, danNet og CMA/IBM. Har siden 2000 arbejdet freelance med vægt på

teknisk infrastruktur, back-ends til Web's og udnyttelsen af eksisterende databaser og netværk som potentiale i organisationers strategi.
Tillidsposter:
Har fulgt lovgivningen på IT-området siden '76 med vægt på den personlige integritet og interaktionen mellem IT og samfund. PROSA's Formand i perioden 96-2000.

**Eva Smith**
Eva Smith er professor i procesret ved Københavns Universitet siden 1990.
Doktordisputats "Vidnebeviset" 1986.
Konstitueret dommer i Østre Landsret 1992-93.
Formand for Det Kriminalpræventive Råd 1995 -
Har skrevet lærebøger i proces samt et stort antal artikler.
Medlem af adskillige udvalg, navnlig under Justitsministeriet samt flere udvalg under Europarådet.
Flittig deltager i den offentlige debat med kronikker og artikler.

**Niels Crone Lyngkjær**
Kontorchef Niels Crone Lyngkjær, Finansrådet, (Brancheorganisation for pengeinstitutter)

Beskæftiget i dansk bankvæsen siden 1962. Ansat side 1997 i Finansrådet.

Varetager blandt andet sikringsområdet. Er "formand" for foreningens sikringsudvalg. Er medlem – og hvert 3. år formand - for Det Fælles Sikringsudvalg, som er etableret af Danmarks Nationalbank, Post Danmark og Finansrådet i 1986. Er sekretær for Kontaktudvalget mellem politi, pengeinstitutter og posthuse, som er et uformelt samtaleforum, hvor spørgsmål af betydning for samarbejdet mellem interessenterne omkring sikringsforhold i pengeinstitutter og posthuse kan drøftes.

**Troels Ørting Jørgensen**
Vicekriminalinspektør Troels Ørting Jørgensen (TØJ), er chef for Nationalt Efterforskningssøttecenter (i daglig tale NEC). Enheden har bl.a. til opgave at monitere organiseret, kompliceret eller ressourcetung kriminalitet i Danmark, herunder også IT-relateret kriminalitet. TØJ har været ansat i politiet siden 1980 og har i sin tjenestetid været ansat i Rigspolitichefens Rejseafdeling samt udstationeret i en årrække som forbindelsesofficer til Europol i Haag/Holland.

**Jørn Bro**
Siden 1990 Politimester i Glostrup Politikreds
Fra 1981 – 1990 chef for Politiskolen og i tre år forud herfor politimester i Middelfart
Fra 1965 – 1977 ved Politiets Efterretningstjeneste, fra 1969 souschef og operationschef.

**Birgitte Kofod Olsen**
Seniorforsker, Det Danske Center for Menneskerettigheder

Cand.jur. 1991, Københavns Universitet,
Lic.jur. 1998, Københavns Universitet.

Stipendiat ved Københavns Universitet 1991, 1993-1994.
Ansat som forsker ved Det Danske Center for Menneskerettigheder 1994.

Medlem af Teknologirådets Repræsentantskab.

Forskningsområde: menneskerettigheder og informationsteknologi, herunder særligt privatlivs- og persondatabeskyttelse. Licentiatafhandling om identifikationsteknologi og integritetsbeskyttelse.

**Laurits Rønn**
Jeg har siden 1994 arbejdet i forskellige organisationer inden for det arbejdsretlige område, herunder Ledernes Hovedorganisation og Dansk Arbejdsgiverforening. Siden 1998 som ansættelsesretlig chef i Dansk Handel & Service. I Dansk Handel & Service har jeg bl.a. haft ansvar for "overvågning" i bred forstand, herunder regeldannelse i lovgivning og overenskomster, dialog med lønmodtager-organisationer, rådgivning og dialog med medlemsvirksomheder mv. Hertil kommer, at jeg har deltaget i en række arrangementer arrangeret af Det Kriminal Præventive Råd. Dansk Handel & Service deltager i debatten om overvågning og jeg ser derfor frem til at deltage i konferencen den 24. oktober 2001.

**Bjarne Petersen**
Faglig sekretær, HK/HANDEL.
Ansættelsesforhold:

| | |
|---|---|
| 2001 – 1982 | HK/HANDEL, HK/DANMARK |
| 1982 - 1979 | Branchesikkerhedsrådet for kontor og adm. |
| 1979 - 1972 | Arbejdsmiljøfondet/arb.beskyttelsesfondet |
| 1972 - 1969 | S. Dyrup & Co. |
| 1969 - 1968 | Værnepligtig, Bornholms Værn |
| 1968 - 1964 | Handelsuddannelse |

Uddannelser:

| | |
|---|---|
| 2001 – 1972 | Løbende efter- og videreuddannelser i relation til job såvel som led i personlig udvikling |
| 1970 – 1972 | Tillidsmandsuddannelse, aftenskole |
| 1968 – 1964 | Handelsskole, Købmandsskolen Nørre Port |
| 1964 – 1955 | 9. kl. afgangsprøve, Bellahøj skole |

Tillidsposter:

| | |
|---|---|
| 1989 – 1985 | Hovedbestyrelsesmedlem (A) |
| 1988 – 1982 | Kredsformand |

1981 – 1985 Kommunalbestyrelsesmedlem
1979 – 1977 Tillidsmand, formand for foreningen af konsulenter i Arbejdsmiljøfondet

**Janne Glæsel**
Stilling:
Advokat (H), partner i Bech-Bruun Dragsted, Nørre Farimagsgade 3, København K

Tillidshverv**:**
Med Medlem af Regeringens IT-sikkerhedsråd
Næstformand for Datarådet
Medlem af Tipsungdomsnævnet
Medlem af bestyrelserne i DIFO og DK Hostmaster A/S samt diverse øvrige bestyrelser i selskaber og fonde
Medlem af Erhvervsudvalget under Advokatsamfundet

Specialeområder:
Rådgiver som advokat virksomheder om immaterialret, markedsføringsret, IT- og telekommunikationsret samt persondataloven.

Skribentvirksomhed:
Forfatter og medforfatter til div. publikationer og artikler om IT-ret og telekommunikation, varemærker og forsknings- og udviklingskontrakter.

**Jon Stokholm**
Født 23/4 1951, student 1969 Frederiksborg Statsskole; studieophold 1980-81, New York, USA; studieophold 1991 Stanford Business School, USA, juridisk embedseksamen 1975 KU. Beskikkelse 1978; møderet for Landsretten 1978; møderet for Højesteret 1983. 1975-80 medarbejder/advokat hos Kammeradvokaten; 1980-85 advokat/medindehaver i Advokatfirmaet Niels Th. Kjølbye m.fl.; fra 1985 i Poulsen, Westergaard, Cadovius & Stokholm (nu Lind & Cadovius Advokataktieselskab); 1988-1997 formand for Advokatrådets Skatteudvalg; 1991-97 medlem af Advokatrådet; 1991-97 hovedbestyrelsesmedlem for DJØF; fra 1991 censor ved Det Retsvidenskabelige Institut ved KU; fra 1991 beneficeret for Højesteret; fra 1994 medlem af Justitsministeriets Udvalg vedr. Undersøgelsesorganer. 1996 medlem af Justitsministeriet Domstolsudvalg. Fra 1999 formand for Advokatrådet.

**Anne-Sofie Dideriksen**
Anne-Sofie Dideriksen (f. 1971), cand. mag. fra Århus Universitet 1998. Ansættelser som gymnasielærer og museumsmedarbejder 1998-1999. Fra 1999 ph.d.-stipendiat på Institut for Germansk Filologi, Århus Universitet. Medlem af Teknologirådets borgerpanel, nedsat til rådets konsensuskonference om elektronisk overvågning i efteråret 2000. Borgerpanelets repræsentant i debatprogrammet Café på P1 i december 2000 om overvågning på arbejdspladsen.

**Per Helge Sørensen**
Per Helge Sørensen, f. 1968, er forfatter og IT-konsulent.

Per Helge Sørensen udgav i september 2000 romanen "Mailstorm" om kryptering og efterretningstjenesternes overvågning af Internet. (www.mailstorm.dk)

Per Helge Sørensen er medstifter og bestyrelsesmedlem i den danske forening Digital Rights, der arbejder for menneskerettigheder på Internet (www.digitalrights.dk). Foreningen har bl.a. været involveret i følgende sager om overvågning:
- Lov om adgang til masteoplysninger, L194
- Europarådets konvention om cyber crime
- Direktiv om privatliv i kommunikationssystemer: COM(2000)385
- Registrering af data hos Internetudbydere

Digital Rights samarbejder med det Danske Center for Menneskerettigheder samt med en række europæiske menneskerettighedsorganisationer.

Fra 1995 - 1999 var Per Helge Sørensen ansat i Forskningsministeriet, hvor han bl.a. var sekretær for regeringens ekspertudvalg om kryptering. Per Helge Sørensen er uddannet civilingeniør fra DTU med speciale i kodningsteori og kryptering.

**Peter Landrock**
Peter Landrock er født i 1948 og blev cand.scient. i matematik og fysik fra Aarhus Universitet i 1972 samt Ph.d. i matematik fra University of Chicago i 1974. Han var herefter ansat som lektor på Matematisk Institut, Aarhus Universitet til 1996, i hvilken periode han var gæsteprofessor/forsker ved en række universiteter i udlandet, inkl. Oxford, Institute for Advanced Study, Princeton, Essen, Mainz, Cambridge og Leuven. I 1997 blev han udnævnt til adjungeret professor i Aarhus. Fra 2001 er han bosiddende i Cambridge, UK. I 1986 grundlagde han sammen med to tidligere studenter Cryptomathic, som har hovedsæde i Aarhus. Firmaet har i dag ca. 80 medarbejdere og kontorer i Leuven, Torino, Cambridge, München og København. Kernen i Cryptomathics produkter er egne krypteringsværktøjer samt en række produkter og løsninger omkring PKI, certificerings-centre, digitale signaturer, mobil sikkerhed samt den nye generation af kreditkort baseret på chipkort teknologi. Firmaet har kunder på 5 kontinenter, hvoraf de fleste er i finansverdenen. Han var præsident for The International Association for Cryptologic Research 1992-95, og har været medlem af regeringens IT-sikkerhedsråd siden dets grundlæggelse i 1996. Desuden sidder han i Technical Advisory Board for Microsoft's Research Laboratory i Cambridge samt i flere bestyrelser inkl. VKR Holding (Velux Industri) og Forskerparken i Århus (fmd.).

# Skriftlige oplæg

## Lovgivning om overvågning - typer og hensyn

*Af Peter Blume, Professor, dr.jur.*

Overvågning er en betegnelse for mange forskellige fænomener, der strækker sig fra de ganske uskyldige til de stærkt problematiske. Overvågning kan rette sig mod fysiske genstande eller personer. Ved den sidstnævnte form for overvågning kan i almindelighed forstås det fænomen at en person observerer en anden persons adfærd i bred forstand. Vi overvåger alle sammen, f.eks. når vi går ned ad gågaden, ligger på stranden eller sidder i arbejdspladsens kantine. Denne overvågning er sjældent problematisk og er udtryk for almindelig menneskelig nysgerrighed.

### Kontrol

Den form for overvågning, der normalt påkalder sig kritisk opmærksomhed og som kan være politisk interessant, er den, der har til formål at fungere som et middel til kontrol, herunder til at forebygge adfærd, der samfundsmæssigt ikke anses for ønskelig. Denne form for overvågning er i vækst. Med den moderne informations-teknologi, der både kan overvåge og er selv overvågelig, har denne tendens ført til, at samfundet undertiden karakteriseres som et overvågningssamfund. Hvorvidt dette er berettiget, tages der ikke stilling til her, idet det følgende fungerer som et grundlag for vurderingen heraf.

### Kategorisering

Overordnet kan det være hensigtsmæssigt at opstille forskellige former for kategoriseringer, når overvågning skal drøftes.

(1) Der må for det første ses på, hvad der er overvågningens genstand. Er denne personer, bygninger eller andre fysiske genstande, dyr, eller naturen. Særligt for så vidt angår personer kan det have betydning i hvilket omfang, de pågældende selv kan forstå den overvågning, de udsættes for, idet der f.eks. kan være tale om børn eller demente. Vurderingen af de modstridende hensyn er generelt betinget af, hvad overvågningen retter sig imod.

(2) For det andet må det tages i betragtning, hvem, der foretager overvågningen. Er det en offentlig myndighed eller er det private. I førstnævnte tilfælde kan det bl.a. have betydning hvilken myndighed, der er tale om. Særlig interesse er ofte knyttet til politiets beføjelser og det kan ligeledes have betydning i hvilket omfang, myndigheden er underlagt en gennemskuelig offentlig kontrol, hvilket er særligt relevant i forhold til efterretningstjenesterne.

(3) For det tredje må der lægges vægt på, hvor overvågningen finder sted. Er det f.eks. på gaden, på nettet, på arbejdspladsen, i fængslet eller i hjemmet. Styrken af

den argumentation, der henviser til retten til et privatliv og retten til at være i fred, varierer i forhold til, hvor overvågningen sker.

(4) For det fjerde har det betydning, hvad overvågningens formål er. Er den eksempelvis begrundet i et ønske om at skabe sikkerhed, at forebygge ødelæggelse af væsentlige samfundsværdier, eller er formålet kontrol af personers adfærd. Formålet indicerer, hvad overvågningens resultater vil blive benyttet til.

(5) Det må endelig tillægges betydning, hvordan overvågningen bliver gennemført. Vigtige spørgsmål er bl.a., om denne finder sted åbent eller skjult, bliver de overvågede informeret og sker dette før eller efter overvågningen. I denne forbindelse har det endvidere interesse, om overvågningen er frivillig eller ufrivillig, jfr. herom i næste afsnit.

Denne opdeling mellem hvad, hvem, hvor, hvorfor og hvordan er væsentlig, når overvågningens lyse og mørke sider vurderes.

**Selvovervågning**
Som nævnt ovenfor har det for personovervågningen betydning, om denne er frivillig eller ufrivillig. Den resterende del af dette papir handler om sidstnævnte, men i det nutidige samfund kendes også forskellige former for selvovervågning. Eksempler er de åbne hjem på Internettet, idet disse ikke behøver at have en erotisk intention, og tv-udsendelser som Big Brother. Den udbredte offentlige brug af mobiltelefoni er et yderligere eksempel på, at den overvågede selv vil overvåges. En form for ekshibitionisme. Selvom denne form for overvågning ikke behandles yderligere her har den betydning ved en almindelig vurdering af holdningen til overvågning.

**Hensyn**
Ved en vurdering af de forskellige former for overvågning vil der typisk skulle ske en afvejning mellem modstridende hensyn. I forhold til overvågning af personer, der er i fokus i dette papir, er det centrale hensyn, der typisk taler imod overvågning, hensynet til værnet af privatlivets fred og den enkelte borgers personlige integritet. Det er karakteristisk, at dette hensyn er forholdsvis luftigt, selvom det i den europæiske menneskerettighedskonventions artikel 8 er anerkendt som en grundrettighed. Det er ikke muligt at præcisere dette hensyn, men det desuagtet klart for de fleste, at det har stor betydning for et aktivt deltagende demokrati, at dette hensyn ikke undergraves. De væsentligste problemer knytter sig til, at det private ikke har fast konturer, at der er varierende begrundelser for at beskytte det private område og at det er individuelt, hvad der opfattes som privat. Hensynet til privatlivet er dermed tit abstrakt og luftigt, hvilket kan være problematisk i forhold til de hensyn, der begrunder konkrete overvågningstiltag. Disse hensyn er ofte slagkraftige, f.eks. kriminalitetsbekæmpelse, og har derfor en tendens til "at vinde" i den retspolitiske diskussion. Det er bl.a. derfor, at det væsentligt at forsøge at have et overblik over hvilket samfund, den samlede lovgivning skaber, jfr. sidst i papiret.

Dette gælder også i forhold til de initiativer, der forventes at blive taget som konsekvens af de tragiske begivenheder 11. september. Blandt disse vil være forslag om øget overvågning, idet udvidede muligheder for teleovervågning allerede er bebudet. Tiltag af denne karakter kan være velbegrundede - naivitet er farligt - men de må overvejes nøje, idet der er tale om det klassiske dilemma, hvorefter midler vendt mod demokratiets fjender ikke må være vendt mod demokratiet. Diskussionen af visse former for overvågning har en beklagelig aktualitet.

**Overvågning som et bredt begreb**

I dette papir er det som nævnt særligt overvågning af personers adfærd eller data med et mere eller mindre direkte kontrolformål, der tillægges interesse, men det er illustrativt for overvågningsbegrebets bredde at starte med at undersøge i hvilken udstrækning, denne betegnelse overhovedet benyttes i lovgivningen, der i denne forbindelse omfatter såvel love som andre statslige retsforskrifter.

En søgning på ordet overvågning i statens database Retsinformation resulterer i 472 hits. De love, der herved opspores, er særdeles varierede og omfatter eksempelvis lov om beskyttelse af de ydre koge i Tøndermarsken, lægemiddelloven, skovloven, fødevareloven, realkreditloven og lov om hold af slagtekyllinger. Omfattet er ligeledes en række love, som omtales nedenfor, idet denne søgning blot er foretaget for at underbygge det forhold, at det ikke er enhver form for overvågning, der er relevant i forhold til meningsudvekslingen ved denne høring. Søgningen har endvidere den begrænsning, at en lovregulering kan vedrøre overvågning, uden at dette ord benyttes. Det er således karakteristisk, at hverken straffeloven eller retsplejeloven er omfattet af de 472 hits.

Denne konstatering begrunder et forbehold i relation til det følgende, idet den samlede lovgivning som bekendt i dag er så omfattende, at det ikke er muligt at indestå for, at alle relevante regelområder er medtaget i det følgende. Et fuldt ud samlet overblik over de muligheder for overvågning, som findes i lovgivningen, er få, om nogen, beskåret.
Formålet er dermed i første række at fremhæve en række karakteristiske former for regulering, der er forbundet med brug af overvågning med henblik på kontrol af personer, herunder deres adfærd og data. I det følgende medtages også eksempler på lovgivning, der fastsætter begrænsninger eller rammer for denne form for lovgivning, idet billedet ellers let bliver for unuanceret.

**Straffeloven**

Lovgivningens udgangspunkt er i almindelighed, at gennemførelse af overvågning i mange tilfælde forudsætter lovhjemmel. Ved vurderingen af, hvornår dette er tilfældet, er udgangspunktet dels Grundlovens § 72, hvorefter kommunikationshemmeligheden er beskyttet, medmindre der ved retskendelse eller ved lov skabes grundlag for overvågning, dels en række bestemmelser i straffeloven, især dennes kapitel 27 om privatlivets fred. Det er her gjort strafbart uberettiget at bryde

kommunikationshemmeligheden, jfr. § 263, stk. 1, herunder at bryde ind i "lukkede meddelelser" og foretage aflytning. I bestemmelsens stk. 2 er det gjort strafbart at trænge ind i digitaliserede data og programmer. Det er endvidere strafbart, jfr. § 264a, at overvåge ikke frit tilgængelige områder. Disse regler har betydning for private samt for offentlige myndigheder, medmindre der er et andet retligt grundlag for at foretage overvågningen. Straffelovens bestemmelser er væsentlige ved en bedømmelse af lovgivningens holdning til overvågning, men de indeholder på ingen måde et absolut værn mod denne.

Dette skyldes, at lovgivningsmagten på en række områder har fundet, at det af samfundsmæssige grunde er nødvendigt, eller i hvert fald ikke betænkeligt, at der er mulighed for at foretage overvågning. Det er selvsagt altid muligt retspolitisk at vurdere, hvorvidt disse grunde er tilstrækkeligt tungtvejende.

**Retsplejeloven**
Et hovedformål, der begrunder, at overvågning kan finde sted, er hensynet til retshåndhævelse, herunder efterforskning af kriminalitet. I retsplejeloven er der åbnet mulighed for at politiet, sædvanligvis på grundlag af en dommerkendelse, kan gennemføre former for overvågning. Reglerne herom findes i lovens kapitel 71 om indgreb i meddelelseshemmeligheden.

I § 780 er der åbnet mulighed for, at der kan foretages aflytning samt optagelse heraf. Især bør fremhæves, at der nyligt er indsat regler, der muliggør teleoplysning og såkaldt udvidet teleoplysning, hvorefter lokaliseringsoplysninger kan indhentes, jfr. videre hertil nedenfor. Endelig bør nævnes, at § 780 giver mulighed for brevåbning. Ved udformningen og praktiseringen af disse bestemmelser anlægges et såkaldt proportionalitetsprincip, hvilket indebærer, at der skal være et rimeligt forhold mellem grovheden af den pågældende forbrydelse og intensiteten af de overvågningsforanstaltninger, der kan iværksættes. Reglerne herom er fastsat i lovens § 781. På denne måde er der en nær sammenhæng mellem straffelov og retsplejelov, idet det er strafferammerne i førstnævnte, der er bestemmende for, at sidstnævntes overvågningsregler kan finde anvendelse. Dette gælder ligeledes for de særlige regler om observation i § 791a, der giver mulighed for at overvåge ikke frit tilgængelige områder. Det tilføjes, at politiet kan overvåge frit tilgængelige områder med hjemmel i § 108, der beskriver politiets almindelige opgaver. Politiet er ikke omfattet af tv-overvågningsloven, der omtales nedenfor. Det er karakteristisk, at den moderne informations- og kommunikationsteknologi har medført, at der er kommet nye overvågningsmuligheder, hvilket belyses yderligere nedenfor i forbindelse med telelovgivningen.

**Telefoni**
Moderne telefoni er karakteriseret ved at efterlade spor. Alle er blevet klar over dette i forbindelse med PFA-sagen. Bruges mobiltelefoni er det muligt at foretage både en aktuel og en tilbageskuende overvågning af en persons bevægelsesmønster. Dette er

blot et blandt flere eksempler på den øgede betydning af lokaliseringsoplysninger, jfr. mere herom nedenfor i forbindelse med transportområdet. I telelovgivningen er der fastsat regler om, hvad teleselskaberne kan benytte disse oplysninger til og hvor længe, de må opbevares. Telelovgivningen danner grundlaget for den overvågning, som politiet som nævnt ovenfor i medfør af retsplejeloven kan foretage. I dennes § 786, stk. 1, er det fastsat, at politiet kan pålægge teleselskaber at levere de nødvendige data. Selve telelovgivningen, jfr. især Bekendtgørelse nr. 1169/2000, søger at forebygge overvågning fra bl.a. teleselskabernes side, medens politiets overvågning således er muliggjort af retsplejeloven. Vi bevæger os ikke så frit som tidligere.

**TV-overvågning**

Vist nok det eneste sted, hvor ordet overvågning optræder i en lovs titel er lov om forbud mod tv-overvågning. Loven fastsætter, at private ikke må video-overvåge frit tilgængelige områder som f.eks. veje, idet der dog er fastsat visse undtagelser herfra. For så vidt angår private eller offentlige områder, hvortil der er almindelig adgang og i henseende til arbejdspladser indeholder loven ikke et forbud, men alene et krav om, at der skal informeres om, at overvågning finder sted. Andre bestemmelse, f.eks. straffelovens § 232 om blufærdighedskrænkelse, indebærer dog visse begrænsninger. Tv-overvågningsloven, der af mange betragtes som svag, er omdiskuteret. Mange opfatter den ikke som et tilstrækkeligt værn overfor denne form for overvågning og informationskravet er ikke imponerende.

Det bør fremhæves, at det alene er adgangen til at overvåge, der reguleres i denne lov, medens brugen af de oplysninger, som overvågningen giver adgang til, normalt må bedømmes efter reglerne i lov om behandling af personoplysninger. Forholdet mellem disse to love kan dog, ej heller for så vidt angår selve overvågningen, ikke siges at være fuldt ud afklaret i dag.

**E-post og Internet**

Som fremhævet tidligere er den moderne informationsteknologi overvågelig og da der er betydelige fordele ved at anvende denne - brugen er nærmest a way of life i dag - afskrækker dette træk sjældent nogen fra at benytte den. Især spørgsmålet om overvågning af e-post og anden brug af Internettet har påkaldt sig stor opmærksomhed. Dette gælder ikke mindst i forhold til arbejdspladser. Der findes ikke i lovgivningen regler, der specifikt vedrører denne problemstilling, der til dels reguleres af de uskrevne arbejdsretlige principper (ledelsesretten). Det er herudover personoplysningslovens almindelige bestemmelser, der finder anvendelse, og på grundlag af disse har Datatilsynet i konkrete afgørelser søgt at afstikke visse rammer for, hvornår denne form for overvågning kan finde sted. Hovedbudskabet er, at dette kan ske, når formålet er sagligt og når de ansatte på forhånd er informeret herom. Man kunne overveje, om der burde være en særskilt lovregulering af denne problematik, men heroverfor står den berømte eller forkætrede danske aftalemodel på arbejdsmarkedet.

Det er nærliggende i denne forbindelse at fremhæve, at især privates overvågning af netbrug, der bl.a. kan have betydelig kommerciel interesse, er vanskeligt at regulere og at en vis effektivitet kun kan opnås via koordineret international lovgivning. Overvågningen er, som vi kommer tilbage til, ikke udelukkende et nationalt anliggende eller problem.

**Transport**
Transportområdet har betydelig interesse i forbindelse med en vurdering af lovgivningen om overvågning. Der er mange forskellige facetter knyttet til dette område. Færdselsloven, der dog ikke selv indeholder bestemmelser herom, giver grundlag for en række overvågningsforanstaltninger, der primært tager sigte på, at lovens regler, f.eks. hastighedsgrænser, bliver overholdt. Som bekendt er der sket en øget anvendelse af video på dette område, hvilket i øvrigt ikke er omfattet af tv-overvågningsloven. Der er ikke nogen tvivl om, at den almindelige færdsel er et felt, hvor lovgiver de kommende år kommer til at tage stilling til mange tiltag, der ganske vist kan tjene gode formål, men som samtidig har et overvågningspotentiale. Der vil kunne blive tale om en forstærket registrering og anvendelse af lokaliseringsdata, hvilket især må anses for en risiko i forbindelse med en eventuel indførelse af roadpricing. I forbindelse med nye former for overvågning vil foreligge det velkendte spørgsmål, om de forskellige foranstaltninger iværksættes af hensyn til færdsel/miljø eller af hensyn til statens fiskale interesser. I hvilket omfang nye former for overvågning forudsætter ændringer af færdselsloven eller særlig lovgivning skal ikke bedømmes her, hvor det er tilstrækkeligt blot at fremhæve problemstillingen.

**De nye broer**
De to love om henholdsvis Storebælts- og Øresundsforbindelsen illustrerer, at overvågningsaspektet er fremtrædende i mange transportsammenhænge. I begge love er der givet adgang til at foretage videoovervågning og i sidstnævnte endog til at udveksle oplysninger med svenske myndigheder, jfr. Øresunds-anlægslovens § 18, stk. 2. Det kan hævdes, at man, bortset fra med tog, ikke på moderne måde kan passere de to farvande uden at blive overvåget. Dermed tages der ikke stilling til, om disse foranstaltninger er nødvendige, da de to broanlæg repræsenterer store samfundsværdier.

**Luftfart**
Luftfartslovgivningen indeholder en række bestemmelser, der giver mulighed for overvågning af personer, jfr. især luftfartslovens § 70a, b og c. I betragtning af de tragiske begivenheder 11.september er det vel mere åbenbart end tidligere, at luftfart er en sårbar transportform, hvor overvågning er velbegrundet. Denne konstatering er dog ikke nogen blankocheck til en hvilken som helst form for overvågning. Forventelige stramninger bør selvsagt overvejes nøje. I det hele taget benyttes dette eksempel til på ny at betone, at den øgede overvågning, som 11. september kan begrunde på en række områder, jfr. også nedenfor, bør vurderes køligt i den forstand,

at overvågningen ikke bør antaste grundlæggende friheder i vores samfund. Vi bør ikke være naive, men vi bør heller ikke handle overilet.

**Samkøring mm.**
På en lang række andre områder end de hidtil nævnte forekommer der lovhjemlede kontrolforanstaltninger, som kan karakteriseres som overvågning. Et eksempel på denne form for kontrol er CPR-lovens § 10, stk. 2 og 3, der tager sigte på at kontrollere, at borgerne opgiver deres korrekte bopæl. Overvågningen sker tit på en ikke særlig synlig måde (modsat "dyneløftning"), idet de store oplysningsmasser, som det offentlige er i besiddelse af i vores velordnede samfund, anvendes til at sikre, at lovgivningen bliver overholdt. Dette sker ved at der spredt i lovgivningen er tilvejebragt vidtgående hjemler til, at forskellige myndigheder elektronisk kan udveksle personoplysninger, herunder at foretage samkøringer.

Dette er som nævnt velkendt på mange områder og her skal blot som eksempel nævnes samkøringsmulighederne på det sociale område, jfr. specielt lov om retssikkerhed og administration på det sociale område § 12, især stk. 4. Denne overvågning kan karakteriseres som diskret i den forstand, at den som nævnt ikke er synlig for de, der overvåges. Dette gælder også, selvom det er forudsat, at der skal gives borgerne information herom. Umiddelbart er der betydelig opbakning til denne form for overvågning. Der er næppe nogen, der vil forsvare socialbedrageri o. lign., og der synes derfor at være tale om en fornuftig brug af den moderne teknologi. Der bør dog også på områder som dette være grænser for, hvor intensiv overvågningen bør være. Hensynet til privatlivsbeskyttelse kan forekomme vagt, men det er trods alt grundlæggende i et samfund, hvor den enkelte ikke bør opsluges af helheden.

**Schengen/Europol**
Overvågning har en international dimension, der også har fundet vej til lovgivningen. Dette gælder f.eks. for reglerne om toldsamarbejde (f.eks. Napoli 2; lov 482 af 7.6.01), men er mest kendt fra Schengen og Europol, idet disse konventionsfastsatte institutioner er gennemført ved lov. Som et centralt element i disse institutioner er der etableret store databasesystemer, der giver mulighed for at udveksle en række mere eller mindre præcist definerede personoplysninger. Formålet hermed er ikke altid overvågning, men dette er dog et af formålene. Det er tænkeligt, at udvekslings-mulighederne vil blive forstærkede som følge af 11 september. Under alle omstændigheder er der en potentiel stærk overvågningsintensitet indbygget i disse systemer og som det i og for sig også kan hævdes på andre områder er det næppe realistisk, at lovgiver kan gennemskue, hvorledes systemerne anvendes i praksis, uanset at særlige kontrolinstanser er etablerede. Spørgsmålet om lovgivers muligheder for at få indblik i konsekvenserne af sin normerende virksomhed er et vigtigt aspekt af overvågningsdiskussionen.

Den tværnationale overvågning ikke mindst af Internettet er formodentlig generelt i vækst. Uanset om man nu tror på, at Echelon findes eller man afviser dette, er der

ikke tvivl om, at Echelon for mange symboliserer de risici, der vil blive aktualiserede i en ikke for fjern fremtid.

**Både helheden og detaljerne**

Som de forrige sider gerne skulle have illustreret, indeholder den samlede lovgivning en mængde muligheder for differentierede former for overvågning med henblik på forskellige former for formål. En samlet vurdering er nyttig, men ikke tilstrækkelig, selvom betegnelsen overvågningssamfund netop tager henblik herpå. I en (rets)politisk sammenhæng bør man ganske vist have blik for sammenhængene, også på tværs af Folketingets udvalgsstruktur, men samtidig må det erkendes, at de hensyn, der kan legitimere begrænsninger i borgernes frie råderum, er af forskellig karakter på de enkelte lovområder. Den foreliggende og ligeledes den kommende lovgivning må bedømmes såvel som en helhed som på det singulære regelniveau.

Det er dog vigtigt særligt at fremhæve helheden. Lovgivningsarbejdet er fragmentarisk i den forstand, at det kan være vanskeligt - vel reelt umuligt - for de enkelte folketingsmedlemmer at have et overblik over hele regelværket, der jo samlet er med til at forme samfundet. Dette er en konstatering og ikke ment som nogen kritik. Denne iagttagelse fremhæves, fordi det ville være ønskeligt, om der blev gjort noget for at skaffe et overblik over denne helhed. En mulighed ville således være at få foretaget en udredning, f.eks. via et sagkyndigt udvalg, af personovervågningen i dag. En sådan udredning ville give Folketinget bedre muligheder for at vurdere kommende tiltag. Den vil ligeledes kunne bidrage til et svar på spørgsmålet om i hvilket omfang, det er berettiget at karakterisere samfundet som et overvågningssamfund.
Ved vurderingen af den samlede overvågning må det holdes for øje, at den vedrører grundlæggende værdier i vores samfundsmåde - og at det privatliv, som borgerne mister ved ny overvågning, næsten altid er mistet for altid.

*Peter Blume*
*Oktober 2001*

## Udvalgte problemstillinger ved tidens overvågningstendenser.

*Af Kim Rasmussen, Center for Institutionsforskning - Højvangsseminariet.*

Fænomenet "overvågning" er kompliceret. Det gælder på alle de niveauer, man kan tænke sig det; staten-borgere, virksomhed-ansatte, institution-brugere, forretning-kunder, etc. Derfor kræver det også stor eftertænksomhed at beskæftige sig med fænomenet, uanset om man er myndig engageret borger, forsker, journalist, eller hvilken indfaldsvinkel man nu har. Og det kræver ikke mindre tænksomhed at få lavet en velreflekteret og fornuftig lovgivning, der på en gang både tager vare på og beskytter individets frihed og demokratiske rettigheder, og samtidig kritisk anerkender at overvågning under visse betingelser og i visse former kan være en acceptabel mulighed til løsning af forskellige problemer i samfundet. I det følgende forsøges dele af det komplicerede præciseret i forbindelse med centrale problemstillinger, der synes uomgængelige ved tidens overvågningstendenser.

### Det komplicerede ved overvågningsfænomenet begynder allerede ved definitionen

En første ting der gør fænomenet kompliceret er, at det er svært klart og entydigt at definere, hvad der skal forstås ved overvågning. Hvad taler vi egentlig om, når vi bruger begrebet overvågning? Adskiller overvågning sig eksempelvis fra iagttagelse? eller observation? Det er svært at svare på. Bl.a. af den grund at *al overvågning forudsætter iagttagelse og observation*. Hvorimod *al iagttagelse og observation ikke nødvendigvis er overvågning*. Samtidig er det vigtigt at fastholde, at overvågning i dag ikke kun er et direkte forhold mellem en overvåger og nogle overvågede, men i udbredt grad er et indirekte teknologisk- og mediebåret forhold.
Overvågning omfatter også iagttagelse, observation og registrering af den slags persondata, der viser sig via elektroniske spor efter personer.

Når vi som civile personer mere eller mindre opmærksomt iagttager hinanden på gaden, i indkøbscentret eller på sportsarenaen, kan man næppe meningsfuldt tale om overvågning. Men hvad når børnene er syge? Er der ikke tale om overvågning, når vi nøje følger at temperaturen ikke kommer over de 40 grader?

Hvornår iagttagelse bliver til overvågning hænger for mig at se bl.a. sammen med et skift i intention. *Overvågning er iagttagelse med henblik på at overvåge og registrere*. Måske kan man tale om en mere eller mindre tydelig graduering fra iagttagelse over observation til overvågning. Det er dog ikke sikkert alle vil være enige heri. Det er heller ikke sikkert at denne bestemmelse er i stand til at indfange alle eksempler. Under alle omstændigheder er begrebet ikke nemt at definere klart og entydigt.

**Det komplicerede ved overvågningsfænomenet ligger også i fænomenets sammensathed**

En anden ting, der gør overvågningsfænomenet kompliceret er, at det er et ***sammensat*** fænomen. Overvågning implicerer forskellige former for iagttagelse (at se, at lytte, at sanse). Derudover er overvågning også båret af bestemte intentioner og interesser (et ønske om, et behov for, et mål om). Endelig er overvågning ofte knyttet til en eller anden form for registrering (især de overvågningsformer der omfatter brug af teknologi (elektroniske spor, fotos, videobånd, o.a.)). Hertil kommer at overvågning hænger sammen med handlemuligheder og handlefunktioner. Man overvåger med henblik på efterfølgende at kunne handle.

Overvågningsfænomenet har altså flere elementer i sig:
- et intentions-element
- et iagttagelses-element
- et registrerings-element
- endelig er der knyttet et potentielt handlingselement.

Om overvågningsfænomenet gælder dét samme som visse andre fænomener: summen er mere end delene.

Hvis overvågning skal reguleres, må hver af delene reflekteres og medtænkes. Dels hver for sig og dels samlet. Med den omfattende overvågning, der kendetegner de moderne samfund i dag, savner man som borger ofte en mere tydelig og klar begrundelse for, HVORFOR overvågningen foregår. Man kan også savne klar information om, HVOR den foregår, ligesom man kan savne oplysning om, HVAD der registreres, HVOR LÆNGE informationerne opbevares, og på HVILKET retsgrundlag, det sker. Kort sagt: i dag er der generelt informationsmangel eller informationsknaphed omkring overvågning.

**Det komplicerede ved overvågningsfænomenet hænger sammen med konteksten**

Vi kan tale alment om overvågning, men overvågning er altid konkret og knyttet til en bestemt sammenhæng (tid, sted, relation). I fængsler, omkring militærområder, lufthavne, på hospitaler, i skoler, ved visse socialcentre, på S-togstationer, i banker, i posthuse, i indkøbscentre, på tankstationer, i butikker, i private hjem, osv.

Overvågning foregår altså et bestemt sted, i bestemte rum (offentlige, private, gråzonefelter).
Overvågning foregår i tid (fx. permanent eller i et afgrænset tidsrum).
Overvågning foregår mellem mennesker i forskellige relationer (flere og flere professioner beskæftiger sig med at overvåge (fra militær, politi, vagtværn, læger, lærere, pædagoger, psykologer, butiksansatte, hvor visse professioner forventes at skulle overvåge og hvor de overvågede forventes at lade sig overvåge).

Overvågningsfænomenet er også sammensat af forskellige typer og former for overvågning - afhængig af sted, tid, profession, social sammenhæng, etc. Der er eksempelvis stor og afgørende forskel på, om man konstant er overvåget i et indkøbscenter, eller om man som patient er overvåget, mens man indlagt på hjerteafdelingen. Man må kritisk spørge om der altid foreligger gode grunde til den stigende overvågning? om der tænkes i alternativer?

**Det komplicerede ved overvågningsfænomenet er også, at det er bi-polært og at det derfor bærer på en potentiel interessekonflikt**

Hvor der er overvågning, er der også altid mindst to parter: en overvåger og en der overvåges. Overvågning kan derfor altid anskues ud fra mindst to forskellige perspektiver. De to parter kan have en fællesinteresse, men dette gælder ikke alle tilfælde. Derfor indebærer fænomenet ofte en interessekonflikt. På arbejdspladsen kan arbejdsgiveren have en interesse i at overvåge medarbejderne. Dette står i direkte modsætning til arbejdstagernes interesse i ikke at være under observation, mistanke og kontrol. I offentligheden har borgerne en interesse i ikke at være under permanent overvågning, fordi dette truer friheden og retten til at kunne færdes frit. Denne interesse står i modsætning til myndighedernes eller forretningsindehavernes interesse i at sikre sig mod kriminalitet, angreb, - i almeninteressen navn, etc. I denne forbindelse er det væsentligt ikke at se bort fra, at når overvågeren er en offentlig myndighed, en offentlig institution, en privat organisation eller virksomhed, da synes overvågning knyttet til et strukturmæssigt magtforhold, hvor den enkelte let kan føle sig afmagtsfuld.

Det gør ikke fænomenet mindre kompliceret, at overvågning generelt betragtet er et strukturelt fænomen, men at vi som aktører kan indtage vekslende pladser i strukturen. Vi tænker måske først og fremmest på de offentlige myndigheder og på arbejdsgiverne som magtfulde instanser, der har magt og agt til at overvåge. Men som borgere er vi ikke mere fastlåste i vores relationer til strukturen, end at vi kan træde ind og ud af denne. Oftest oplever vi, at vi hører til de overvågede, men befinder vi os ikke oftere og oftere i positioner, hvor vi selv hører til de overvågende. Ikke mindst teknologiens indlejring i hverdagen giver borgerne mulighed for selv via TV, computere og mobiltelefon, at overvåge. Man kan ligefrem finde særlige underholdningsprogrammer, hvis formål er at gøre seerne til overvågere. Dette bidrager til at komplicere fænomenet. Vi er selv en del af problematikken og det kan være særdeles vanskeligt at drøfte overvågningsspørgsmålet nøgternt og tænksomt, fordi der altid er involveret interesser, følelser, angst og kalkulationer til problemstillingen.

**Det komplicerede ved overvågningsfænomenet er, at det ikke er normativt entydigt**

Overvågningsfænomenet er yderligere kompliceret, fordi det ikke entydigt kan vurderes som enten negativt eller positivt. I det mindste ikke på det generelle plan. På dette niveau har overvågning nemlig både positive og negative aspekter i sig.

Et det eksempelvis ikke positivt at overvåge giftdepoter, spildevandsudledning, senildemente der ikke kan tage vare på sig selv? Omvendt er det ikke negativt at flere og flere offentlige rum overvåges mere eller mindre rutinemæssigt? At vi i stigende grad ikke kan gå på gaden uden at blive filmet af et anonymt kamera? At vi med betalingskort sætter elektroniske spor, der gør det mulig at registrere og overvåge os globalt? At vi med vores brug af mobiltelefon og pc'er ikke kan vide os sikre om, i hvilket omfang vi er registrerede og overvågede? Det komplicerede består i, at overvågning på en og samme tid omfatter omsorg og kontrol. Den samme proces har både en omsorgsside og en kontrolside og disse kan vanskeligt adskilles.

På det konkrete plan vil en af siderne positiv / negativ dog ofte dominere, - afhængig af tid, sted, sammenhæng og ikke mindst af interesserne bag de øjne der ser. Ikke desto mindre må man fremhæve, at da overvågning altid er indfældet i en konkret sammenhæng, må de konkrete forhold ikke bagatelliseres. Det er ikke svært at opremse en række negative aspekter ved overvågningsfænomenet. Mistænkeliggørelse, manglende tiltro og tillid, ufrihed, usikkerhed, er nogle af de oplevelser og følelser, man som overvåget kan have. Dette på trods af at argumenterne for overvågning ofte er de modsatte: overvågerne vil skabe sikkerhed, forebygge ulykker, øge trygheden, etc. Men det må ikke ignoreres, at en del mennesker hævder, at de føler sig sikrere på togstationen eller i parkerings-kældrene ved eksempelvis kamera-overvågning. Også selvom det er relativt nemt at afvise som "falske sikkerhedsfølelser", da erfaringerne viser, at hvis nogle vil omgå alt det teknologiske grej, da tager de blot masker over hovedet, tilsprøjter linserne, kaster jakker over kameraerne, hacker sig ind i computersystemerne eller er kreative og opfindsomme på andre måder.

**Det komplicerede ved overvågningsfænomenet drejer sig også om dets udbredelse**

Endnu et forhold der bidrager til at gøre fænomenet kompliceret er, at overvågning i sine nye former, allerede er blevet så udbredt. Ikke mindst fordi overvågning er blevet en integreret del af de måder, som vi organiserer vore økonomiske, politiske og sociale relationer på. I et moderne samfund der på den ene side bygger på mobilitet, hastighed, sikkerhed, og som på den anden side betragter flere og flere forhold ud fra et risiko-perspektiv, der vil der overvågning i stigende grad blive betragtet som en betingelse. Forsøget på at få demokratisk kontrol over overvågningen kommer altså EFTER fænomenets udbredelse, - ikke samtidig.

Overvågning er i sig selv ikke noget historisk nyt. Nærovervågning, eller overvågning af typen "ansigt til ansigtovervågning", er gammelkendt. Overvågning af typen - panoptikon - som især kendes fra fængsler, hvor én person eller få, gennem arkitekturens udformning kan overvåge og kontrollere de mange indsatte, har også mange år på bagen. Det nye er snarere, at nutidens overvågningstendens i vidt omfang er båret af flere samvirkende tendenser i samfundet; samfundets stigende *teknologisering, øgningen af menneskeskabte risikoområder, tendensen til at tænke i forebyggelse,* er nogle af de markante. En del teknologi har således specifikt overvågning som sit formål (fx. anonyme overvågningskameraer). Mens overvågning i andre tilfælde fremkommer som ledsagefænomen (fremkomsten af mobiltelefonen havde næppe overvågning som sit formål). Overvågning synes at være et uvilkårligt ledsagefænomen ved mange af de nye teknologier.

Med overvågningstendensens stigende udbredelse er stadig flere mennesker - børn, unge voksne, ældre omfattet af overvågning enten de vil det eller ej. Og overvågningskapaciteten er overvældende. Den tid vi er under overvågning af forskellig slags, er stigende og omfattende. Udbredelsen af overvågning omfatter stadig flere både private og offentlige rum.

Samtidig er denne udbredelse ikke sket ud fra demokratisk debat og på basis af politiske beslutninger. Ej heller selvom tendensen har afgørende og alvorlige demokratiske følgevirkninger (oplevelse af at være uden indflydelse, oplevelse af at demokratiet er sat i parentes). Overvågningstendenserne er snarere kommet listende på kattepoter, - undertiden mere eller mindre som en lus i skindpelsen. Den eftertragtede pels kender vi som elektronisk teknologisk isenkram. Vi har i mange tilfælde endda selv anskaffet os de teknologiske vidundere. Lusen opdagede vi først hen ad vejen - som overvågning og en række af ubesvarede spørgsmål. Både på det personlige plan:

- hvor meget er jeg overvåget/registreret?
- hvad kan og skal det bruges til?
- har jeg og vil jeg få nogen indflydelse på overvågningstendenserne?
- hvilke rettigheder har jeg til ikke at lade mig overvåge?

Men også på det samfundsmæssige plan:

- skal vi acceptere og er det nødvendigt at flere og flere offentlige rum overvåges?
- skal vi acceptere og er det nødvendigt at privathed og frihed skrumper?
- undergraver overvågningstendenserne demokratiet eller kan de komme under demokratisk kontrol?

Det komplicerede i udbredelsen består så vidt jeg kan vurdere det i flere ting:
overvågning er ikke altid under demokratisk kontrol
overvågning er bundet til mere og mere hverdagsteknologi
overvågning er ikke altid det primære formål men undertiden en følgeeffekt
overvågning angår i dag principielt ALLE og ikke kun NOGEN (fx. kriminelle, syge, etc.)

overvågning er oftere og oftere svaret, men hvad spørgsmålet? (effekt af vanetænkning)
overvågningstendensen har bredt sig til næsten alle rum, sektorer, organisationer og institutioner og er med til fundamentalt at ændre på vores begreber og forestillinger om, hvad der er offentligt og privat, hvad der er sikkert og usikkert, hvad man kan forebygge osv.

**Særligt udvalgte problemstillinger**
I det følgende vil der blive fokuseret på nogle udvalgte problemstillinger, der synes helt centrale i forbindelse med tidens overvågningstendenser.

For det første:
***Er overvågningen frivillig eller påtvunget?*** eller formuleret på en anden måde: Hvilke valgmuligheder har vi som borgere for at vælge til og fra - i forhold til overvågningstendensen?

Som sagt er overvågningstendensen allerede vidt udbredt. Faktisk så udbredt at man sociologisk betragtet kan tale om, at samfundet i en vis forstand ikke længere er på vej imod, men allerede er blevet omformet til, et overvågningssamfund. Ikke som et Big Brother samfund a la Orwells totalitære skrækvision, men som et pluralistisk samfund, hvor der overvåges på mange niveauer og af mange instanser - i forebyggelsens og omsorgens navn. Hvis overvågning og social kontrol før var kendetegnet ved ansigt til ansigtsrelationer, da er tendensen nu, at vi i dag ud over overvågningens gamle og velkendte former, også har en række nye; den anonyme og teknologisk bårede overvågning. Denne gør sig ikke kun gældende i de offentlige rum, men rækker også ind i de private på en så indgribende måde, at man undertiden må spørge sig selv om privatheden ikke er ved at blive ophævet.

Da spørgsmålet om overvågningens positive og negative sider ofte opleves at hænge tæt sammen med om den er frivillig eller påtvungen, er det væsentligt at få dette skel fremdraget. Mange ældre borgere oplever det positivt, at de er overvåget i eget hjem, så de kan få hjælp, når de har behov for det. Hjertepatienterne oplever det som positivt, at de er overvågede på hospitalet, så de kan få hjælp i tide, når det er påkrævet. Meget tyder på, at overvågning ikke er så problematisk, når man selv har bedt om den, - ej heller selvom den er personrettet, når blot man kender dens mål, dens form og dens omfang. Omvendt, dér hvor overvågningen foregår automatisk, alment, anonymt og påtvunget, hvilket i stigende grad er tilfældet i de offentlige rum, dér vil overvågningen ofte i lige så høj grad afføde usikkerhed, ubehag, ubesvarede spørgsmål som den bidrager til følelse af tryghed og sikkerhed. De psykologiske konsekvenser af overvågningen er tilsyneladende ikke entydige. Men generelt ved vi kun lidt, da der ikke er lavet nævneværdig forskning på området. På et meget alment plan synes konsekvenserne at veksle fra de afmagts- og tilpasningsfølelser mange udtrykker i spørgsmålet: Jamen, hvis man ikke har noget at skjule, hvad så? - til frustration, indignation, modstand på den ene side og til dæmpelse af angst og

utryghed på den anden. I det mindste blandt de generationer, der er vokset op under overvågningens og den sociale kontrols gamle former. De yngre generationer, - 80ernes og 90ernes børn og unge, der er vokset op med alle de nye tendenser som en selvfølge, hvordan forholder de sig til overvågningen? Det ved vi meget lidt om. Men man kan antage, at de forskellige generationers erfaringer med overvågning, vil afføde forskellige generationsforskelle i opfattelse, holdninger og synspunkter til overvågning.

***En særlig problemstilling***, der rejser sig i forbindelse med spørgsmålet om overvågningen er frivillig eller påtvungen, gælder de yngste generationer; *børnene* - og måske til en vis grad også andre grupper i samfundet med begrænset myndighed, så som psykisk udviklingshæmmede o.a. Der er ingen grund til at antage, at børn følelsesmæssigt adskiller sig væsentligt fra voksne i forbindelse med det at blive overvåget. Hvad der er anderledes er, at hvor voksne kan sige fra - på arbejdspladsen, i institutioner, etc., der er børn uden egentlige midler til at sige fra, kæmpe imod, vurdere konsekvenser. Da børn i dag i stadigt mindre omfang befinder sig på gader og veje, men i stigende grad er i skole og institutioner, hvor de tilbringer en stor del af dagen på et ofte begrænset område, der ikke er særlig vanskeligt at overvåge, er de ofte tvunget til at lade sig overvåge: dels nærovervåge af pædagoger og lærere, og visse steder nu også fjern-overvåge af forældre og andre i den udstrækning, at der i visse børneinstitutioner og skoler anbringes web-kameraer, som de voksne kan klikke sig ind på efter behov. Har børn ingen ret til privathed og frihed, når de er i institution? Har børn ingen ret til at bestemme og være medbestemmende om deres eget liv i børneinstitutioner og skoler? Spørgsmålet her er om særlige grupper i samfundet skal have særlige rettigheder, der kan beskytte dem imod overvågningstendenserne?

***For det andet:***
***Er der ikke en afgørende forskel på om overvågningen er personlig og synlig eller om den er automatisk og upersonlig***?

Som tidligere antydet går nutidens overvågningstendens i retning af at lade overvågningen være automatisk og upersonlig. Teknologi og medier er blevet skubbet ind imellem menneskene. De nye overvågningsformer har udviklet sig i samme takt som samfundet har udviklet sig til et risiko-samfund. Overvågningstendenserne er en del af risikosamfundets ansigt. Måske kan man ligefrem tale om, at overvågningssamfundet og risikosamfundet er to sider af samme sag. Via overvågning af flere og flere forhold søger man at forebygge uheld, ulykker, katastrofer, terror og kriminalitet. En af de priser der betales er, at overvågning afpersonaliseres.

Afpersonaliseringen af overvågningen er båret af flere samvirkende forhold:
- der søges tekniske løsninger på problemstillinger, der før blev søgt løst alene af mennesker,

- der er stor tillid og tiltro til teknologi, mens alternative løsninger sjældent overvejes,
- det er blevet trendy, mode-rigtig og vanemæssigt at søge teknologisk kontrol og magt,
- driftsomkostningerne ved teknologisk overvågning er billigere end ved personlig,
Disse forhold synes selvforstærkende og virker ikke stimulerende på at tænke i alternativer.

Nogle af konsekvenserne ved den anonyme elektroniske overvågning er, at overvågeren bliver ansigtsløs, upersonlig, følelsesløs og distanceret. Magten mister sit ansigt. Ansigtet gemmer sig bag en linse, en skærm, et stykke isenkram. Det er systemer der overvåger.

Tilsyneladende får overvågerne mere magt og kontrol over de overvågede. Den der overvåger kan føle sig mere magtfuld, kan kontrollere mere, kan med teknologiens hjælp registrere mere og vidtrækkende. Den overvågede kan føle sig afmagtsfuld, kan føle sig iagttaget, observeret og registreret uden at kunne gøre ret meget ved det. Dette gælder både når overvågningen er båret af mennesker (nærovervågning), og når den er båret af teknologi (fjernovervågning). Men eksemplerne er talrige på, hvordan der i samme takt som teknologien udvikles og udbredes, opstår nye måder at unddrage sig overvågningen på, måder at ødelægge og sætte ud af drift, etc. Ligesom magten har skjult sit ansigt, skjuler modmagten sit. Hver ny magtform afføder nye modmagtsformer.

Prisen for det overvågede samfund kan blive høj, da den nemmest betales på de konti, der hedder tillid, åbenhed, dialog, frihed. Forhold og værdier i samfundet, der er nemme at miste, men vanskelige at bygge op. Tillid, åbenhed, dialog og frihed kræver mod - herunder mod til at få tidens overvågningstendenser under demokratisk kontrol.

## Teknologier på arbejdspladsen

*Af Peter Christensen, CNDO*

Anvendelsen af teknologier til overvågning på arbejdspladsen afspejler den økonomiske udvikling på dette område: faldet i omkostninger ved teknologi-investeringer sætter i dag ikke nogen økonomiske grænse og gør behovet for regelsæt og etiske principper på dette område nærværende.

### Analoge teknologier

Den fysiske overvågning af arbejdet og arbejdspladser via video-overvågning er i de seneste år eksploderet; både fordi teknologien med web-cams er faldet drastisk i pris og fordi størrelsen af apparaterne er faldet og de dermed kan skjules.

Samtidig er denne form for overvågning blevet digitaliseret, hvilket medfører muligheden for at 'genkende' skikkelser, profiler m.m. Dermed kan man sammenholde uafhængige registreringer med hinanden og drage slutninger, som ofte alene vil basere sig på teknologiens konklusioner.

I denne sammenhæng er det nødvendigt at fastslå, at enhver registrering på et netværk nødvendigvis må bestå af 2 elementer: en identifikation af den person, der er ansvarlig for trafikken, og de kvalitative elementer i trafikken f.eks. opslag på specifikke bankkonti, web-sider osv. På Internettet vil en person-registrering i dag ofte bestå af at sammenholde data fra flere servere.

### Server-logning

For at sikre, at IT-systemer er tilgængelige og kunne registrere eventuelle fejl udskrives en log og dannes backup på næsten alle IT-systemer. I alle former for servere registrerer/logger man mange data alene for at kunne registrere/undgå nedbrud. F.eks. i en firewall, der er døren ud mod Internettet og hackere, der forsøger at komme ind udefra. Disse logs indeholder oplysninger om alle data, der er forsøgt/lykkedes at få igennem en firewall dvs. mails, fil-transmissioner, opslag på web-sider osv.

Logs fra firewalls og andre former for servere f.eks. web-servere kan derfor også tilpasses og bearbejdes så personlige oplysninger kan aflæses ved at sammenholde med en arbejdsstations IP-adresse. En arbejdsstation og dermed en IP-adresse vil normalt i praksis være knyttet til en bestemt person. En server-log vil således kunne være en brik i en registrering af en persons adfærd på en bestemt server – og i det tilfælde hvor serveren formidler den generelle netværkstrafik som f.eks. firewalls altså en meget væsentlig brik. Dette gælder f.eks. de web-sites, man har besøgt på Internettet, de e-mails man har afsendt og de telefonnumre, man eventuelt har ringet til. Men det er en beslutning om man vil anvende logs og backup-kopier til dette formål eller blot anvende dem til det formål, de er skabt til: sikre systemernes stabilitet. I den nye lov om behandling af persondata lægges vægt på, at man kan

relatere det formål, som registrerede persondata anvendes til, med det formål, som der oprindeligt var argumentet for at opsamle samme data.

Samtidig eksisterer der en analogi til den tidligere lov om registrering af persondata, som forbød registrering af telefonnumre med mindre der var en forretningsmæssig årsag til dette f.eks. på hoteller. Forbuddet mod denne specifikke form for registrering blev i udvalget vedrørende betænkningsarbejdet i '77 begrundet i, at en person ikke skulle kunne ligge under for en registrering af udgående og specielt indgående kommunikation – samt en mulig sammenknytning med en person i den anden ende af samtalen. Denne analogi er meget simpel; men viser, at den manglende gennemskuelighed i dagens kommunikationsformer ser ud til at skabe grobund for et ønske om en stærkere kontrol med disse.

**Aktiv registrering**

Med de nye systemer er begrebet 'agenter' begyndt at dukke op. Agenter er enten intelligente dele af software-systemet, der holder øje med, om man har fået virus på maskinen, om man behøver en ny opdatering af software osv. eller også registreringsfiler, cookies, som visse Internet-sider efterlader som elektroniske spor på harddisken. Disse elementer har til formål at gøre brugen af systemerne nemmere; men anvendes via deres formål nødvendigvis også til at registrere profilen af den, der arbejder på maskinen. F.eks. kan visse agenter foreslå Internet-adresser, der ligner dem, man plejer at besøge og i cookies vil der være registreret hvornår du sidst var på en bestemt Internet-adresse og hvad du valgte at kigge på. Næste besøg på den samme adresse kan så tilpasses denne profil ved at præsentere de sider, der 'matcher' indholdet af din profil.

Disse agenter er i dag så udbyggede, at de i realiteten kan anvendes til digital registrering af det totale forløb af dagens arbejde på en arbejdsstation eller en person uanset om snakker om tastningen på tastaturet eller hvilke web-sider, der anvendes. For ansatte kan denne registrering kan sammenlignes med den mekaniske registrering af tasteoperatørers arbejde, som PROSA fik afskaffet ultimo 70'erne på statens edb-central: Datacentralen. Ligesom dengang er det altså nødvendigt at sikre en beslutning om ikke at anvende disse data til kontrol. Forskellen i dag vil være, at man har indset det urimelige i en kvantitativ overvågning af arbejdet; men hælder til en mere kvalitativ overvågning ud fra hvad arbejdstiden *ikke* skal anvendes til. Det ser således ud til, at arbejdsgiverside kompenserer for manglende tilpasning af ledelsesmetoder til den IT-baserede arbejdsplads med en IT-baseret registrering/ kontrol. "Management by Eye"-syndromet i stedet for den opgave/resultatorienterede management er på samme måde også en af barriererne for udvidelsen af distance/ hjemme-arbejde.

Agent-teknologier er forholdsvis simple og allerede meget udbredte. Kombinationen af oplysninger fra agenter, cookies og mere traditionelle registreringer af kunder m.m. er tiltagende i forbindelse med arbejde på Intra- og Internettet. De nyeste

versioner af office-systemer er direkte lagt an på, at den enkelte bruger har en veldefineret offentlig profil, der kan aflæses ude på Internettet. Et eksempel på dette er Microsofts Hailstorm, hvor hver bruger via en standard kan/forventes identificere sig overfor Internettet, således at e-handels- eller andre systemer, der behøver sikker identifikation, blot kan forespørge på denne profil.

En begrænsning af denne type overvågning vil nødvendigvis kræve et indgreb i retten til at sammenkæde person-data, hvilket i dag kun ville kunne ske ved en eksplicit fortolkning af lovgivningens krav om formålsberettigelse ved enhver behandling af persondata.

**Personregistrering og udveksling**
Inden for statsligt/kommunalt regi, der hidtil har foretaget de kvantitativt største personregistreringer ad mere traditionel form, er interaktionen mellem registrene øget. Sammenkøring/udveksling af personoplysninger foregår nu ikke kun på nationalt plan; men den nye registerlov har åbnet for en større interaktion, der dog stadig i hvert tilfælde skal retfærdiggøres.

Specielt politimæssige registreringer udveksles i stort omfang via Schengen-samarbejdet med andre europæiske politiinstanser. Den nationalt baserede lovgivning tager omvendt ikke højde for anvendelse udenfor landets grænser: om data er forkerte og misbrugte registreringer er reelt umulige at opdage og få rettet. Dette står i skarp kontrast til de intentioner om en overordnet fælles beskyttelse af EU-borgeren mod misbrug af persondata, som EU-direktivet til grundlag for lov om behandling af persondata foreskriver.

**Uddybning**
Privatliv: http://www.privatliv.net
Elektroniske spor: http://www.fsk.dk/cgi-bin/doc-show.cgi?doc_id=3810&doc_type=37&markwords=elektroniske+spor
Hailstorm: http://www.microsoft.com/presspass/features/2001/mar01/03-19hailstorm.asp

## Overvågning med kriminalpræventivt og –opklarende sigte

*Af Professor dr. jur. Eva Smith, Formand for Det Kriminalpræventive Råd.*

### Indledning

Mit navn er Eva Smith. Jeg er professor ved Københavns Universitet og formand for Det Kriminalpræventive Råd, der er en sammenslutning af knap 50 private og offentlige paraplyorganisationer, der ønsker at medvirke til forebyggelse af kriminalitet i det danske samfund.

Jeg vil takke Teknologirådet for, at også Det Kriminalpræventive Råd har fået muligheden for et indlæg på denne spændende konference.

Temaet for konferencen her i eftermiddag er "Overvågning med et kriminal-præventivt og - opklarende sigte". Hovedspørgsmålet er i denne forbindelse, hvordan vi kan sikre, at lovgivningen og administrationen er på højde med udviklingen, således at det enkelte menneskes retssikkerhed tilgodeses?

Et meget vigtigt spørgsmål, som vi i Det Kriminalpræventive Råd faktisk har brugt megen tid på at diskutere, og som vi sidste år udsendte et gennemarbejdet debat-oplæg omkring.

Jeg er i dag særligt blevet bedt om at komme ind på fire underspørgsmål:

- Hvad er virkningerne af kriminalpræventiv overvågning?
- Hvad synes borgerne om video-overvågning?
- Brug af elektronisk overvågning i Politiets arbejde.
- Bankernes ønsker om mere videoovervågning.

Hvis elektronisk overvågning skaber en forventning om forøget sikkerhed for de overvågede, medfører det så nogle særlige ansvarsmæssige forhold for den, hvis job, det er at overvåge?

Inden vi overhovedet går i gang, er det måske kort på sin plads lige at vise Det Kriminalpræventive Råds bidrag til debatten om elektronisk overvågning "TV-overvågning - Mellem forebyggelse og krænkelse" og orientere om, at hæftet er til rådighed bagerst i lokalet.

### TV-overvågning

Dette indlæg skal være kort, og derfor vil jeg alene koncentrere mig om en del - men måske nok den mest markante del af den elektroniske overvågning - nemlig TV-overvågningen.

TV-overvågning er et område i stærk vækst - både hvad angår hvor, hvordan og af hvem det anvendes. Der udbydes og sælges flere og flere overvågningssystemer, priserne falder og teknologien tilbyder stadig flere og mere avancerede løsninger.

TV-overvågningen vinder med andre ord i stigende grad indpas i alle danskeres liv.

Ikke mindst TV-overvågning som et kriminalpræventivt "Vidunder-middel" er med jævne mellemrum oppe at vende i debatten. Skal vi i stigende grad gøre brug af TV-overvågning som kriminalpræventivt middel? Eller risikerer vi derved at opbygge et samfund, hvor det enkelte individs grænser overskrides i forebyggelsens hellige navn. Hvor tryghed forvandles til utryghed, tillid til mistro, forebyggelse til kontrol. Altså et samfund, hvor kriminalitet forebygges og opklares, men måske på bekostning af almindelige menneskers almindelige trivsel.

**Erfaringer og undersøgelser**

Erfaringer og undersøgelser viser, at TV-overvågning ofte kan være et effektivt middel til at tilbyde sikkerhed og tryghed for borgere og erhvervsliv. Erfaringerne fra ind- og udland viser, at tv-overvågning rent faktisk har en forebyggende effekt over for en række former for kriminalitet. Samtidig er TV-overvågning ikke sjældent et godt bidrag i forbindelse med opklaringen af forbrydelser, som ellers kunne frygtes at forblive uopklarede.

Det modstående hensyn er imidlertid, at TV-overvågning kan medføre, at folk føler sig utrygge og krænkede. Hertil kommer, at overvågning for andre måske medfører en falsk fornemmelse af tryghed.

En Gallup-undersøgelse gennemført af Det Kriminalpræventive Råd viser, at danskerne i hovedsagen er ganske positivt indstillede over fortovsovervågning på afgrænsede områder. Men der er på den anden side også en helt klar grænse, hvor TV-overvågning kan få folk til at føle sig både utrygge, "udspionerede" og kontrollerede.

Den danske befolkning er efter vores undersøgelse generelt meget positiv indstillet over for overvågning i butikker, tankstationer, banker, indkøbscentre og togstationer. Derimod er befolkningen kraftigt imod overvågning på f.eks. arbejdspladsen eller i den mere private sfære (ved
og omkring boligen m.v.).

På den måde kommer TV-overvågning til at befinde sig i et spændingsfelt mellem forebyggelse af kriminalitet og krænkelse af individets integritet. Spørgsmålet er, hvor et acceptabelt balance-punkt findes.

**Et trygt samfund med TV-overvågning??**
Det Kriminalpræventive Råd interesserer sig naturligt for udviklingen i TV-overvågning af flere årsager. Helt naturligt tager vi udgangspunkt i, at TV-overvågning har en forebyggende effekt og udgør et godt bidrag i forbindelse med opklaringen af forbrydelser. Vi ser derfor en række positive muligheder i TV-overvågning.

Men Det Kriminalpræventive Råd har også i et bredere perspektiv til opgave at vurdere, hvad der skal til, for at vi har et trygt samfund - og for at vi føler os trygge.

Den øgede brug af TV-overvågning må ikke medføre, at vi hver især fralægger os ansvaret for "at passe på hinanden".

Et ubemandet, eller måske et bemandet overvågningsanlæg på et offentligt tilgængeligt sted kan bidrage til, at vi føler os trygge, men denne følelse kan jo til dels være falsk.

Ved det ubemandede kamera kommer ingen til hjælp, hvis der sker noget. Et ubemandet kamera er således alene noget, der kan bruges ved en senere opklaring af forbrydelser.

Og selv ved et bemandet Tv-overvågningssystem må man overveje, om den forventning om forøget sikkerhed, der ofte opstår hos de overvågede, rent faktisk er reel. Man kan ikke med sikkerhed regne med, at det personale, der sidder bag overvågningssystemet nødvendigvis vil handle. Man kan altså ikke umiddelbart fæstne lid til, at der kommer hjælp, hvis uheldet er ude.

Dette forstærkes yderligere ved det faktum, at der i en del systemer faktisk overvåges fra stor distance, hvor overvågningspersonalet fysisk befinder sig langt væk fra den lokalitet, der overvåges.

TV-overvågning kan med andre ord skabe en "falsk tryghed". Og samtidig er det også et faktum, at selve synet af et overvågningskamera kan gøre mange utrygge, fordi det leder tankerne hen på risikoen for at blive udsat for kriminalitet.

Samlet kan man måske sige, at en fortsat udvidet adgang til TV-overvågning, som givetvis vil være ønsket og realiteten i fremtiden, rejser spørgsmålet om, hvorvidt der skal pålægges nogle særlige ansvarsmæssige forhold hos den, hvis job, det er eller bliver at overvåge.

Og set med Det Kriminalpræventive Råds øjne skulle vi i hvert fald nødig komme derhen, hvor den "sociale kontrol" afløses af TV-overvågning, uden at vi samtidig har gjort os tanker om, hvilket ansvar det så medfører, for de firmaer eller personer, som tilbyder og gennemfører overvågningen.

**Dilemmaer**
En udvidelse af området for TV-overvågning vil samtidig betyde, at overvågerne og dermed også politiet og andre myndigheder nødvendigvis vil komme i besiddelse af en lang række oplysninger og måske også blive vidne til en række mere "bagatelagtige" lovovertrædelser, som vi ikke før har været bekendt med. Hvordan skal denne informationsstrøm håndteres? Har vi tilstrækkelige regler til at håndtere opbevaring, brug, videregivelse m.v. af de mange oplysninger, som gennem en udvidelse af TV-overvågningen nødvendigvis vil komme til at ligge på adskillige bånd mange forskellige steder i det danske samfund? Hvordan er slettereglerne?

Jeg tror disse spørgsmål vil være en ganske stor udfordring for lovgivningssystemet i de kommende år. Og herudover vil der være en række moralske og etiske dilemmaer, som sideløbende skal håndteres.

**Afslutning**
Debatten om TV-overvågning og kriminalitet er således tostrenget: Der er både et "forebyggende aspekt" og et "trygheds-krænkelsesaspekt", som vi må forholde os til.

Det Kriminalpræventive Råd har gjort sin holdning op i debathæftet "TV-overvågning - mellem forebyggelse og krænkelse", hvor vi kommer med en række råd og anbefalinger, der søger at skabe en balance mellem på den ene side hensynet til individet og på den anden side til den kriminalpræventive effekt af TV-overvågning.

I vores anbefalinger - som jeg desværre ikke har tid til at komme nærmere ind på her, men som jeg opfordrer jer til at læse i debatoplægget - har vi søgt at tilgodese det enkelte menneskes retssikkerhed mest muligt. Og det bliver i stigende grad nødvendigt i takt med den teknologiske udvikling, der i dag er i stand til at tilfredsstille selv den mest livlige fantasi.

Der findes populært sagt kun kortsigtede begrænsninger for, hvad man kan med TV-overvågning nu og i fremtiden.

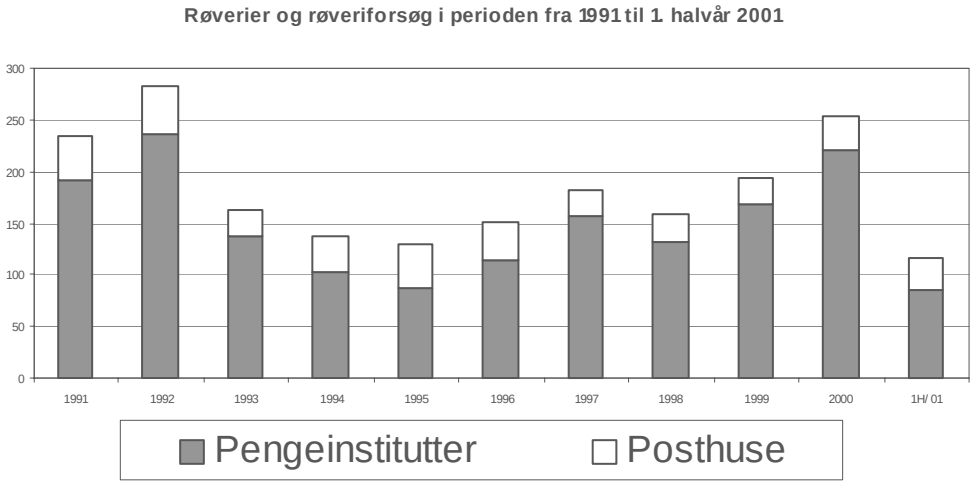
Den store udfordring for lovgivningsmagten bliver at sikre, at området er tilstrækkeligt reguleret til at beskytte individet godt nok. Ønsket om, at netop dette område skal lovreguleres grundigt, deles i øvrigt af ca. 90 % af den danske befolkning ifølge Det Kriminalpræventive Råds borgerundersøgelse.

Lovgivningen gør sit bedste for at følge med. Der justeres og ændres således med jævne mellemrum, men den teknologiske udvikling vil i sagens natur være et skridt foran lovgivningen. Ikke mindst derfor er også mere moralske og etiske overvejelser og en klar holdning på området nødvendig.

## Overvågning med kriminalpræventivt og -opklarende sigte

*Af Niels Crone Lyngkjær, Kontorchef i Finansrådet*

Pengeinstitutterne og Post Danmark har siden 1991 oplevet den i figur 1 viste udvikling i antal røverier og røveriforsøg.




Til trods for meget betydelige investeringer på sikringsområdet må det med beklagelse konstateres, at det ikke har været muligt at nedbringe antallet af røverier til et acceptabelt niveau.

Pengeinstitutterne driver, som andre erhvervsdrivende, en virksomhed, som har berøring med hele den danske befolkning. Uanset en kraftig automatisering gennem de sidste 40 år, hvor blandt andet Dankortet har slået kraftigt igennem op gennem 1990'erne, og i dag benyttes mere end 400 millioner gange på årsbasis af kortholderne, har pengeinstitutsektoren stadig en kraftig berøring med kunderne i de ca. 2.200 filialer, som eksisterer rundet omkring i landet. I 1990, da de store fusioner gennemførtes, havde sektoren mere end 3.000 filialer.

Sektoren har et ønske om i fred og ro at få lov til at drive virksomheden, men en ganske lille minoritet i befolkningen er af den opfattelse, at den vare, som pengeinstitutterne har på hylden – nemlig kontanter – står til denne lille minoritets frie afbenyttelse.

### "Passive" sikringstiltag

Uanset at pengeinstitutterne gennem de sidste 15-20 år har udbygget deres alarmanlæg, opsat fotoanlæg og i de senere år videoanlæg, som følge af den tekniske udvikling, har indført røg- og farvepatronsystemer i en række filialer og andre tekniske tiltag i atter andre filialer, så har dette ikke virket afskrækkende på den lille

minoritet af kriminelle elementer, som føler sig draget af pengeinstitutternes vare på hylden.

Pengeinstitutternes sikringskoncept drøftes nøje løbende med politiets repræsentanter i kontaktudvalget (uformelt samtaleforum mellem politi, Post Danmark og Finansrådet). For ikke at optrappe volden i forbindelse med røverier har politiets repræsentanter i kontaktudvalget været enige i det "passive" sikringskoncept, som pengeinstitutterne søger at efterleve i stort omfang, og som fremgår af de af Det Fælles Sikringsudvalg (nedsat af Danmarks Nationalbank, Post Danmark og Finansrådet) udgivne anbefalinger til sikring af pengeinstitutter og posthuse.

Som nævnt er der tale om "passive" sikringsforanstaltninger, idet pengeinstitutterne i deres egenskab af arbejdsgivere – og i nøje overensstemmelse med politiets ønsker – ikke ønsker at medarbejderne skal forsøge at forhindre røverne i deres forehavende. Penge er døde ting, for hvilke der ikke skal kæmpes. Pengeinstitutternes medarbejdere er nøje instrueret heri og gennemgår med jævne mellemrum en vedligeholdelse af den på sikringsområdet givne uddannelse, således at der, når situationen opstår, ageres på rygmarven.

**De menneskelige omkostninger**

Det største problem for pengeinstitutterne i forbindelse med røverierne er de menneskelige omkostninger for de medarbejdere, som udsættes for røverierne. Også kunder, som overværer røverier, kan blive psykisk belastet heraf. Pengeinstitutterne ofrer derfor – udover på den uddannelsesmæssige side – også væsentlige ressourcer i form af psykologhjælp til medarbejdere, som har været udsat for røverier. Uanset dette må det med beklagelse konstateres, at mange medarbejdere først ad åre er i stand til så nogenlunde at fortrænge hændelserne. Og det er desværre således, at der er medarbejdere, som aldring overvinder, hvad de har været udsat for, og derfor på et tidspunkt må sygepensioneres. I sandhed en hård straf specielt set i forhold til den som oftest bliver gerningsmanden til del.

**"Aktivt sikringskoncept"**

Det har været drøftet, hvorvidt et mere "aktivt" sikringskoncept fx i form af adgangskontrol, slusesystemer med detektorer, vagter etc. kunne nedbringe antallet af røverier. Sektoren er ikke i tvivl om, at sådanne tiltag vil have en effekt. Men prisen herfor skal betales af de 99,9999 pct. af kunderne, som i lovligt ærinde besøger pengeinstitutternes filialer. Og sektoren er bange for, at den slags tiltag vil medføre, at de røverier, som bliver tilbage, vil blive væsentligt mere voldelige end tilfældet generelt er i dag, og eventuelt medføre gidseltagninger etc.

**Yderligere "passive" sikringstiltag**

Sektoren går derfor fremdeles primært efter de "passive" sikringstiltag. Gennem de sidste par år har sektoren generelt søgt at nedbringe størrelsen af den kassebeholdning, som er tilgængelig for ekspeditionernes gennemførelse. Afhængig af den

enkelte filials størrelse, beliggenhed og kundesammensætning kan også dette tiltag være problematisk, idet røvere, dersom der ikke er kontanter nok til disposition i kassen, forlanger boksen og/eller pengeautomaten åbnet. Denne trafik er ikke ganske ualmindelig i mere afsides beliggende områder af landet, hvor det vil tage en vis tid for politiet at nå frem, når alarmen går. Det er sektorens opfattelse, at de kriminelle elementer spekulerer heri, for derved at have mest mulig tid til disposition for røveriets udførelse.

Sektoren installerer derfor p.t. en del steder tidsforsinkelseslåse i forhåbning om, at de kriminelle elementer, når de konstaterer denne foranstaltning, opgiver adgangen til kasseskuffer, pengeautomatskabe og boksanlæg.

**Hvorfor et ønske om mulighed for udendørs overvågning**
Finansrådet rettede i januar 2000 henvendelse til Justitsministeriet om en ændring af Lov om forbud mod TV-overvågning mv. med henblik på, at det for penge-institutterne kunne blive muligt at foretage videoovervågning af pengeinstitutfacader, pengeautomater etc. Som anført i skrivelse til Justitsministeriet er sektorens begrundelse, at man mener, at det vil være af største værdi for politiet, at få optagelser af de kriminelle personer, såvel når disse ankommer, som når de forlader filialer med udendørs overvågning. Det antages, at de kriminelle oftest i forvejen har holdt pågældende filial under observation og eventuelt aflagt besøg i denne inden røveriets gennemførelse. Endvidere antages det, at røveren oftest først iører sig maskering, når pågældende nærmer sig filialen, og straks røveriet er overstået og filialen forlades affører sig maskeringen. Begge dele for ikke at vække mere opsigt end strengt nødvendigt.

Endelig vil en sådan adgang kunne være til gavn for politiet også i situationer, hvor der er begået svindel ved anvendelse af pengeautomater og valutavekslings-automater, idet pengeinstitutterne gennem de senere år har konstateret et stigende antal forsøg på denne form for svindel.

**Værdien af de gennemførte "passive" sikringstiltag**
Sektoren tror på, at de gennemførte sikringstiltag har en kriminalpræventiv effekt, således at nogle "kriminelle kandidater" opgiver deres forehavende. Dels er en del af tiltagene synlige, dels orienteres befolkningen generelt via mediernes dækning ganske udmærket om, at det at begå røveri mod en pengeinstitutfilial ikke er uden risiko for at blive anholdt, som følge af pengeinstitutternes sikringsforanstaltninger.

De gennemførte "passive" sikringstiltag er imidlertid primært til gavn for politiets opklaringsarbejde. Jo bedre oplysninger om gerningsmanden pengeinstitutterne kan give, desto større er politiets muligheder for at få anholdt pågældende. Og jo hurtigere dette sker, desto større er chancen for at eventuelt våben, maskering, penge etc. er til stede, hvilket vil føre til en hurtigere opklaring af sagen og dermed hurtigere mulighed for domfældelse. Alt sammen forhold, som bør virke

afskrækkende på andre, som overvejer beskæftigelse i denne branche. Sektoren er i øvrigt glad for, at politiets opklaringsprocent, set over en periode, nærmere sig de 75 pct.

**Hvor mange steder vil pengeinstitutterne sætte udendørs overvågning**
Pengeinstitutterne forestiller sig ikke opsætning af udendørs overvågning i forbindelse med alle filialer. Hertil vil det udstyr, som skal opsættes, være alt for bekosteligt. Imidlertid vil det kunne være af værdi i forbindelse med et antal filialer, som ofte har været udsat for røveri, at kunne opsætte sådant udstyr permanent eller i en periode – afhængig af situationen.

Det opsatte udstyr vil blive koblet på eksisterende udstyr. Optagelserne vil blive lagret i en periode frem – oftest 30 dage – hvor disse vil være tilgængelige for politiet i tilfælde af kriminelle hændelser.

Selvfølgelig vil medarbejderne i pengeinstituttet have adgang til optagelserne, så længe disse lagres, men kun i situationer, hvor det viser sig nødvendigt, vil medarbejdere bruge tid på at se i de lagrede oplysninger.

**Det Kriminalpræventive Råds undersøgelse og anbefalinger samt politiets vurdering**
Et par måneder efter, at Finansrådet havde rettet henvendelse til Justitsministeriet i begyndelsen af 2000, offentliggjorde Det Kriminalpræventive Råd anbefalinger i forbindelse med TV-overvågning. Finansrådet har noteret sig, at i den holdnings-undersøgelse om TV-overvågning, som fremgår af hæftet "TV-overvågning – Mellem forebyggelse og krænkelse", er 93 pct. af de adspurgte overvejende positive for TV-overvågning i pengeinstitutter (banker), mens alene 3 pct. af de adspurgte er overvejende negative.

Finansrådet er i øvrigt ganske enige i de holdninger og anbefalinger, som Det Kriminalpræventive Råd har fremlagt i ovennævnte hæfte.

Finansrådet har også noteret sig, at politiet i hæftet er citeret for at vurdere, at TV-overvågning spiller en vigtig rolle i forbindelse med at forebygge især røveri og indbrud mod blandt andet pengeinstitutter. Dette ligger i øvrigt helt på linie med de synspunkter, som politiet har fremlagt i kontaktudvalget.

Det kan i øvrigt oplyses, at Finansrådets henvendelse til Justitsministeriet primo 2000 havde været drøftet i kontaktudvalget og støttedes af såvel politiets repræsentanter i udvalget som Det Kriminalpræventive Råds repræsentant i dette.

**Finansforbundet**
Finansforbundet, som er de pengeinstitutansattes hovedorganisation, er repræsenteret i Finansrådets sikringsudvalg. Finansforbundet står bag pengeinstitutsektorens ønske

om mulighed for at kunne foretage opsætning af overvågningsudstyr udendørs i forbindelse med pengeinstitutternes filialer.

**Afslutning**

På denne baggrund ser Finansrådet hen til, at en ændring af Lov om forbud mod TV-overvågning mv. gennemføres snarest, således at pengeinstitutterne får adgang til den ønskede udendørs opsætning af overvågningsudstyr på steder, hvor dette vurderes at have såvel præventiv som god opklaringsmæssig effekt.

## Overvågning med kriminalpræventivt og –opklarende sigte

*Disposition for oplæg af Troels Ørting Jørgensen, Vicekriminalinspektør i Rigspolitiets afdeling A*

- Teknologi og overvågning.

- Internettets muligheder og begrænsninger.
  - peer to peer,
  - IRC,
  - Freenet,
  - kryptering,
  - instant messages,
  - "X-drives"
  - IP telefoni,
  - lagringskapacitet – log informationer.

- GSM telefoni.

## Overvågning med efterretningssigte

*Af Jørn Bro, Politimester i Glostrup og tidligere souschef i Politiets Efterretnings Tjeneste*

Generelt drejer efterretningstjeneste sig om at tilvejebringe, kontrollere, analysere, vurdere, bearbejde og sammenstille oplysninger fra mange kilder, så der på relevante områder skabes en fond af kendsgerninger, hvorpå politiske, militære, politimæssige og andre beslutningsprocesser kan foretages.

Uden et velfungerende efterretningsvæsen vil en stat på mange måder være blind.

Den løbende tilvejebringelse af efterretningsbilledet vedrørende de udpegede interesse- og målområder sker i vid udstrækning på basis af åbne kilder. Efterretningstjeneste adskiller sig på dette felt principielt ikke fra den virksomhed, der udøves af diplomater, journalister, forskere og virksomhedskonsulenter. I et åbent samfund som det danske kan efterretningsbilledet i væsentlig grad skabes ad denne vej.

Efterretningstjenesten kan derfor også med rette betegnes som dybdeborende journalistik, om end med en stærkt begrænset, men på den anden side også højt kvalificeret læserkreds.

I sine bestræbelser på at komme ned under overskrifterne og på at afdække skjulte, farlige og samfundsskadelige aktiviteter må efterretningstjenester også sætte ind med foranstaltninger og metoder, der berettiger betegnelsen "hemmelig tjeneste". Til dette begreb er knyttet megen fascination, og mange uklarheder og myter – herunder den udbredte misforståelse, at de danske efterretningstjenester overvåger borgerne. Ihærdige bestræbelser på at "Stasi-gøre" vore såre beskedne efterretningstjenester har med mellemrum vundet urimeligt megen gehør i den politiske og samfundsmæssige debat.

### Et historisk fænomen

Efterretningstjenesters virke og metoder er ikke et moderne fænomen, men et historisk. Der findes en omfattende litteratur, der beskriver, hvordan stater og politiske partier og grupperinger, og etniske og religiøse organisationer har forsøgt at fremme deres mål gennem spionage, sabotage, undergravende virksomhed, anstiftelse af vold, desinformation og psykologisk krigsførelse, og terrorisme. Fælles for disse aktiviteter er, at de normalt udføres skjult og hyppigt under dække af og sideløbende med mere eller mindre lovlige aktiviteter. Afdækning af og især forebyggende imødegåelse af sådanne aktiviteter må i vid udstrækning ske ved anvendelse af efterretningsmæssige metoder.

**De danske efterretningstjenester**
Forsvarets Efterretningstjeneste henhører under Forsvarskommandoen og Forsvarsministeriet. Den varetager den udlandsrettede politiske, økonomiske og militære efterretningsvirksomhed, samt den militære, præventive sikkerhedstjeneste.

Politiets Efterretningstjeneste er organisatorisk en landsdækkende politiafdeling under Rigspolitichefen. PET's chef refererer imidlertid direkte til Justitsministeriet, som løbende holdes underrettet om såvel væsentlige enkeltsager som om mere generelle forhold.

PET er den nationale sikkerhedstjeneste, der har til opgave at overvåge, forebygge, modvirke og forhindre foretagender og handlinger, som må antages at rumme en fare for rigets selvstændighed og sikkerhed og den lovlige samfundsorden.

PET beskæftiger sig således med at modvirke spionage, anden ulovlig efterretningsvirksomhed, terrorisme, voldelige aktiviteter, der udgår fra ekstremistiske organisationer og grupperinger, organiseret kriminalitet af en grovhed og et omfang, der truer statens sikkerhed og samfundsordenen, samt sager om spredning af masseødelæggelsesvåben. Tjenesten varetager endvidere en række opgaver i forbindelse med den forebyggende sikkerhed i den offentlige administration. Endelig varetager PET en række sikkerhedsbeskyttelsesopgaver, omfattende kongehuset, regeringens medlemmer og fremtrædende udenlandske gæster.

Henset til denne emnekreds, der her er under behandling, vil mine efterfølgende betragtninger i alt væsentligt alene dreje som om den af Politiets Efterretningstjeneste udøvede virksomhed, der i modsætning til Forsvarets Efterretningstjenestes udøvede virksomhed har direkte relation til borgerne og deres retssikkerhed.

**PET's virkemidler**
Som en del af politiet er PET i sit virke som andre politimyndigheder omfattet af retsplejeloven. Særligt er der grund til at pege på bestemmelserne i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden og observation.

Her er der i paragrafferne 780 – 791 a givet detaljerede regler for anvendelsen af efterforskningsmidler som telefonaflytning, rumaflytning og anden aflytning, teleoplysninger (hvem har været i forbindelse med hvem), brevåbning og brevstandsning, ligesom der er givet regler for observation på ikke frit tilgængeligt sted ved hjælp af tekniske hjælpemidler.
Anvendelsen af disse indgreb forudsætter retskendelse, hvis meddelelse hviler på en række kvalificerede krav.
Retsplejelovens indgående regelstyring er udtryk for den store vægt, der i det danske samfund tillægges borgernes retssikkerhed. De, der administrerer disse regler – dommere, anklagere og politifolk -, er nøje uddannet og opdraget i den samme juridiske tradition med den største respekt for legalitetsprincippet. Hertil kommer de

meget væsentlige retssikkerhedsmæssige garantier, der følger af forsvars-advokaternes kompetente og energiske indsats.
På årsbasis meddeler retterne i hele landet ca. 1700 kendelser om indgreb i meddelelseshemmeligheden. Heraf er ca. 800 telefonaflytningskendelser og ca. 900 kendelser om teleoplysninger. Ca. 900 kendelser relaterer sig til narkosager, og i denne sagskategori er der hyppigt tale om bandeforbrydelser, hvor en enkelt efterforskning let fordrer 5 – 10 kendelser. Det samme gør sig gældende i de grove sager om vold, drab, organiserede røverier og tyverier og anden grov organiseret kriminalitet, i nyere tid sager om menneskesmugling, hvor telefonaflytning og teleoplysninger tages i anvendelse.

Da telefonaflytningssager og bearbejdning af teleoplysninger er overordentligt ressourcekrævende, siger det sig selv, at politiet, herunder PET kun i meget begrænset omfang gør brug af disse midler.
Når man sammenholder antallet af kendelser om indgreb i meddelelses-hemmeligheden med antallet af telefoner – faste som mobile – i Danmark, og det umådelige antal samtaler, der dagligt føres over disse apparater med antallet af telefon- og telekendelser, forekommer det mig proportionsforvrængende at tale om overvågning af borgerne i forbindelse med en vurdering af politiets, herunder PET's anvendelse af og mulighed for anvendelse af disse virkemidler, der er helt afgørende i bekæmpelsen af organiseret kriminalitet, hvad enten denne er båret af økonomiske, politiske eller ideologiske motiver.

PET's interesse- og målområder fremgår af en instruks til chefen for PET, sådan som den er beskrevet i den udmærkede Redegørelse vedrørende dele af PET's virksomhed, som tjenesten med Justitsministeriets samtykke udgav i marts 1998. Den konkrete afgrænsning af, hvad PET til skiftende tider skal beskæftige sig med, afgøres i sidste instans af regeringen, i det daglige af Justitsministeriet. PET beskæftiger sig kort og godt med de områder, som regeringen og de øverste stats-myndigheder har et nødvendigt og legitimt krav på at være ordentligt informeret om, således at der kan træffes de fornødne foranstaltninger til beskyttelse af samfundet og borgerne. PET er landets mest kontrollerede politiafdeling, og det er uden hold i virkeligheden i forbindelse med PET at tale om en stat i staten.

**Registrering**
PET's registre er fortegnelser over de personer, organisationer, emner m.v., som forekommer i PET's sager. Arten og omfanget er bestemt af de opgaver, interesse- og målområder, der udstikkes af regeringen.
Mens tidsperspektivet i de sager, politiet i almindelighed beskæftiger sig med, normalt kan opgøres i uger og måneder, er tidsperspektivet i PET's virksomhed hyppigt mange år. Enhver med kendskab til spionage, efterretningsvirksomhed og terrorisme understreger behovet for langsigtethed og indsamling og bearbejdning af store stofmængder, herunder et betydeligt navnemateriale. Fænomenet er for så vidt velkendt i store kriminalsager, f.eks. drabssager, hvor navnekartoteket som en

efterforskningsnøgle let løber op i flere tusinde navne. Forskellen er, som nævnt, at i kriminalsagerne er tidsperspektivet normalt meget kortere. Det er derfor væsentligt at understrege, at det forhold at ens navn figurerer i PET's registre ikke i sig selv siger noget som helst om, hvorvidt vedkommende person er genstand for særlig mistanke eller belastende opmærksomhed.

Borgernes retssikkerhed sikres gennem de for tjenesten udarbejdede instrukser og tilsynsudvalgene, dels det såkaldte Wamberg-udvalgs tilsyn med PET's registrering og videregivelse af oplysninger, dels det parlamentariske tilsynsudvalg.

PET beskæftiger sig ikke med overvågning af borgerne. Overvågning af borgerne ville forudsætte et ganske andet politisk system, omfattende ændringer af især retsplejeloven, helt andre instrukser til PET og endeligt tilførsel af ganske andre personaleressourcer, så det for tiden værende medarbejderantal på ca. 300 skulle øges til mindst 3000 og formentligt langt højere.

**Luftbåren kommunikation – Elektronisk indhentning**
Fra omkring den 1. verdenskrig, hvor luftbåren kommunikation i form af telegrafi blev et betydningsfuldt også militært kommunikationsmiddel, har alle stater i større eller mindre omfang udviklet lyttetjenester med dertil hørende kodebrydningskapacitet, og som beskyttelse herimod chiffrering og kryptering.
Den elektroniske indhentnings betydning er omfattende beskrevet i litteratur fra den 2. verdenskrig, og vil formentlig om nogle år blive nærmere beskrevet som et uvurderligt efterretningsmiddel under Den kolde Krig. Betydningen er ikke blevet mindre, og mulighederne i takt med den elektroniske udvikling stadig større. Uden at vide det vil jeg uden videre gå ud fra, at den amerikanske regerings bevisførelse med hensyn til skylden for terrorangrebet den 11. september i meget høj grad støtter sig på elektronisk opklaring, herunder sammenstilling af historiske teleoplysninger fra alle former for kommunikationsmidler.
Anlæg og kapacitet til at kortlægge og aflytte også mobiltelefonkommunikation må nødvendigvis indgå i det efterretningsmæssige arsenal. Jeg er sikker på, at der i disse dage og timer lyttes intensivt til mobiltelefonsnakken i Kabul, for herigennem at udvinde brikker til det efterretningsmæssige puslespil, der skal klarlægge situationen i dette lukkede samfund.
Aflytning af telekommunikationen her i landet fordrer på samme måde som ved almindelig telefonaflytning retskendelse.

I den hjemlige debat har begrebet Echelon som betegnelse for aktivitet udøvet af det amerikanske National Secretary Agency i samarbejde med en række vestlige efterretningstjenester spillet en "Big Brother watching you"-rolle.
Mærkværdigvis har ingen af de bekymrede interesseret sig for tilsvarende lyttetjenester i Rusland, Kina, Iran, Irak, Nordkorea etc. – Som historisk illustration kan jeg blot minde om det betydelige antal lyttefartøjer fra Østblokken, der for få år siden permanent befandt sig i danske farvande.

Den bagvedliggende indsigt og kapacitet eksisterer stadigvæk.

Et dagblads såkaldte afsløring af, at mobiltelefonen kan aflyttes, rummer ingen nyhed. Fastnettelefonen er væsentligt mere sikker, men hvad der råbes ud i verdensrummet, kan naturligvis opsamles af hvem som helst, der har kapaciteten hertil.
Lyttetjenesterne er imidlertid – allerede af ressourcemæssige grunde – meget selektive og målrettede, så den danske befolkning kan som privatpersoner eller firmaer være bedøvende ligeglade med, om amerikanere, russere eller kinesere muligvis lytter. At vore politikere, embedsmænd og andre beslutningstagere skal tænke sig lidt om, inden de råber op i mobiltelefonen eller e-mailer ud i verden, er en helt anden snak!

For almindelige mennesker er der efter min vurdering intet behov for kryptering, og de krypteringssystemer der i givet fald ville kunne udbydes på markedet, vil ikke give beskyttelse  mod professionel aflytning og dekryptering.

På den anden side er der ikke tvivl om, at narkohandlere, menneskesmuglere, terrorister, anstiftere af alvorlige optøjer og andre grove, organiserede kriminelle savner kvalificerede krypteringsmuligheder.
Det er sådanne typer politiet, herunder PET overvåger, og ikke borgerne.

# Beskyttelse af borgerens privatliv – fra en menneskeretlig synsvinkel

*Af Birgitte Kofod Olsen, seniorforsker, ph.d., Det Danske Center for Menneskerettigheder*

## 1. Indledende bemærkninger

Næsten alle former for overvågning af borgere, herunder de der foregår med et efterretningssigte, kan betragtes som et indgreb i privatlivets fred.

Privatlivet og muligheden for at nyde dette uden indblanding er beskyttet ved den danske Grundlov og menneskeretlige konventioner. Behovet for at se nærmere på overvågning fra en menneskeretlig synsvinkel udspringer således af den retlige forpligtelse til at respektere privatlivets fred, der følger det nævnte retsgrundlag.

Det er vigtigt i denne sammenhæng at være opmærksom på, at menneskerettighederne fungerer som spilleregler i forholdet mellem borger og stat - hvor borgerens beskyttelse som udgangspunkt går forud for samfundets interesser som helhed.

Der er dog ikke tale om en kamp mellem modsatrettede interesser, men derimod om et samspil, der søger at forene statens interesse i at sikre, at dens borgere kan nyde deres beskyttede rettigheder uden vilkårlig indblanding og opfyldelse af samfundsinteresser med borgernes interesse i beskyttelse af egne rettigheder. Samfundsinteressen udgøres i denne sammenhæng af statens ønske om og behov for en effektiv efterretningsvirksomhed, der skal tjene til at fremme landets sikkerhed – og dermed også til at sikre borgernes adgang til at nyde deres beskyttede rettigheder.

I praksis vil dette samspil udmønte sig i en afvejning af den enkelte borgers interesse i beskyttelse af sit privatliv i forhold til interessen i effektiv efterretningsvirksomhed i et konkret tilfælde.

Menneskeretten tager højde for den situation, at samfundsinteressen i nogle tilfælde vejer tungere end borgerens interesse med det resultat, at beskyttelsen må tilsidesættes. Der er derfor i tilknytning til privatlivsbeskyttelsen åbnet adgang for, at staten kan gribe ind i det beskyttede privatlivsområde, hvis der findes lovhjemmel dertil i den nationale lovgivning, hvis der findes et lovligt hensyn og hvis det i den konkrete situation er nødvendigt.

## 2. Borgerens privatlivsbeskyttelse

### 2.1. Retsgrundlaget

Retten til at få respekteret sit privatliv er et eksempel på en af de grundlæggende frihedsrettigheder, som har fundet udtryk i såvel den danske Grundlov som i de menneskeretlige dokumenter, der er tilvejebragt efter 2. verdenskrig af medlemsstaterne i FN og Europarådet.

I Grundlovens § 72 er den del af borgerens privatliv, der omfatter retten til at være i fred på et bestemt sted fastsat, ligesom bestemmelsen indeholder beskyttelse af korrespondance. Bestemmelsen har følgende ordlyd:

> ”Boligen er ukrænkelig. Husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse.”

I FN Konvention om Civile og Politiske rettigheder er i art. 17 fastsat en privatlivs-beskyttelse, som udvider beskyttelsesområdet til også at omfatte andre dele af privatlivet samt familieliv, ære og omdømme. I bestemmelsen står:

> ”Ingen må udsættes for vilkårlig eller ulovlig indblanding i sit privatliv eller familieliv, sit hjem eller sin brevveksling, eller for ulovlige angreb på sin ære og omdømme.
> Stk. 2. Enhver har ret til lovens beskyttelse mod sådan indblanding eller sådanne angreb.”

Den Europæiske Menneskerettighedskonvention indeholder i art. 8 beskyttelsen af privatlivet. Denne bestemmelse afgrænser beskyttelsesområdet stort set på samme måde som FN-konventionen, men er klarere i sin definition af indgrebsmuligheden i stk. 2. Bestemmelsen lyder:

> ”Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
> Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder.”

### 2.2. Hvad dækker privatlivsbeskyttelsen?

Af ordlyden af bestemmelserne om privatlivsbeskyttelse, forstår man kun tilnærmelsesvis, hvad beskyttelsen omfatter. Fortolkningsbidrag og retspraksis fra de kontrolorganer, der er etableret i medfør af de menneskeretlige konventioner samt fortolkningsbidrag og diskussioner i den juridiske litteratur kan dog bidrage til væsentlig og yderligere forståelse af beskyttelsens udstrækning.

På baggrund af afgørelser, anbefalinger og retlige analyser, kan der opstilles fire kategorier, som må anses at være dækket af den menneskeretlige privatlivs-beskyttelse:

Den første kategori dækker den ***fysiske integritet.*** Det vil sige at personen selv eller vedkommendes krop skal respekteres og beskyttes mod overgreb. Forhold der udgør en del af kroppen - som fx udseende - eller knytter sig til kroppen - så som påklædning - nyder også privatlivsbeskyttelse.

Den næste kategori omfatter den sfære, der formes af vores ***adfærd.*** Beskyttelsen dækker her vores familieliv og seksualliv eller øvrige sociale liv, herunder hvem vi interagerer og kommunikerer med, men også hvilke præferencer og vaner vi har og den måde, de kommer til udtryk på.

I den tredje kategori, ser vi beskyttelse af de ***materielle ting***, vi omgiver os med eller gør brug af. Det kan være vores hus, bil eller de kommunikationsmidler, som vi anvender. Denne beskyttelse knytter sig især til retten til at være i fred på et bestemt sted.

Den fjerde kategori omfatter ***oplysninger*** om de forhold, som er dækket af de tre øvrige kategorier, dvs. oplysninger, der relaterer sig til kroppen, til adfærden og til bestemte steder eller ejendele. Beskyttelsen omfatter såvel indsamling som opbevaring og behandling af person-oplysninger. Denne form for *information privacy* er på grund af den teknologiske udvikling måske den vigtigste at være opmærksom på i relation til overvågning.

### 2.3. Privatlivsbeskyttelse og overvågning

I forbindelse med efterretningsvirksomhed er det især beskyttelsen af oplysninger om borgernes adfærd, der er relevant.

Aflytning af telefonsamtaler, rumaflytning, tapning af elektronisk kommunikation, herunder dekryptering af krypteret kommunikation, registrering af tele- og datakommunikation, brevåbning, overvågning og observation i det private og offentlige rum ved hjælp af teknologi eller person er alle midler, der kan anvendes til at indsamle oplysninger om bestemte personers adfærd.

Også privatlivsbeskyttelsen af materielle ting er vigtig. Den vil fx være relevant i tilfælde, hvor ransagning og beslaglæggelse er nødvendige midler til at forfølge et efterretningsmæssigt formål.

Uden at have konkret kendskab til de efterforskningsmidler, som den danske efterretningstjeneste anvender, er det mit indtryk, at hovedparten heraf – måske endda alle relevante efterforskningsmidler – griber ind i den privatlivsbeskyttelse, som den enkelte borger kan påberåbe sig i kraft af menneskeretten og delvis også af Grundloven.

## 3. Statens interesse i at gøre indgreb i privatlivsbeskyttelsen

### 3.1. Indgrebsbetingelserne

Stort set ingen menneskerettigheder er absolutte i deres beskyttelse af borgeren. Statens interesse i at tage hensyn til samfundet som helhed kan således under særlige omstændigheder tillægges mere vægt end den enkelte borgers – og dermed føre til et indgreb fra statens side i en beskyttet rettighed. Beskyttelsen af privatlivet er et eksempel på en sådan relativt formuleret rettighed, dvs. en rettighed med indgrebs-mulighed.

Et indgreb i en menneskerettighed er et brud på det overordnede princip om, at borgerens beskyttelse er udgangspunktet. Denne prioritering ses tydeligst i den Europæiske Menneske-rettighedskonventions art. 8, hvor beskyttelsesområdet er fastlagt i stk. 1, mens indgrebs-muligheden er nævnt i stk. 2 som en undtagelses-bestemmelse.

Der er i menneskeretten opstillet en række betingelser, som skal være opfyldt før et indgreb kan anses for legitimeret - og dermed gennemføres i praksis i en konkret sag. Betingelserne er anført i art. 8, stk. 2 i den Europæiske Menneskerettigheds-konvention:

- lovhjemmel
- lovligt hensyn
- nødvendighed

Den første betingelse er tilstedeværelse af lovhjemmel og betyder, at national lovgivning skal indeholde en bestemmelse, der hjemler adgang til at foretage indgreb. De bestemmelser, der findes i den danske retsplejelov om aflytning, ransagning, beslaglæggelse og legemsindgreb kan derfor danne grundlag for at foretage indgreb i privatlivsbeskyttelsen.

Den anden betingelse er, at der skal kunne påpeges et lovligt hensyn. De lovlige hensyn, som kan påberåbes i relation til indgreb i privatlivsbeskyttelsen, omfatter bl.a.

- den nationale sikkerhed
- den offentlige tryghed
- landets økonomiske velfærd
- forebyggelse af uro eller forbrydelse

I relation til efterretningsvirksomhed burde det være selvfølgeligt, at disse lovlige hensyn – enten hver for sig eller til sammen – kan fastslås som værende tilstede i forbindelse med overvågning, der krænker privatlivsbeskyttelsen.

Den tredje betingelse, der skal opfyldes, er kravet om nødvendighed i et demokratisk samfund. Via nødvendighedskravet søges det sikret, at der består en rimelig balance i afvejningen mellem borger- og samfundsinteresse. Derudover følger det af nødvendighedskravet, at et indgrebs begrundelse skal findes i et påtrængende samfundsmæssigt behov.

Undersøgelsen af om nødvendighedskravet er opfyldt skal suppleres af en proportionalitets-vurdering. Denne vurdering skal skabe sikkerhed for, at indgreb foretages med et middel, der må anses for proportionalt i forhold til målet, dvs. at midlet skal stå i et rimeligt forhold til det angivne mål, og tillige som det mindre indgribende i sammenligning med en række mulige mere indgribende alternativer. Derudover følger det af proportionalitetskravet, at begrundelsen for indgrebet skal være relevant og dækkende.

De tre indgrebsbetingelser skal være opfyldt på to niveauer – et generelt og et konkret.

Det generelle niveau refererer til selve lovhjemlen. I forbindelse med vedtagelse af lovgivning, der hjemler adgang til indgreb i en menneskerettighed, er det således nødvendigt at påse, at indgrebet kun kan iværksættes for at imødekomme et lovligt hensyn og at det på et abstrakt plan må anses for nødvendigt i et demokratisk samfund. Fx må det generelt anses for nødvendigt, at politi og efterretningsvæsen har adgang til en række anvendelige og effektive efterforskningsmidler som led i forebyggelsen af forbrydelser.

Opfyldelsen på det konkrete niveau er aktuel, når en lovbestemmelse, der hjemler indgreb i en menneskerettighed, bringes i anvendelse i en konkret sag. I sådanne tilfælde må det igen undersøges, om indgrebsbetingelserne er opfyldt. Her spiller det en væsentlig rolle, om det kan godtgøres, at indgrebet er proportionalt. I det konkrete tilfælde skal indgrebet således fremstå som det mindre indgribende middel, der med rimelighed kan bringes i anvendelse under de konkrete omstændigheder.

### 3.2. Statens interesse i overvågning med et efterretningssigte

Staten har en samfundsmæssig interesse i effektivt at beskytte landet mod kriminalitet, terrorisme og andre angreb på samfundet og den offentlige orden. Hertil kan bl.a. efterretningsvirksomhed være et egnet og nødvendigt middel.

Når overvågning bringes i anvendelse i efterretningsøjemed, skal der foretages en afvejning af borgerens interesse i egen privatlivsbeskyttelse og statens interesse i at hindre konkret misbrug af efterforskningsmæssige beføjelser vis-a-vis effektiv efterretningsvirksomhed og den bagvedliggende interesse i beskyttelse af landet som helhed.

Overvågning giver - som det er fremgået ovenfor – i sig selv anledning til indgreb i privatlivs-beskyttelsen og et deraf følgende krav om opfyldelse af en række indgrebs-betingelser, der kan legitimere indgrebet.

Hvis anvendelsen af overvågning som efterforskningsmiddel har et efterretnings-mæssigt sigte, er det et iboende problem, at efterretningsvirksomhed typisk vil kræve hemmeligholdelse - både under et indgreb og efterfølgende - for at undgå at efterretningsformålet forspildes.

Dette behov for hemmeligholdelse giver anledning til en række yderligere problemer, der fx kan medføre et skærpet proportionalitetskrav. Dette vil være tilfældet i situationer, hvor overvågningen foregår uden den overvågedes vidende eller uden at vedkommende efterfølgende underrettes om en gennemført overvågning.

### 3.3. Hemmelig overvågning og underretningskravet

Den Europæiske Menneskerettighedsdomstol i Strasbourg har haft lejlighed til at bedømme sager, hvori der er foretaget indgreb i privatlivsbeskyttelsen i form af hemmelig efterforskning af hensyn til statens sikkerhed.

Af disse sager kan udledes, at et af de menneskeretlige krav, som normalt må stilles i forbindelse med brug af efterforskningsmidler uden den efterforskedes vidende, er en – i forhold til indgrebet – efterfølgende underretning. Dette skal fx ske ved hemmelig aflytning og antagelig også ved hemmeligransagning.

Underretningskravet i tilknytning til et hemmeligt foretaget indgreb skal ses som udtryk for to af menneskerettens beskyttelsesgarantier, nemlig proportionalitets-kravet og adgang til efterprøvelse.

Menneskerettens krav om proportionalitet må i denne sammenhæng anses for skærpet.

Baggrunden herfor er, at der vil være en øget risiko for misbrug af overvågning, når hemmeligholdelse gennemføres konsekvent. Domstolen har således udtalt i en sag om afskærelse af domstolsprøvelse af indgreb i meddelelseshemmeligheden, at der er grænser for, hvor langt myndigheder kan gå i bestræbelserne på at opklare forbrydelser. Der skal skabes sikkerhed for, at hemmelig overvågning begrænses til sager, hvor der foreligger særlige omstændigheder, og hvor det anses som værende strengt nødvendigt for at sikre demokratiske institutioner.

Kravet om adgang til domstolsprøvelse finder direkte udtryk i den Europæiske Menneskerettigheds-konventions art. 13, hvori det er fastslået, at

> ”Enhver, hvis rettigheder og friheder efter denne konvention er blevet krænket, skal have adgang til effektive retsmidler herimod for en national

myndighed, uanset om krænkelsen er begået af personer, der handler i embeds medfør".

På trods af disse skærpede betingelser i forbindelse med hemmelig overvågning er der eksempler fra retspraksis, der viser at underretningskravet i særlige tilfælde kan tilsidesættes.

De kontrolorganer, der er eller har været knyttet til den Europæiske Menneskerettighedskonvention, nemlig den Europæiske Menneskerettighedsdomstol og den nu nedlagte Europæiske Menneskerettighedskommission, har således accepteret at underretning ikke blev foretaget i sager, hvor hensynet til statens sikkerhed måtte anses at fortrænge hensynet til privatlivsbeskyttelsen.

Det er indlysende, at borgeren i forbindelse med efterretningsmæssig anvendelse af hemmelige efterforskningsmidler og beslutning om undladelse af efterfølgende underretning, bliver afskåret fra at få prøvet indgrebets lovlighed ved domstolene. For at begrænse misbrug, er det derfor af afgørende betydning, at der etableres en form for effektiv demokratisk kontrol med de hemmelige overvågningsmidler og metoder, som anvendes med et efterretningssigte.

### 3.4. Overskudsinformation

I forbindelse med anvendelse af overvågningsteknikker i efterretningsmæssigt øjemed kan det ikke undgås, at en overvågning bibringer efterretningstjenesten oplysninger om forhold, som omfatter mere end det, der er relevant og nødvendigt for at opfylde formålet med overvågningen. Det kan dreje sig om vaner og præferencer i forhold til nærings- og nydelsesmidler, forbrugsgoder, fritidsbeskæftigelse eller seksualitet, men også om andre sociale og familiemæssige forhold, helbredsmæssige eller økonomiske forhold.

Sådan overskydende og irrelevant information er omfattet af privatlivsbeskyttelsen i den forstand, at den ikke må opbevares og anvendes. I praksis vil det sige, at overskudsinformation ikke må registreres og opbevares i en sag, der behandles af efterretningstjenesten. Det kan måske være vanskeligt at håndtere et sådant krav i dagligdagen, idet relevant og irrelevant information nok typisk vil være viklet sammen. En praktisk regel kan derfor være, at man sørger for at destruere overskudsinformation straks det står klart, at det ikke kan anses at ligge indenfor det formål, man forfølger med overvågningen.

## 4. Afsluttende bemærkninger

Uanset hvordan den overvågning, som foregår med et efterretningssigte tilrettelægges, er det vigtigt at være opmærksom på borgerens privatlivsbeskyttelse. Både i forbindelse med selve overvågningen og ved efterfølgende behandling og anvendelse af det materiale, som overvågningen har frembragt, er det nødvendigt at påse, at de indgrebsbetingelser, som er formuleret i menneskeretten, overholdes. Det forhold, at

overvågning iværksættes med det formål at sikre den nationale sikkerhed, kan således ikke i selv legitimere, at der foretages indgreb i en borgers privatliv. Afgørende er, at indgrebet i det konkrete tilfælde tillige kan anses for nødvendigt og proportionalt.

## Overvågning i efterretningssammenhænge

*Af Peter Christensen, CNDO*

Overvågning/aflytning skal i dag ske via en dommerkendelse byggende på indicier om en væsentlig forbrydelse eller det kan ske på Forsvarets område og dermed ikke reguleret af civil lovgivning.

**Kollektiv overvågning**

EU's STOA-rapport fra '99 om signal-opsamling fremlagde stærke indicier for, at der eksisterede et amerikansk baseret overvågningssystem ved navn Echelon, som scannede og sammenkædede sattelit-kommunikation opsamlet fra store dele af jordkloden. Dette system er drevet af NSA og skulle enten omfatte eller være suppleret med funktioner, der via en mønstergenkendelse af fraser kunne fremfinde elektroniske tekster i kommunikationen vedrørende disse fraser. Ifølge rapporten skulle systemet primært efter koldkrigstiden være blevet brugt til efterretninger om den civile industri. Siden er denne beskrivelse blevet bekræftet fra mange sider f.eks. tidligere CIA-ansat Richelson trods en officiel afvisning af tilstedeværelsen af dette system: Echelon.

Tidligere CIA-chef  Wolsey udtrykte det i en udtalelse, at denne aflytning af den civile elektroniske kommunikation reelt var begrundet i den europæiske industris anvendelse af bestikkelse i deres forsøg på at vinde opgaver. Straks efter denne udtalelse fastslog USA's regering overfor EU-kommissionen, at der ikke var noget grundlag for denne og andre udtalelser om eksistensen af et sådant system. Dette skete netop op til EU-parlamentets behandling af den oprindelige STOA-rapport og kravet om nedsættelse af en særlig komité til at afdække problemet.

Denne komité har for nyligt afleveret en rapport, der præciserer dette aflytningssystems tilstedeværelse og mere pinligt: UK's aktive deltagelse i dette. STOA- og komité-rapporten påpeger dog også, at flere andre lande som f.eks. Frankrig, Rusland og Kina har forsøgt sig med opstillingen af tilsvarende systemer dog uden samme geografiske dækningsgrad som Echelon.

Rapportens konklusioner er, at Echelon principielt er ulovligt, at EU-lande ikke bør deltage og at EU burde sikre sig USA's accept af, at systemet ikke blev brugt mod EU-lande. Desuden foreskriver rapporten som det eneste middel mod systemet: krypteringsværktøjer og lægger op til udviklingen af et europæisk, open source-baseret værktøj.

**Kryptering mod overvågning**

Denne overvågning/aflytning af den civile kommunikation er naturligvis i strid med al lovgivning på området; men omvendt meget svær at retsforfølge, da det er en ikke-civil og international myndighed, der står bag civil aflytning. Med eksistensen af en lytte-station på Amager er der stærke indicier for, at Danmark bidrager med

oplysninger til Echelon som et af de få lande, der ikke er medlem af den engelsk-baserede gruppe: USA, UK, Australien og New Zealand.

Reaktionen er derfor, at anvende kryptering ved kommunikation, der kan forventes overvåget. I forvejen er kryptering mere og mere almindelig på Internettet for at undgå at bankoplysninger, persondata m.m. kan opsnappes og desuden medfører kryptering ifm. Internethandel, at man indirekte får foræret en entydig identifikation af køber, da en personlig nøgle indgår som en af flere faktorer i krypterings-algoritmen.

Situationen med en stigende anvendelse af kryptering ser ud til at være forudset fra amerikansk side og man oplever en nærmest  koordineret indsats for at sikre bagdøre i mange amerikanske software-produkter – bagdøre, der skal kunne gøre det nemmere at identificere og dekryptere en given brugers kommunikation. Dette er specielt kommet frem omkring Microsofts og IBM's Office-produkter, mens Sun meget offensivt direkte sælger budskabet om det ikke-eksisterende privatliv som en konsekvens af IT-udviklingen(deres produkter?).

**Kryptering er svaret**
Echelon er et system, der principielt undergraver den nationale lovgivnings krav om en retsregulering af alle brud på brevhemmeligheden. Det ser desværre ikke ud til at det internationale samfund vil, kan eller for den sags skyld ønsker at ændre på dette.

Den enkelte borger kan derfor kun beskytte sig mod denne overvågning ved at kryptere sine e-mails. Samfundet bør således stille de værktøjer til rådighed, der gør det muligt for den enkelte borger at kunne vælge retten til at bevare brevhemmeligheden. Som ovenstående viser er dette i sig selv ikke blot en kompliceret proces; men kræver også udvikling af værktøjer, hvis indhold kun er reguleret efter ønsket om af beskytte afsender og modtager samt deres fælles kommunikation.

**Uddybning**
Privatliv: http://www.privatliv.net
Echelon Watch: http://www.echelonwatch.org
EPIC: http://www.epic.org
Cyber Rights: http://www.cyber-rights.org
Kommissionsrapport: http://www2.europarl.eu.int/omk/OM-Europarl?PROG=REPORT&L=EN&PUBREF=-//EP//TEXT+REPORT+A5-2001-0264+0+NOT+SGML+V0//EN&LEVEL=2

## Arbejdsgivernes brug af overvågning

*Af ansættelsesretschef, advokat Laurits Rønn, Dansk Handel & Service.*

Med den rivende teknologiske udvikling samfundet er midt i og med de deraf flydende muligheder for overvågning, er det meget forståeligt at, tanken om overvågning optager mange mennesker. Overvågning findes i mange varianter, men fokus i denne sammenhæng vil være overvågning på arbejdspladser i form af videoovervågning samt kontrol med e-mail og internet-brug.

Først og fremmest er det meget relevant at vide, hvorfor en arbejdsgiver i det hele taget vælger at tage skridtet til at etablere overvågning på arbejdspladsen.

Det er fra flere sider – herunder fra arbejdstagerorganisationers - blevet anført, at overvågning skaber utryghed og mistænkeliggørelse af medarbejderne, og således er noget virksomhederne skal afholde sig fra. Her er det dog vigtigt at holde sig for øje, at medarbejderen er virksomhedens vigtigste ressource. Hvilken interesse har arbejdsgiveren i at skabe utryghed eller genere medarbejderen? Ingen. Arbejdsgiverne føler ikke nogen glæde ved at etablere overvågning af virksomheden, men gør det alene for at sikre sig selv mod uregelmæssigheder og for at sikre medarbejderen. Med hensyn til e-mail og internetbrug sker kontrol heraf for at sikre virksomhedens informationsflow, IT og systemernes driftsikkerhed samt for sikre at misbrug ikke finder sted.

Det er forståeligt, at de fleste umiddelbart ikke bryder sig om at blive overvåget. Derfor skal indførelsen af overvågningen ske i åbenhed og i dialog med medarbejderne. Der skal ikke være utryghed. Dette skal arbejdsgiverne bidrage til at sikre. Utryghed kan netop komme til livs ved. at der er klarhed over, hvorfor der indføres overvågning, og under hvilke omstændigheder den indføres. Udover naturligvis at overholde gældende lovgivning skal arbejdsgiveren fastsætte retningslinier for kontrollen, og det skal sikres, at medarbejderne kender disse retningslinier. Åbenhed og motivation skaber tryghed og eliminerer utrygheden.

### Videoovervågning

Overvågning af arbejdspladsen ved hjælp af TV eller video anvendes primært i detailhandelen, hvor man har et betydeligt svind – anslået til minimum 3 mia. kr. pr. år. Der er tale om kundetyveri og medarbejdertyveri samt svind i øvrigt. Detail-handelen er derfor nødsaget til at iværksætte nogle kontrolforanstaltninger, herunder videoovervågning for at mindske svindet.

Er der svind i en forretning, er det også ubehageligt for medarbejderen. Uregel-mæssighederne består overvejende i, at der sker kundetyverier. Disse tyverier er medarbejderne lige så interesserede i at få opklaret, som arbejdsgiveren er. Medarbejderne opfatter også kameraer som en lettelse, fordi de ikke skal bruge deres

tid på at holde øje med kunderne, og undgår at skulle konfrontere kunder der har stjålet.

Det er også vigtigt at fremhæve det sikkerhedsmæssige aspekt. Det giver medarbejderne en tryghed at vide, at der overvåges, især hvis man arbejder om aftenen eller natten. Der vil ske færre røverier med deraf følgende sikkerhed for medarbejderne.

Kameraerne opstilles således for at sikre virksomhedens værdier og sikre medarbejderen mod risikoen for at blive udsat for vold. Opsætningen har et forebyggende, opklarende, sagligt og driftsmæssigt formål. Det er ikke nogen hemmelighed, at arbejdsgiverne hellere var overvågningen foruden, for det er ikke nogen fornøjelse af overvåge kunder eller medarbejdere, men man er på den anden side nødsaget til at sikre sig mod tyveri.

Tv-overvågning kan ske i selve forretningslokaler, hvortil der er almindelig adgang for alle mennesker. Der er faste regler for tv-overvågningen af forretninger. Man skal skilte med det, så kunderne kan se, at de nu går ind i en forretning med overvågning. Også medarbejderne skal vide, at der overvåges i området. Den tv-overvågning der foretages sker i ganske overvejende grad i de områder hvortil der er almindelig adgang. Forsvinder der ting for eksempel fra et butikslokale, kan det være kunderne, der har taget tingene, men det kan også være personalet.

Tv-overvågning kan også ske i områder, hvor der ikke er almindelig adgang til. Det kan være lageret eller kantinen. Forsvinder der ting herfra, kan gerningsmanden kun findes blandt dem, der har adgang til området; personalet, eller dem der uretmæssigt trænger ind i området. Reglerne i Lov om privates tv-overvågning er således, at der skal skiltes eller på anden måde oplyses for medarbejderne, hvis der overvåges på områder, der ikke er almindelig adgang til. Det kan for eksempel være lageret. Den eneste mulighed for overvågning uden skiltning, er, hvis det sker som led i en strafferetlig efterforskning.

Det hører til blandt sjældenhederne at overvåge de områder, som kun personalet har adgang til. Og det er meget sjældent, at overvågningen bevidst rettes mod de ansatte i forretningslokalet med henblik på overvågningen af disse. Det sker, hvis der er en begrundet mistanket om tyveri. Her har overvågningen et opklarende formål og er med til at rense de uskyldige medarbejder.

Det er vigtigt at understrege, at videoovervågning skal være sagligt begrundet og have et driftsmæssigt formål. Går en arbejdsgiver for vidt, kan den eller de berørte medarbejdere få foranstaltningen prøvet i det fagretlige system ligesom virksomheden kan ifalde bødestraf ved overtrædelse af loven. Der er ingen der har en interesse i at holde hånden over arbejdsgivere, der ikke overholder loven.

**Kontrol med e-mail og internetbrug**
I de seneste år er der sket en eksplosiv vækst i anvendelsen af moderne informationsteknologi (IT) på virksomhederne. Elektronisk post (e-mail) og anvendelse af internettet har efterhånden vundet indpas i de fleste virksomheder.

Medarbejdernes adgang til e-mail og internettet giver dog også anledning til problemer hos virksomhederne, hvilket har skabt et behov for fastsættelse af retningslinier herfor. For at sikre såvel arbejdsgiverens som medarbejdernes interesser anbefaler Dansk Handel & Service, at der på virksomheden udarbejdes retningslinier for medarbejdernes brug af e-mail og internettet. Sådanne retningslinier har som deres primære formål at sikre driften af virksomheden og har ikke som umiddelbart mål at kontrollere medarbejderen alene for kontrollens skyld.

I det følgende redegøres der kort for de problemstillinger der er relevante i denne henseende.

- Filer, der downloades fra internettet, eller som vedhæftes en e-mail kan indeholde virus, ligesom der kan hentes eller vedhæftes filer, der lægger beslag på en meget stor del af virksomhedens IT-kapacitet. En virus på netværket kan meget vel resultere i systemnedbrud, der betyder tab af arbejdsdage og informationer. Derfor er det hensigtsmæssigt at fastlægge retningslinier for tilladte størrelser af på ind- og udgående e-mail. For at sikre at virksomhedens IT-kapacitet er tilstrækkelig, kan der fastsættes en maksimal tilladt størrelse på ind- og udgående e-mail.
- Filer der hentes fra internettet eller som modtages pr. e-mail, kan indeholde billed- og lydmateriale og programmer, der er beskyttet af tredjemands ophavsrettigheder. Beskyttet materiale og programmer må kun kopieres/ installeres efter aftale med rettighedsindehaveren. I praksis betyder det, at materialet/programmet skal købes igennem kanaler, der sikrer rettighedsindehaverens vederlagskrav. Kopieres, installeres eller placeres ulovligt materiale på en af virksomhedens computere risikerer virksomheden, dels at pådrage sig et erstatningsansvar over for rettighedsindehaveren, dels at ifalde bødestraf. Derfor skal tredjemands ophavsrettigheder respekteres og dette kan sikres gennem retningslinier udarbejdet af virksomheden. Virksomheden kan i denne sammenhæng have behov for med jævne mellemrum at kontrollere, at der ikke findes ulovlige kopier og installationer.
- Efterhånden er det blevet almindeligt, at virksomheder tager stilling til samfundsmæssige eller etiske spørgsmål og samtidig ønsker at sende klare signaler om denne stillingtagen såvel internt i virksomheden som i forhold til omverdenen. For sådanne virksomheder vil det være særligt generende eller ligefrem skadeligt, hvis virksomhedens medarbejdere opsøger hjemmesider eller via e-mail udvekslede personlige opfattelser eller vittigheder af indhold, der strider mod virksomhedens værdigrundlag. Men også virksomheder, der ikke aktivt har taget stilling til eller formuleret et værdigrundlag vil typisk ønske at

medarbejderne, når de færdes på internettet alene opsøger de seriøse og sobre hjemmesider og undgår eksempelvis hjemmesider med et pornografisk indhold, politisk ekstremistisk eller diskriminerende karakter. Tilsvarende ønsker virksomheden typisk ikke, at medarbejderen ved brug af e-mail sender materiale af ovennævnte karakter.

- Ikke al elektronisk kommunikation på virksomheden er arbejdsrelateret. De fleste virksomheder stiller også e-mail og internetadgang til rådighed for medarbejderne til privat brug. Adgangen til brug af e-mail og internettet giver derfor en risiko for uforholdsmæssig brug af privat karakter. Arbejdsgiver har derfor et behov for at kontrollere, at de teknologiske muligheder ikke misbruges.
- Driften af virksomheden sker i stigende omfang via korrespondance over e-mail og internettet. Såfremt en medarbejder er fraværende fra virksomheden i en periode, eksempelvis pga. sygdom eller ferie, kan dette betyde, at vigtige meddelelser ikke bliver besvaret, at opgaver ikke bliver løst og at aftaler ikke bliver overholdt. Arbejdsgiver har også i disse tilfælde behov for adgang til medarbejdernes elektroniske kommunikation af driftsmæssige årsager.

Ovenstående overvejelser er baggrunden for at Dansk Handel & Service anbefaler, at man i virksomhederne fastsætter retningslinier for medarbejdernes brug af e-mail og internettet og orienterer om kontrollen heraf.

Det er problematisk ikke at have retningslinier. Manglende retningslinier kan give konflikter om virksomhedens ret til at åbne og/eller læse medarbejderens e-mail – f.eks. i forbindelse med fravær og ferie – og det kan være vanskeligt uden retningslinier at gribe ind over for en uhensigtsmæssig brug af e-mail og internettet. Tilsvarende kan det hæmme muligheden for hurtigt at komme et virusangreb til livs, såfremt virksomheden ikke må åbne alle de e-mails, der er tilgået virksomhedens server.

Dansk Handel & Service oplever, at virksomhederne anvender kontrol af e-mail og internetbrug af hensyn til IT-sikkerheden og driftsikkerheden, og for at forhindre misbrug. Der er ikke tale om kontrol for kontrollens skyld.

**Gældende lovgivning.**
Der er ikke frit spil med hensyn til at etablere kontrolforanstaltninger - herunder overvågning samt kontrol med e-mail og internetbrug.

- Lov om privates tv-overvågninger stiller som nævnt tidligere krav om skiltning bortset fra strafferetlig efterforskning.
- Lov om behandling af personoplysninger regulerer virksomhedens adgang til indsamling og registrering af oplysninger om medarbejderens brug af e-mail og færden på internettet.
- Straffeloven har bestemmelser om brevhemmeligheden.

- Med virkning fra den 15. maj i år udvidede DA og LO Hovedaftalen til også at regulere kontrolforanstaltninger. Aftalen kodificerer en arbejdsretlig praksis. Aftalen regulerer kontrolforanstaltninger i bred forstand – herunder både videoovervågning og kontrol af e-mail og internetbrug, og fokuserer netop på afvejningen af hensynene til såvel medarbejderens som virksomhedens interesser i forbindelse med indførelsen af kontrolforanstaltninger.
  Foruden, at kontrolforanstaltningen skal have et fornuftigt og sagligt formål, ikke må gå længere end påkrævet og ikke må være krænkende, så er det nu klart blevet aftalt, at medarbejderne skal informeres senest 2 uger før der iværksættes en kontrolforanstaltning. Dette er en glimrende lejlighed til at få gennemdrøftet, hvorfor det er nødvendigt at tage skridtet til kontrolforanstaltningen. Det er faktisk oplevet, at den blotte orientering om en påtænkt overvågning betyder at svindtallene retter sig.
  Arbejdsmarkedets parter er i øvrigt enige om at der er en god aftale, og at der ikke er brug for yderligere regler på området.

**Afslutning**
På baggrund af ovenstående mener Dansk Handel & Service, at adgangen til overvågning på arbejdspladsen er gennemreguleret af lovgivning og aftaler mellem arbejdsmarkedets parter, hvorfor der ikke er behov for yderligere tiltag.

Det bliver fra flere anført, at der forekommer et voldsomt misbrug af kontrol-foranstaltninger, og at der ude på arbejdspladserne skulle være udbredt utryghed ved det. Dansk Handel & Service organiserer en betydelig del af dansk erhvervsliv, og vi har ikke det samme indtryk.
Vi har meget få sager på dette område og betragter ikke overvågning på arbejdspladsen som et problem.

## Overvågning på arbejdspladsen

*Af Bjarne Petersen, faglig sekretær i HK/HANDEL*

Begrebet overvågning - i denne forbindelse **tv-overvågning** - er i danskernes bevidsthed ændret fundamentalt i løbet af de sidste 20 år.

Tragedien i USA d. 11. september 2001 har utvivlsomt rokket yderligere ved holdningen til overvågningssystemernes anvendelsesmuligheder og berettigelse.

Den teknologiske udvikling har ført et utal af overvågningsmuligheder med sig. Nogle betegnes som udelukkende positive – andre som direkte negative. Afhængigt af, hvem man spørger. Og afhængigt af, hvilke oplevelser man har haft med overvågningssystemerne.

Set i historisk perspektiv, havde vi i Danmark den første reelle diskussion om privates anvendelse af tv-overvågning i 1981. Årsagen til drøftelserne dengang, var opsætningen af et antal tv-overvågningskameraer i et butikscenter i Holstebro.

Diskussionerne og "billederne" af, hvad overvågning reelt indebar af begrænsninger i det enkelte individs samlede frihedsrettigheder, havde hidtil været baseret på George Orwells skræmmende beskrivelse af Big Brother samfundet i romanen "1984" samt andre tilsvarende "fantasibeskrivelser". Med ét blev "fantasibeskrivelserne" indhentet af virkeligheden. Befolkningens reaktion var ikke til at tage fejl af; man var skræmt. Folketinget tog affære og vedtog den første lov om forbud mod privates anvendelse af tv-overvågning.

Befolkningen blev beroliget, og som det så ofte går, har udviklingen derefter nærmest fået karakter af at være naturgiven, hvor kun få stiller spørgsmål ved udbredelsen af overvågningskameraerne såvel som ved udvidelsen af kameraernes tekniske formåen.

Tv-overvågning i dagens Danmark er helt, helt anderledes fra den tv-overvågning, som Folketinget lovgav om i 1981 og for den sags skyld også fra den lovgivning folketinget vedtog i 1998.

I virkeligheden er vi – grundet ovennævnte næsten stiltiende accept af udviklingen – i dag tættere på Georg Orwells Big Brother samfund, end vi vil acceptere, hvis vi stiller de frihedsrettigheder, vi værdsætter, op overfor de indgreb i samme friheds-rettigheder, som tv-overvågningen har "fået lov" til at berøve os i al ubemærkethed.

I det efterfølgende er i opremsningsform beskrevet eksempler på områder på det danske arbejdsmarked, hvor tv-overvågning – eller kontrolforanstaltninger, der kan sammenlignes med tv-overvågning – er blevet indført, uden det har ført til diskussioner, om hvilke konsekvenser indførelsen ville medføre i relation til

beskyttelsen af privatlivets fred såvel som beskyttelse af ytrings-, forsamlings- og foreningsfrihed.

- Banker og posthuse
- Kiosker, servicestationer og bagerbutikker
- Dagligvarebutikker
- Stormagasiner og lavprisvarehuse
- Guld- og sølvsmedebutikker
- Specialvarebutikker
- Busser i rutefart
- Speditionskørsel
- Skibsfart
- Postudbringning
- Ældrepleje
- Børneinstitutioner
- Kriminalforsorgen
- Bistandskontorer
- Fartkontrol

Kendetegnende for samtlige de områder, hvor anvendelse af overvågningssystemer i dag bliver anvendt er, at det i næsten alle tilfælde altid er de **"positive"** muligheder, der bliver fremhævet i forbindelse med indførelsen af overvågningen, hvorimod de **"negative"** konsekvenser, udelukkende fremføres af mennesker, der – ofte ved et tilfælde – har konstateret sig selv optaget i uventede situationer.

De personer, der har en udelukkende **"positiv"** tilgang til anvendelse af tv-overvågning, ser alene anvendelsen som en **forebyggende og tryghedsskabende** foranstaltning, hvorimod de **"negative"** personer, der har haft eller som forstiller sig ubehageligheder som følge af installeringen, føler en **utryghed og en stærk begrænsning i deres udfoldelsesmuligheder.**
Umiddelbart kan der med andre ord sættes lighedstegn mellem "positiv" og tryghed og mellem "negativ" og utryghed.

Det er imidlertid HK/HANDELs erfaring, at der desværre ofte skal en ubehagelig oplevelse til, før man reelt indser rækkevidden af overvågningen.

Ud fra samtaler med repræsentanter fra de øvrige anførte områder, kan det konstateres, at det tilsyneladende forholder sig på nøjagtig samme måde, indenfor andre områder af arbejdsmarkedet, hvor overvågning i en eller anden form og i større eller mindre udstrækning har fundet anvendelse indenfor de seneste år:

Hver gang en person, der er mistænkt for tyveri, bliver afsløret via f.eks. skjult kamera, lyder kommentaren fra dem, der alene føler sig trygge ved

overvågningssystemerne, at det var godt, at overvågningen førte til, at mistanken blev fjernet fra alle de uskyldige.

De samme uskyldige personer tænker tilsyneladende ikke på, hvor mange mere eller mindre pikante situationer de sideløbende med afsløringen er blevet indfanget i.

De kameraer, der benyttes til tv-overvågning har i den grad skiftet karakter og udseende fra dengang i begyndelsen af 80'erne, hvor Folketinget vedtog den første lov om forbud mod privates anvendelse af tv-overvågning.
Hvor kameraerne dengang, var så store og klodsede, at de nærmest var umulige ikke at se, er kameraerne i dag så små, at de nærmest er umulige at få øje på, med mindre man ved, hvor de er placeret.

Tilmed kan kameraerne i dag leveres i trådløs udgave, hvilket betyder, at man kan flytte rundt på kameraerne efter for godt befindende. Kameraerne kan tilmed "skjules" som en slipsenål eller en broche og derved fungere som transportabelt kamera ind og ud mellem folk.

Den lovbefalede skiltning om tv-overvågning, er reelt den eneste "modvægt", der findes til tv-overvågningen. Skiltekravet er lovgivernes tilbud til de ansatte - og kunderne – om at de selvfølgelig har krav på at vide, at de bliver tv-overvåget således, at de kan tilpasse deres adfærd herefter.

Lovgivernes ønske om således at hjælpe de ansatte – og kunderne – over det værst tænkelige scenarium; skjult overvågning, er i sig selv sympatisk, men udviklingen, såvel den teknologiske som den holdningsmæssige, har gjort skiltekravet i sin nuværende form illusorisk og efterlader derfor både de ansatte og kunderne i et tomrum af falsk tryghed.

Den største frygt for overvågning er frygten for den overvågning, der foregår skjult. Hvis der skiltes – evt. bare med et enkelt skilt på indgangsdøren til en butik – med det anerkendte tv-overvågningsskilt, kan butiksindehaveren i realiteten opsætte nok så mange små skjulte kameraer.

Der skal godt nok være overensstemmelse mellem skiltningen og overvågningen, hvilket vil sige, at der ikke må skiltes med, at der foregår tv-overvågning, hvis dette ikke reelt er tilfældet. Men reel oplysning til de ansatte om, hvor kameraerne præcist er placeret, er der derimod ikke krav om.

Dette faktum – sammenholdt med ovenstående oplysning om kameraernes minimale størrelse – gør det nærmest umuligt for de ansatte at tilpasse deres adfærd til kameraernes placering, hvilket fører til situationer, der af den enkelte opleves krænkende, hvis vedkommende ved et tilfælde opdager, at hun/han er blevet optaget på tv.

Det manglende krav om at de ansatte har krav på at vide, hvor kameraerne er placeret, kan – set i bakspejlet - tolkes som en tilladelse til arbejdsgiveren om at tv-overvåge de ansatte i det skjulte.

Udviklingen – den teknologiske såvel som den holdningsmæssige – har desuden ført til, at skjult aflytning, er blevet mere udbredt.

Det må således konstateres, at det i dag er meget udbredt, at anskaffe sig tv-overvågningsudstyr, der samtidig er forsynet med en mikrofon. Den indbyggede mikrofon gør det muligt at aflytte personalet og personalets samtaler indbyrdes såvel som med kunder.

Uanset at straffeloven forbyder aflytning, foregår dette altså sideløbende med den visuelle overvågning. Straffelovens bestemmelse om at aflytning kun må finde sted, dersom der er givet samtykke hertil, afholder tilsyneladende ikke et større og større antal arbejdsgivere fra at investere i udstyr med begge overvågningsmuligheder. "Samtykkebestemmelsen" i straffeloven, der i lighed med "skiltekravet" i "tv-overvågningsloven" er tænkt som en beskyttelse af den ansatte/borgeren, er i denne sammenhæng ligeledes illusorisk, idet det eksempelvis vil være tilstrækkeligt for en arbejdsgiver at indhente samtykke hos en af sine nærmeste medarbejdere – f.eks. en arbejdsleder – hvorefter aflytning af personalet vil være tilladt.

Den medarbejder, der via tv-overvågning bliver grebet i at foretage sig noget uregelmæssigt – eller den medarbejder, der via de(n) mikrofon(er), som er påmonteret overvågningsudstyret, udtaler sig på en måde, der ikke passer arbejdsgiveren, straffes sandsynligvis med bortvisning.

Den arbejdsgiver, der med et enkelt skilt på indgangsdøren til butikken, har lovmedhold til at opsætte et antal skjulte tv-overvågningskameraer med indbygget mikrofon, kan ikke straffes, fordi overvågningen – qua det ene skilt på indgangsdøren – ikke er skjult og fordi han via samtykke med sin arbejdsleder, har tilladelse til at aflytte sit personale.

Den manglende debat i forbindelse med de enkelte overvågningssystemers indtrængen i samfundet, burde give anledning til dybe panderynker.

De minimale overvågningskameraer, med eller uden ledning, men med mikrofon, der kan opsættes/iværksættes, hvor som helst i løbet af splitsekunder, har langt større konsekvenser for vort demokrati, end flertallet af danskere åbenbart er sig bevidst.

Man behøver ikke være udstyret med megen fantasi for at se Georg Orwells Big Brother samfund for sig.

Når jeg ovenfor påstår, at vi måske er tættere på Big Brother samfundet i dag, end vi var, da Folketinget i 1981 vedtog den første lov om forbud mod privates anvendelse af tv-overvågning, bygger jeg min påstand på de fakta om tv-overvågnings udbredelse og anvendelse, jeg i mit daglige virke i HK/HANDEL jævnligt bliver mindet om.

Såvel den visuelle som den auditive overvågning, som jeg har beskrevet ovenfor, og som bygger på utallige medlemshenvendelser, kombineret med den udbredte anvendelse af elektronisk post og internet, efterlader et billede af et demokrati med stolte traditioner, hvor den enkeltes privatlivsfred, såvel som de grundlovssikrede frihedsbegreber ytringsfriheden, foreningsfriheden samt forsamlingsfriheden i den grad trues, grundet en manglende debat om konsekvenserne af fortsat uhæmmet indførelse og accept af overvågnings- og kontrolforanstaltninger.

Den manglende debat, ikke alene skader demokratiet på kort sigt, men risikere på lidt længere sigt totalt at udhule den yngre generations opfattelse af hvilken værdi oven-nævnte frihedsrettigheder har for det enkelte individ og for at kunne virke og færdes i fællesskabet.

Tv-optagelser med skjult kamera har tillige fundet indpas på underholdningssiden og har på rekordtid flyttet sig fra de harmløse hjemmevideo-udsendelser som ”Ren kage mand” til Big Brother udsendelserne.

I lande – tæt på Danmark – hvor man ikke, som vi, er ”privatlivsbeskyttet”, er ”Ren kage Mand” udsendelserne allerede blevet afløst af udsendelser med klip fra arbejdspladser, hvor ansatte i virkelig krænkende og nærgående situationer udstilles.

Optagelser fra danske arbejdspladser – optaget helt i strid med al anstændighed, moral og lovgivning - er åbenbart blevet en ”eksportvare”, idet man ofte på bl.a. tysk tv kan se ”dumme dänen” i situationer, der herhjemme kunne føre til retsforfølgelse, hvis den krænkede i øvrigt havde psykisk overskud hertil.

Det er kendetegnende for utallige af de henvendelser, HK/HANDEL modtager, at medlemmerne ofte føler sig så krænket, at de dels har det psykisk dårligt dels totalt mangler overskud til at føre en sag imod den, der har krænket dem.

# Overvågning på arbejdspladser

*Af Janne Glæsel, advokat, Næstformand for Datarådet*

## 1. Indledning

Persondataloven gælder for behandling af personoplysninger, som helt eller delvist foretages ved hjælp af elektronisk databehandling og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Loven gælder tillige for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden.

Sagsbehandling, der foregår på papirbaseret måde, således at oplysninger, dokumenter og andre sagsakter håndteres uden anvendelse af edb, vil ikke være omfattet af lovens almindelige anvendelsesområde. Betydningen heraf er bl.a., at så længe sagsbehandlingen i den offentlige forvaltning foregår på denne måde, vil alene forvaltningslovens regler og reglerne om god forvaltningsskik skulle iagttages.

I det følgende forudsættes det om de omtalte personoplysninger om medarbejdere i organisationer, at der er tale om hel eller delvis behandling ved hjælp af elektronisk databehandling eller om ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

I de følgende afsnit forudsættes det endvidere, at de generelle behandlingsregler er fulgt, herunder at indsamling og behandling sker i henhold til et sagligt formål. Organisationerne må løbende vurdere, om formålet er sagligt, idet behandlingsbegrebet omfatter opbevaring af personoplysninger.

En organisations personaleafdeling beskæftiger sig med mennesker, og det er derfor indlysende, at behandling af personoplysninger indgår i det daglige arbejde, og at personaleafdelingen er i besiddelse af et kartotek og/eller en database (registre) med oplysninger om organisationens ansatte.

Personoplysninger kan grundlæggende inddeles i to hovedgrupper:

Følsomme oplysninger, der omfatter oplysninger om etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsmæssige og seksuelle forhold samt oplysninger om strafbare forhold, væsentlige sociale problemer eller andre rent private forhold. Rent private forhold kan bl.a. omfatte oplysninger om selvmordsforsøg, personlighedstests, bortvisning etc.

Personoplysninger, der ikke falder ind under ovennævnte kategori, kan samles benævnes *almindelige oplysninger* eller *ikke-følsomme oplysninger*. Disse oplysninger udgøres fx af generelle oplysninger i form af navn, billede, adresse, telefon- , telefax- og mobiltelefonnummer, stilling, køn, produkt-præferencer og lignende.

Behandling af følsomme oplysninger kræver som altovervejende hovedregel, at den registrerede giver sit udtrykkelige samtykke til behandlingen. Ikke-følsomme oplysninger vil ud fra et interesseafvejningssynspunkt som udgangs-punkt kunne registreres uden samtykke af en arbejdsgiver.

I relation til sondringen mellem følsomme og almindelige oplysninger er Datatilsynet af den opfattelse, at følgende personaleoplysninger falder i kategorien *almindelige* personoplysninger:

(i) Identifikationsoplysninger, såsom medarbejderens navn, adresse og telefonnummer.
(ii) Fødselsdato.
(iii) Nær familie.
(iv) Oplysninger om uddannelse, udtalelser, tidligere beskæftigelse, nuværende stilling, arbejdsopgaver, arbejdstider og andre tjenstlige forhold.
(v) Oplysninger om andet fravær fra arbejdet.
(vi) Oplysninger om pensionsforhold.
(vii) Kildeskatteoplysninger.
(viii) Oplysninger om kontonummer, hvortil lønnen skal anvises.

Følgende oplysninger anser Datatilsynet for at falde i kategorien *følsomme* oplysninger:

(i) Oplysninger om helbredsforhold, herunder misbrug af nydelsesmidler, alkohol mv.
(ii) Oplysninger om medlemskab af en fagforening.
(iii) Oplysninger om strafbare forhold.
(iv) Oplysninger om andre tilsvarende rent private forhold, såsom at en medarbejder er bortvist fra jobbet på grund af en grov tilsidesættelse af ansættelsesforholdet, eller at medarbejderen har indgået registreret partnerskab.

På baggrund af Datatilsynets sondring ovenfor må det formodes, at vurderings-skemaer og samtalereferater (medarbejderudviklingssamtaler) som udgangs-punkt vil falde under kategorien almindelige oplysninger, hvorimod egentlige personlighedstests, straffeattester og politianmeldelser må formodes at falde i kategorien følsomme oplysninger.

De nærmere betingelser, der skal være opfyldt, før en behandling af henholdsvis følsomme og almindelige oplysninger er tilladt i henhold til persondataloven, er nærmere beskrevet i pkt. 4.2.1.2 ovenfor.

**2. Ansættelse af medarbejdere**

I forbindelse med ansættelse af medarbejdere er det normalt, at ansøgeren fremsender en række dokumenter, herunder eksamensbeviser, anbefalinger mv., til virksomheden. En række af disse fremsendte personoplysninger kan være af følsom karakter, jf. det ovenfor anførte. Formålet med virksomhedens behandling af sådanne oplysninger er naturligvis at opnå det fornødne grundlag til at træffe beslutning om, hvorvidt personen skal ansættes eller ej. Når afgørelsen er truffet, kan man spørge, om virksomheden har pligt til at slette de modtagne oplysninger og tilbagesende modtagne dokumenter vedrørende ansøgere.

Hvis personen *ikke* ansættes, forekommer svaret at være ja, idet en senere behandling typisk ikke vil være forenelig med det formål til hvilket, oplysningerne blev indsamlet. Hvis virksomheden imidlertid gemmer ansøgningerne i en kortere periode med det formål eventuelt at kunne dokumentere, at der ikke er sket forskelsbehandling, må dette anses for at falde inden for formålet. Opbevaring til senere brug, eksempelvis til brug for datterselskaber eller indlæggelse i en "jobbank" kræver derimod samtykke.

**3. Behandlinger efter ansættelsen**

Den person, der fremsender en ansøgning med diverse bilag i form af anbefalinger og eventuelle andre relevante oplysninger, herunder eksempelvis af helbredsmæssig karakter, som efterfølgende bliver ansat til det pågældende job, må som udgangspunkt anses for at have givet samtykke til, at ansøgningen og bilagsmaterialet opbevares under ansættelsesforholdet. I tilknytning hertil bemærkes, at en række ufravigelige regler i de såkaldte ikke-diskriminationslove har forrang i forhold til persondataloven.

Hvis organisationen rutinemæssigt opbevarer ansættelsespapirer, må det generelt anbefales at få medarbejderens samtykke for at undgå tvivl om rækkevidden af et sådant indforstået samtykke, herunder også fordi dokumenter modtaget i forbindelse med ansættelsen kan indeholde følsomme oplysninger. Dette samtykke vil mest hensigtsmæssigt kunne indhentes i forbindelse med indgåelsen af ansættelseskontrakten ved at indsætte en klausul herom. Organisationen skal naturligvis være opmærksom på, at medarbejderen har mulighed for efterfølgende at trække et givet samtykke tilbage og kræve vedkommendes personoplysninger slettet eller udleveret, forudsat at det ikke er nødvendigt, at oplysningerne beror i virksomheden. I forbindelse med indhentelse af et sådant samtykke vil det være praktisk, at virksomheden i ansættelseskontrakten sikrer sig adgang til at videregive personoplysninger om

den ansatte koncerninternt og i forbindelse med en eventuel senere due diligence og virksomhedsoverdragelse.

I løbet af et ansættelsesforhold har en arbejdsgiver i mange tilfælde interesse i at indsamle (behandle) en række oplysninger om medarbejderne. Ud over at påse at behandlingsbetingelserne er opfyldt, som anført ovenfor, bør arbejdsgiveren i forbindelse hermed tillige være opmærksom på de generelle regler om oplysningspligt, samt indsigts- og indsigelsesret.

Efter ansættelsesforholdets ophør må det antages, at virksomheden i en vis periode, hvis længde må afgøres konkret, kan behandle personoplysninger om tidligere ansatte.

## 4. Medarbejdernes brug af internettet

Et forhold, der har påkaldt sig en del opmærksomhed, er virksomhedernes overvågning af medarbejdernes brug af internettet med henblik på at forhindre, at medarbejderne i arbejdstiden bruger tid på at surfe rundt på internettet, hvis dette ikke sker i forbindelse med udførelsen af medarbejdernes arbejdsopgaver. Datatilsynet har i december 2000 i et nyhedsbrev udtalt, hvorledes persondataloven i denne forbindelse skal fortolkes.

> Forudsat at nedenstående kriterier er opfyldt, skal anmeldelse ved private virksomheders logning og kontrol af medarbejdernes internetbrug ikke ske:

(i) Registreringen og kontrollen af internet-brugen skal være nødvendig for, at arbejdsgiveren kan forfølge en berettiget interesse, og hensynet til den enkelte medarbejder må ikke overstige denne interesse. Eksempler på berettigede interesser er tekniske og sikkerhedsmæssige hensyn samt hensynet til kontrol af medarbejdernes brug af internet.

(ii) Medarbejderne skal på forhånd - på en klar og utvetydig måde - være informeret om, at registreringen/logningen finder sted, og at registreringen eventuelt vil blive gennemset som led i en kontrol ved mistanke om brug af internet i strid med arbejdspladsens retningslinier herom.

Eftersom misbrug - afhængig af forseelsens karakter - kan føre til afskedigelse eller i grove tilfælde bortvisning, er det vigtigt, at virksomhederne aktivt påser, at medarbejderne på en klar måde informeres om, hvorvidt privat brug af internettet i arbejdstiden er tilladt og omfanget heraf, samt om virksomhedens politik i henseende til forbud mod i arbejdstiden at se og downloade materiale fra f.eks. porno-sites. Virksomhederne skal foretage denne information såvel over for

eksisterende som alle nye medarbejdere og specifikt gøre opmærksom herpå. I alles interesse bør "internetpolitikken" nedfældes skriftligt, eksempelvis i en personalehåndbog eller i et tillæg til ansættelseskontrakten.

## 5. Medarbejdernes brug af e-mails

På samme måde som ved brug af internettet bør virksomhederne informere sine ansatte om, hvorvidt virksomhedens edb-system må bruges til at modtage og sende private e-mails. Ud over den mere almindelige brug af e-mail og internet har virksomheder i vidt omfang erfaret, at medarbejdere internt til venner og kolleger sender e-mails vedhæftet såkaldte attachments, som kan være alt lige fra uskyldige vittigheder, kulørte billeder til små videoklip af op til adskillige sekunders varighed. Fra arbejdsgiverens synspunkt er attachments ofte en kilde til virusinfektioner og server-nedbrud. De førnævnte filer med video-sekvenser er pladskrævende på harddiske mv., og enhver kan forstille sig, at såfremt en medarbejder, efter at have modtaget en video-attachment, videresender denne til 15 af sine nærmeste kolleger in-house, der igen videresender filen til deres venner og kolleger osv., udgør noget sådant en stor belastning af virksomhedens IT-system med deraf følgende risiko for nedbrud.

Afhængigt af omfanget af virksomhedens brug af e-mail er der mange gode grunde til, at en arbejdsgiver på samme måde som i relation til brug af internettet implementerer en "e-mail-politik". Datatilsynet har tilladt, at virksomheder ud fra ledelses-, drifts- og sikkerhedsmæssige hensyn må foretage logning og kontrol af medarbejdernes brug af e-mail, hvis nedennævnte retningslinier overholdes.

Organisationer skal ikke foretage anmeldelse af logning og kontrol af medarbejdernes brug af e-mail, forudsat at nedenstående krav er opfyldt

(i) Sikkerhedskopieringen af e-mails og en eventuel gennemgang af en medarbejders e-mails må kun ske, hvis det er nødvendigt for, at arbejdsgiveren kan forfølge en berettiget interesse, og hensynet til den ansatte ikke overstiger denne interesse. En berettiget interesse kan f.eks. være hensynet til drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af medarbejderes brug.

(ii) Medarbejderne skal på forhånd - på en klar og utvetydig måde - være informeret om sikkerhedskopieringen og den eventuelle gennemgang af den enkelte medarbejders e-mails.

(iii) Ved en gennemgang af en medarbejders e-mails må arbejdsgiveren ikke læse medarbejderens e-mails, der er identificeret som private.

De samme bemærkninger vedrørende informering af medarbejdere som anført i pkt. 4.3.3 gælder også i relation til virksomheders kontrol af medarbejdernes brug af e-mail.

**6. Medarbejdernes brug af telefon (mobil- og fastnet)**

Som hovedregel må virksomheder ikke foretage automatisk registrering af, hvilket telefonnumre medarbejderne foretager opkald til fra deres telefoner. Undtagelsesvis kan der fra Datatilsynet opnås tilladelse til en sådan registrering, hvor afgørende hensyn til private interesser taler herfor, f.eks. hvis videredebitering til kunden kan eller skal ske. I så fald vil Datatilsynet typisk fastsætte vilkår for den tilladte registrering.

Organisationers automatiske registrering af indgående opkald er derimod ikke reguleret.

**7. Video-overvågning**

Behandling af personoplysninger i forbindelse med video-overvågning vil efter omstændighederne være omfattet at persondataloven, forudsat at de optagne personer er identificerbare. For den offentlige sektors vedkommende vil oplysninger fra video-overvågning skulle opbevares i digital form, for at persondataloven finder anvendelse, hvorimod persondatalovens regulering også i vidt omfang vil finde anvendelse på manuel behandling af sådanne oplysninger i den private sektor. Generelt må det antages, at samlinger af video-optagelser, fx fra arbejdspladser, i meget vidt omfang vil være beskyttet af persondataloven. Det bemærkes endvidere, at lov om forbud mod video-overvågning ikke indeholder regler om opbevaring mv. af optagelser, der hidrører fra video-overvågning. Overvågningsloven anses primært for at regulere spørgsmålet om selve adgangen til at foretage filmisk overvågning, mens persondataloven gælder i relation til hvilken måde, optagelserne af en lovlig video-overvågning kan opbevares og anvendes på.

**8. Offentliggørelse af medarbejderoplysninger på en hjemmeside**

Organisationer kan efter Datatilsynets praksis på en hjemmeside offentliggøre arbejdsrelaterede oplysninger (navn, stillingsbetegnelse, arbejdsområde, ansættelsesår, direkte arbejdstelefonnummer, e-postadresse uden samtykke). Medarbejderen vil dog efter omstændighederne kunne modsætte sig offentliggørelse, hvis der foreligger særlige omstændigheder. Der kan ikke uden den enkelte ansattes samtykke offentliggøres oplysninger som billede af den ansatte, privatadresse, privat e-postadresse og telefonnummer.

**9. CPR-numre**

Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på entydig identifikation eller som journalnummer. Private virksomheder må som udgangspunkt kun behandle oplysninger om

personnummer, når det følger af lov eller bestemmelser fastsat i henhold til lov, eller den registrerede har givet sit udtrykkelige samtykke hertil.

## 10. Afsluttende bemærkninger

Under hovedoverskriften **"Overvågning på arbejdspladser"** er der – ud over spørgsmålet om hvad arbejdsgiveren må overvåge – rejst spørgsmål om, **hvad der bekymrer de ansatte mest** og **sammenhængen mellem lovgivning og informationspligt**.

Det er min opfattelse, at det der giver anledning til mest bekymring er, hvis medarbejderen ikke har en klar viden om, hvad arbejdsgiveren registrerer og overvåger, og hvad formålet er. Det må derfor meget anbefales, at organisationer drøfter disse forhold i samarbejdsudvalg, og at der fastsættes klare retningslinjer, der er tilgængelige for alle medarbejdere, herunder nye medarbejdere.

I de situationer, hvor persondataloven ikke kræver et egentligt udtrykkeligt samtykke fra medarbejderen til behandling af personoplysninger, vil bestemmelserne i persondataloven generelt indeholde et krav om/forudsætte, at medarbejderen har fået klar underretning om, hvad organisationen overvåger/ registrerer/behandler. Samtidig skal man huske, at det ikke kun handler om overvågning som noget negativt. Det handler primært for organisationer om sikkerhed i bred forstand, herunder sikkerhed omkring sagshåndtering, systemsikkerhed mv.

**Fokus må derfor rettes på, at organisationerne udarbejder e-post-, internet- og video-overvågningspolitikker og derved synliggør organisationens holdninger over for medarbejderne og er i aktiv dialog med medarbejderne herom.**

**Der synes på ovennævnte baggrund ikke at være behov for at foretage en revision af persondataloven, men snarere et behov for at informere mere bredt om arbejdsgiverens informationspligt.**

## ”Hvor er Folketingets indsats påkrævet ?”

*Af Jon Stokholm, advokat, Formand for Advokatrådet*

Indlægget omhandler de retssikkerhedsmæssige aspekter, som er forbundet med lovgivningsmæssige initiativer vedrørende overvågning.

- - - - - - - - - - -- - -

Begrebet ***retssikkerhed*** er det helt centrale begreb for Folketinget i deres lovgivende arbejde. Det er et ideal for hele den retspolitiske debat og et ideal for ethvert samfund. Det er ikke tilfældigt, at begrebet er en del af en århundrede lang rets-tradition i den vestlige verden.

Retssikkerhed er ikke et entydigt begreb. Men netop dets flertydighed er formentlig årsagen til, at det til stadighed er muligt at fortolke begrebet dynamisk i lyset af nutidens krav og behov. Der er tale om et fundamentalt hensyn og om nogle helt centrale garantier.

Hvis man forsøger at ”fastfryse” begrebet, så dækker det for det første over en bestræbelse på at beskytte og udbygge samfundets vedtagne og internationalt anerkendte menneskerettigheder, herunder sikre borgernes kendskab til disse rettigheder. Retssikkerhed er således en anerkendelse af, at der er behov for at begrænse statens ret til magtudøvelse, så den alene finder sted i henhold til regler, som er tilvejebragt i overensstemmelse med et demokratisk samfunds spilleregler og med den nødvendige respekt for mindretalsgarantier.

Dernæst indeholder begrebet retssikkerhed et krav om at forebygge og beskytte den enkelte borger mod overgreb fra offentlige myndigheders side, samt sikre kravet om en retfærdig rettergang, det som ofte kaldes ”fair trial”.

Også associationer som retfærdighed, retshåndhævelse og retsfølelse dukker op, så snart man begynder at tænke over, hvad retssikkerhed dækker over. Retssikkerhed er på denne måde et sammensat begreb, hvor der er mange forskellige hensyn, der skal iagttages.

Det aktuelle retssikkerhedsniveau udgør på denne måde altid et skæringspunkt eller en politisk afvejning mellem forskellige interesser og hensyn.

Retssikkerheden afvejes i praksis ofte over for økonomiske ressourcer – hvor meget er man villig til at betale for retssikkerhed ? Retssikkerheden afvejes også over for ikke-økonomiske faktorer. Eksempler herpå findes i straffeprocessuelle reguleringer, f.eks. overvågning, herunder aflytning og andre indgreb i meddelelseshemmelig-heden (retsplejelovens § 781), observation (retsplejelovens § 791 a) og ransagning (retsplejelovens § 794, jf. 799). Her er der på den ene side krav om beskyttelse af

sigtede, mistænkte og ikke-mistænkte personers retsstilling, og på den anden side behov for at beskytte såvel borgere som samfundet mod vold eller andre forbrydelser.

Det store spørgsmål – og den store udfordring for Folketinget - er da også, hvordan man sikrer den rette afvejning af på den ene side retssikkerheden og på den anden side opklaring af kriminalitet. Afvejningen er således relevant dels for de tvangsindgreb, som er affødt af vores egne nationale behov, men i lige så høj grad for den lovgivning om tvangsindgreb, som er en følge af Danmarks deltagelse i EU-samarbejdet.

Et godt sted at starte, når den udfordring skal løftes, er i selve lovgivningsprocessen. Netop kvalitet i lovgivningsprocessen har i efterhånden mange år været en mærkesag for Advokatrådet.

Selvom fokus i de senere år har været rettet mod forløbet af lovgivningsprocessen og kvaliteten heraf, og selvom der også er gjort fremskridt, er der efter Advokatrådets opfattelse fortsat behov for forbedringer, så retssikkerheden til stadighed sikres fastholdt og eventuelt udbygget i dansk ret.

Advokatrådet har ved enhver given lejlighed påpeget, at hastværk og utilstrækkelig forberedelse i lovarbejdet giver anledning til retssikkerhedsmæssige betænkeligheder. Hertil kommer, at selve væksten i lovgivningsinitiativerne i stigende grad øger behovet for retssikkerhedsmæssige vurderinger.

Det er derfor vigtigt, at der i videst mulige omfang gøres brug af de mekanismer, som er med til at sikre, at lovforberedelsen finder sted i betryggende former. Forud for fremsættelse af nye vigtige lovforslag og forud for gennemførelse af lovændringer på fundamentale områder bør der således som altovervejende hovedregel finde en grundig behandling sted i uafhængige og alsidige sammensatte udvalg, ligesom der bør afsættes den fornødne tid til at høre relevante interesseorganisationer m.v., inden lovforslag færdiggøres og fremsættes i Folketinget.

Ofte fastsættes så korte høringsfrister, at høring af organisationer m.v., som kunne bidrage med saglige kommentarer, derved bliver gjort illusorisk. I andre tilfælde undlader det ministerium, der har ansvaret for lovforslagets fremsættelse, at gennemføre en høring inden forslagets fremsættelse for Folketinget, typisk på grund af tidsnød. Endelig er der eksempler på, at resultatet af en høring tilsidesættes for ikke at kompromittere et politisk forlig.

Henset til at en meget stor del af den lovgivning, som vedtages i Folketinget, udspringer af forordninger og direktiver vedtaget i EU, er det ekstra vigtigt, at man på alle mulige måder styrker muligheden for, at både Folketinget og alle relevante faglige organisationer i tide kan præge EU´s beslutningsproces.

Advokatrådet har således ofte været undergivet endog meget korte tidsfrister, hvilket naturligvis giver anledning til problemer i de meget tunge sager, hvor der modtages store mængder "papir" om ofte overordentlige komplicerede regler, der f.eks. skal drøftes på et specialudvalgsmøde få dage efter.

Det er også vigtigt at påpege, at stemningsbaserede lovgivningsinitiativer og lovgivningsinitiativer, bygget op omkring konkrete enkeltsager, generelt er uegnede til at skabe det fornødne saglige fundament for lovgivning.

Der findes flere eksempler herpå, men mest nærværende er de tragiske begivenheder i forbindelse med terrorangrebene på World Trade Centre og Pentagon den 11. september 2001. Her kommer begrebet retssikkerhed virkelig på en af sine største prøver i nyere tid, idet der som følge af tragedien er opstået et stort politisk ønske – både nationalt og internationalt – for lovgivningsmæssigt at skabe de bedst mulige midler til terrorbekæmpelse. Den "uofficielle lovgivningsproces" kører også her på højtryk. Aviser og tv indeholder således daglig inspiration til nye lovgivningsinitiativer i kampen mod terroren.

Regeringen har i lyset heraf bebudet en række lovgivningsmæssige initiativer med henblik på at bekæmpe terrorisme. Det forlyder, at et af tiltagene er, at der vil ske en forbedring af politiets grundlag for at foretage overvågning. Således skal det sikres, at teleselskaber og internetudbydere registrerer og opbevarer oplysninger om tele- og Internetkommunikation til brug for politiet. Der bliver også øget adgang til at foretage telefonaflytning m.v. i særlige sager.

Nu kender jeg ikke det præcise indhold af regeringens initiativer, men regeringens reaktion viser, at der kan være grund til at frygte, at hensynet til retssikkerheden ikke får den vægt, som det fortjener i et demokratisk samfund.

Ligeledes er spørgsmålet om adgangen til brug af anonyme vidner rejst på ny. Også her har det altid været Advokatrådets opfattelse, at anonym vidneførelse indebærer en øget risiko for usandfærdige vidneforklaringer og en uacceptabel risiko for urigtige domfældelser.

Hvis Folketinget alligevel skulle finde, at hensynet til at bekæmpe kriminalitet i nogle tilfælde vejer så tungt, at der er behov for overveje yderligere regulering vil jeg opfordre Folketinget til også at overveje, hvordan man dog vil være i stand til tilgodese hensynet til retssikkerhed til en vis grad.

Dette kan f.eks. ske ved at indsætte revisionsbestemmelser i lovgivningen. Herved sikres, at loven efter en nærmere fastsat periode gennemgår en revurdering i lyset af de hidtidige erfaringer.

Som et andet eksempel på en sådan form for kompensation for retssikkerhed kan nævnes udvidet adgang til at få beskikket en forsvarer, f.eks. så snart overvågningen påbegyndes. Udvidet adgang til at foretage tvangsindgreb bør således gå "hånd i hånd" med en udvidet adgang til forsvarsbeskikkelse, således at der f.eks. indføres generelle regler om beskikkelse af forsvarer allerede inden der foreligger en sigtelse. I den forbindelse er det naturligvis afgørende, at advokatens tavshedspligt er intakt, hvilket ellers i øjeblikket er under hårdt pres fra EU´s side. Klienten må efter Advokatrådets opfattelse kunne betro sig i fortrolighed til sin advokat. Dette er en helt central forudsætning for den enkeltes retssikkerhed.

Dertil kommer, at det er nødvendigt at også kommende lovgivningsinitiativer på dette område indeholder en klar angivelse og definition af, hvad de oplysninger og data, som myndighederne kommer i besiddelse af i forbindelse med overvågningen, kan og må bruges til. Det er også netop sådanne overvejelser, som IT- og forskningsministeren har tilkendegivet omkring lovinitiativet om registrering af spor hos Internetudbydere. I overensstemmelse hermed ser jeg gerne, at ministre, der har en tilsvarende holdning, får tilført yderligere ressourcer, der så kan bruges til at udmønte opprioritering af retssikkerhedshensynet i praksis.

På spørgsmålet om "Hvor Folketingets indsats er påkrævet", er mit svar, at der ikke umiddelbart er et særligt behov for at sætte ind med ny lovgivning. De eksisterende regler udgør således tilstrækkelig værn mod endog meget grov kriminalitet. Hvis der er behov for ændringer, kan der højst blive tale om små finjusteringer. Det, der i virkeligheden er brug for, er, at Folketingets medlemmer - også i pressede situationer - formår at holde hovedet koldt og til stadighed påser at væsentlige retssikkerhedsgarantier ikke går tabt.

## Teknologirådets borgerpanel

*Af Anne-Sofie Dideriksen, Medlem af Teknologirådets borgerpanel ved konsensuskonference om elektronisk overvågning i efteråret 2000.*

I november 2000 gennemførte Teknologirådet en konsensuskonference om emnet elektronisk overvågning. Et borgerpanel på 11 kvinder og mænd blev af rådet nedsat til at arbejde med emnet. Forud for konferencen var borgerpanelet samlet i to forberedelsesweekender for at opstille en række spørgsmål til uddybning af overvågningstemaet. Spørgsmålene blev ved selve konsensuskonferencen besvaret af indkaldte eksperter, og som afslutning på konferencen udarbejdede panelet et slutdokument med anbefalinger på området. Min opgave er her kort at gøre rede for centrale vurderinger og anbefalinger, som vi i borgerpanelet i november 2000 kunne skabe konsensus om. Borgerpanelets slutdokument, som den følgende tekst således er et sammendrag af, findes andetsteds i denne høringsmappe.

Hvad jeg i det følgende fremlægger, er selvsagt kommet til verden uden den påvirkning, som terrorangrebene d. 11. september 2001 i USA måtte have haft på vores tilgang til temaet elektronisk overvågning. Panelets anbefalinger og vurderinger skal naturligt nok ses i lyset af den tid, de er blevet til. På nogle punkter ville vores diskussionsgrundlag være radikalt anderledes, på andre punkter måske ikke helt så forandret.

### BORGERPANELETS VURDERINGER OG ANBEFALINGER

I borgerpanelets slutdokument behandles det komplekse emne elektronisk overvågning under de følgende fire overskrifter, som også vil strukturere denne sammenfatning af slutdokumentet:

I: Menneskelige konsekvenser af elektronisk overvågning
II: Overvågningens konsekvenser for samfundet
III: Lovgivning og retssikkerhed vedrørende registrering og brug af oplysninger samt elektronisk overvågning
IV: Overvågning på arbejdspladsen

Hvor så vi dengang problemer og hvad anbefalede vi? Indledningsvist vil kort jeg gøre opmærksom på en generel erfaring, borgerpanelet gjorde sig, nemlig at emnet elektronisk overvågning var en uhyre kompleks størrelse, og at de svar, de indkaldte eksperter gav på panelets spørgsmål, var af særdeles overordnet karakter. Dette forhold havde naturligvis betydning for borgerpanelets opgave, dvs. at give anbefalinger på området. I slutdokumentets indledning skriver panelet således: "Eksperternes vanskeligheder med at give konkrete svar afspejler sig i borgerpanelets slutdokument, hvor det har været svært at give absolutte anbefalinger. Udviklingen kræver, at der hele tiden må følges med rent lovgivningsmæssigt efterhånden som

teknologierne bliver udviklet." (8)[*] Panelets anbefalinger, som de kommer til udtryk i slutdokumentet og det følgende sammendrag, skal læses med disse erfaringer in mente.

## I: Menneskelige konsekvenser af elektronisk overvågning

- **Hvordan påvirker overvågning mennesket?**

Panelets indtryk var, at der ikke var forsket meget i, hvordan overvågning påvirker mennesket, og formulerede derpå selv en vurdering af de menneskelige konsekvenser af elektronisk overvågning: ”Man flytter ind i et offentligt og privat glashus og udsættes for at blive kigget efter i sømmene. Den sociale kontrol erstattes af en teknisk 'gennemlysning' af ens handlinger.” (9)

På dette område var borgerpanelets centrale anbefaling, at der "generelt bør rejses en debat, som skaber bevidsthed om, at den elektroniske overvågning i sig selv ikke er en garanti for tryghed og at overvågning ikke kan erstatte den sociale kontrol." (10)

- **Overvågning af børn**

Panelet vurderede, at der herskede særlige forhold for børn, og at det var problematisk, at der ikke fandtes lovgivning, som tager specielt hensyn til børns rettigheder. Om de skal overvåges i institutioner er afhængig af forældres og pædagogers holdninger til overvågning, og panelet var af den opfattelse, at en del overvågningsforanstaltninger “opfylder de voksnes behov for kontrol" (10).

På baggrund af disse vurderinger anbefalede panelet, at der rådes bod på, at ingen instanser varetager børns rettigheder i forbindelse med lovgivning på dette område, og at der er behov for oplysning og rådgivning til forældre og institutioner angående overvågning af børn.

## II: Overvågningens konsekvenser for samfundet

- **Overvågningens rolle i samfundet**

"Overvågningsteknologien udgør i sig selv ikke en trussel" (13), understregede panelet. Men for at overvågning ikke udvikler sig til en trussel mod individet og samfundet anbefalede borgerpanelet, at der sikres et stærkt og levende demokrati og en løbende etisk debat om, hvilket samfund vi ønsker. Det skal bl.a. debatteres, hvordan vi takler spændingsfeltet mellem den krænkende overvågning og den forebyggende overvågning og om overvågning erstatter tillid og fællesskab med mistillid og egoisme.

[*] I det følgende henviser sidetal i parentes til borgerpanelets slutdokument i: *Elektronisk overvågning. Slutdokument og ekspertindlæg fra konsensuskonference d. 17.-20. november 2000*. Teknologirådets rapporter 2000/9.

På baggrund af disse holdninger anbefalede borgerpanelet, at "man overalt i samfundet prioriterer omsorg og opdragelse højere end kontrol og overvågning" (13), så overvågning ikke forskubber fokus fra reglens begrundelse til en kontrol af, om reglen bliver overholdt. Man skal med andre ord ikke holde med at stjæle i en videoovervåget butik, fordi det kan opdages, men fordi man skal respektere den private ejendomsret.

- **Forvaltning af oplysninger**

Panelet fremhævede vigtigheden af, at den enkelte bør beskyttes mod overdreven kontrol og overvågning og bør have selvbestemmelse med hensyn til, hvilken overvågning vedkommende udsættes for. Men den enkelte har også selv "et individuelt ansvar for at sige fra, når den enkeltes grænse er nået." (13)

Med udgangspunkt i dette anbefalede panelet generelt bedre oplysning til borgerne om sikkerhed i forbindelse med brug af internet m.m. og om rettigheder til indsigt i f.eks. persondata. I en videre anbefaling opfordrede panelet til åbenhed i omgangen med oplysninger indenfor det offentlige og i private virksomheder.

**III: Lovgivning og retssikkerhed vedrørende registrering og brug af oplysninger samt elektronisk overvågning**

- **Lovgivningen**

Er lovgivningen på de områder, som vedrører elektronisk overvågning, på højde med de forandringer, den teknologiske udvikling medfører? Dette interesserede borger-panelet, som så problemer på flere områder. At tele-, medie, forsikrings-, bank- og kreditvirksomheder efterhånden samles i store enheder kan eksempelvis medføre et pres på de love, som regulerer brugen og samkøringen af registrerede kunde-oplysninger. F.eks. kan man også forvente, at forsikringsselskaber ønsker at gøre brug af helbredsoplysninger og dna-materiale i forbindelse med risikovurdering.

Panelet anbefalede i denne forbindelse, at persondataloven og andre love som vedrører overvågning til stadighed revideres af de relevante myndigheder. Ligeledes var det panelets anbefaling til de danske myndigheder at holde et vågent øje med, om international lovgivning på området ville kunne udvande eksisterende dansk lovgivning, der skal sikre den enkelte borgers integritet.

- **Den enkeltes retssikkerhed**

Panelet vurderede på dette område bl.a., at den enkelte under overvågning med præventive formål potentielt kunne krænkes, fordi overvågningsteknologi gør det muligt at fastslå ens blotte tilstedeværelse i nærheden at et gerningssted: "[E]n omvendt bevisbyrde kunne komme til at gælde. Man ville være skyldig indtil det modsatte var bevist. Man kunne f.eks. komme under mistanke eller ligefrem blive erklæret skyldig i en forbrydelse […]" (15)

Med denne risiko for krænkelse af den enkeltes retssikkerhed for øje anbefalede panelet en nøje afvejning af gevinsten ved opsætning af overvågningsudstyr overfor den potentielle krænkelse af retssikkerheden og efterlyste mere debat på området.

**IV. Overvågning på arbejdspladsen**
Borgerpanelet fandt, at den direkte påvirkning fra overvågning og uklare spilleregler på arbejdspladserne vedrørende den elektroniske overvågning "har en negativ indflydelse på det psykiske arbejdsmiljø, og at dette vil blive et stigende problem i takt med den øgede brug af elektronisk overvågning." (17) Helt overordnet anbefalede panelet, at arbejdsmarkedets parter udarbejder et sæt regler for indførelse og regulering af elektronisk overvågning, som gøres til lov af Folketinget.

- **Video-overvågning**

Panelet var af den opfattelse, at medarbejderinddragelse er centralt for håndteringen af overvågningsproblematikken: "I forbindelse med overvågning bør betydningen af overvågningsfrie zoner, håndtering af data, placering af kameraer nøje overvejes i samarbejde med de ansatte." (18)

Hvad angår videoovervågning, vurderede panelet, at den kan have en vigtig tryghedsskabende virkning, men at alternative muligheder til at begrænse f.eks. svind i forretninger på bør overvejes. På steder, hvor der ikke kommer kunder, bør der efter panelets mening benyttes andre metoder end videoovervågning i arbejdstiden. Desuden finder panelet en statsautorisation af forhandlere og montører af overvågningsudstyr nødvendig for at sikre en lovlig og korrekt opsætning af videoovervågningsudstyr.

- **Kontrol af e-mail og internetbrug**

Teknologien medfører ændrede arbejdsgange og kommunikationsformer i arbejdslivet. I forbindelse med arbejdsgiverens kontrol af e-mails anbefalede borgerpanelet, at der på den enkelte arbejdsplads skal være en klar adskillelse mellem, hvad der er privat kommunikation, og hvad der er en del af firmaets dokumentation, der skal arkiveres og være tilgængelig for relevante personer i firmaet.

## Staten og individet - det gradvise skred mod et overvågningssamfund

*Af Per Helge Sørensen, forfatter, bestyrelsesmedlem i Digital Rights*

### Generelt om privatliv

Et væsentligt element i overvågningsdiskussionen er balancen mellem statens kontrolmuligheder og individets privatliv.

Det er denne balance, der er på spil, når betingelserne for politiets efterforskning af kriminalitet - f.eks. brug af aflytning - diskuteres. Tilsvarende er det denne balance der skal opretholdes, når grænserne for efterretningstjenesternes overvågnings-muligheder er til debat.

Menneskerettighedskonventionerne fastslår individets ret til privatliv som et grundprincip, og at staten derfor kun bør gribe ind i dette privatliv, når der er væsentlige grunde til det, samtidig med at der i statens indgreb skal være proportionalitet mellem indgrebets karakter og det formål der søges opnået.

Selv i et land som Danmark, hvor borgerne næppe bør frygte, at staten misbruger sine magtmidler - hvor politiet formodentlig kun ønsker at opklare forbrydelser til borgernes bedste - er det væsentligt, at statens muligheder for at gribe ind i borgernes privatliv ikke bliver for store.

Lod vi f.eks. politiet anvende telefonaflytning i selv de mindst alvorlige forbrydelser (f.eks. færdselsforseelser) ville vi skabe et samfund, hvor alle borgere kunne frygte, at nogen lyttede med, når de løftede røret. Tilsvarende ville risikoen for misbrug af aflytningsmuligheden blive større. Samfundet ville være blevet mindre frit.

### Skreddet mod overvågningssamfundet

Den teknologiske udvikling har på en række områder forrykket balancen mellem statens kontrolmuligheder og individets privatliv. Dette skyldes tre forhold:

- de større kontrolmuligheder, der er integreret i den nye teknologi
- en målrettet tilpasning af teknologien mhp. at muliggøre overvågning
- en gradvis udvidelse af politiets mulighed for brug af elektronisk overvågning i takt med udbredelsen af elektronisk kommunikation i samfundet

#### *Større kontrolmuligheder*

En væsentlig grund til skreddet mod mere overvågning er, at den nye teknologi i sig selv giver større kontrolmuligheder end den gamle "analoge" verden.

Brug af elektroniske betalingsmidler er et eksempel. Drift af et betalingskort som DAN-kortet forudsætter, at det registreres, hvor borgeren har brugt sit kort, og hvor mange penge borgeren har brugt. Mens anvendelse af kontanter er meget svær at

spore, giver overgangen til brug af betalingskort mulighed for præcist at kontrollere borgerens pengeforbrug. Samtidig opnås som sideeffekt en mulighed for at kortlægge borgerens fysiske færden via deres kontoudtog - at følge borgeren fra penge-automaten, til cafeen, til dagligvarebutikken osv. - en mulighed, som politiet naturligvis benytter i opklaringen af forbrydelser.

De øgede overvågningsmuligheder var næppe tiltænkt da man indførte DAN-kort systemet - man ønskede blot et mere effektivt betalingsmiddel. Overvågnings-muligheden er kommet med som sideeffekt.

Tilsvarende sideeffekter opstår på mange andre områder i takt med at samfundet bliver mere "elektronisk":

- når avislæsning flytter fra papiret til nettet
- når sundhedsinformation fås på nettet (netdoktor.dk) frem for hos lægen
- når indkøb sker på nettet frem for i butikker
- når folks seksuelle kontakter skabes på nettet frem for på barer
- når diskussionen i forsamlingshuset flytter til elektroniske chatrooms
- når mobiltelefonen giver mulighed for at spore borgerens fysiske færden

Politiets anvendelse af disse elektroniske spor i deres efterforskning har sjældent været til politisk diskussion - anvendelsen er blot sket som en videreførelse af sædvanlige efterforskningsmuligheder samt ved anvendelse af regler om teleaflytning - regler der var indført med henblik på en teknologi (telefoner) som gav væsentlig færre muligheder for at kontrollere borgerens færden og kommunikation.

***Målrettet tilretning af teknologien***

Selvom teknologien i sig selv har givet en markant udvidelse af statens kontrol-muligheder, har man i mange tilfælde ikke ladet det blive ved det.

I en række tilfælde har man således overvejet - og i visse tilfælde valgt - at *udvide* de overvågningsmuligheder, som teknologien tilbyder, ved at tilrette systemerne særligt med henblik på overvågning.

Implementering af GSM-systemet er et eksempel. Systemet var i sig selv vanskeligt at aflytte på grund af systemets opbygning med decentrale sendemaster. Efter systemets etablering valgte man derfor at implementere særlig teknologi, der gav politiet samme aflytningsmulighed som kendes fra fastnettelefoner. Tilsvarende har der været overvejelser om at pålægge Tele- og Internetudbydere at gemme data om brugerne - data som ikke er nødvendige for systemernes drift men som gemmes udelukkende af efterforskningshensyn. Dette gælder f.eks. data om brugernes e-mail kommunikationsmønster, samt data der kan identificere brugerne, når de surfer på nettet. (Et sådant krav er tilsyneladende en del af Justitsministerens terror-bekæmpelsespakke efter 11. september 2001).

Samtidig har man flere gange forsøgt at bremse teknologi, som kunne give en bedre beskyttelse af borgernes privatliv. Dette gælder f.eks. kryptering, som ville give borgere (og dermed også kriminelle) mulighed for at beskytte deres kommunikation mod aflytning. Tilsvarende har man haft overvejelser om at begrænse udbredelsen af forudbetalte (og anonyme) taletidskort til mobiltelefoner.

I forhold til telesystemer har man fra efterforskningsside ligefrem valgt at se det som et *grundkrav* til systemernes design, at systemerne kan aflyttes. I et samarbejde mellem en lang række (vestlige) landes efterforskningsmyndigheder har man således fastslået en række krav til telesystemer, som skal sikre aflytningsmulighederne (de såkaldte IUR - International User Requirements). Disse krav blev støttet i en Rådsresolution fra 1995, hvor EU's ministerråd anbefalede medlemsstaterne at implementere kravene i national telelovgivning. Samtidig har der været et udstrakt samarbejde mellem efterforskningsmyndigheder og leverandører af kommunikationssystemer med henblik på at sikre aflytningsmulighed. Efterretningstjenesterne har således traditionelt deltaget i standardiseringsarbejdet på telekommunikationsområdet (f.eks. i det europæiske standardiseringsorgan ETSI) ligesom der har været direkte kontakter mellem efterforskningsmyndighederne og leverandører.

Selvom teknologien i sig selv ofte giver en række øgede kontrolmuligheder har man altså valgt at udvidede kontrolmulighederne ved på en række områder at tilrette teknologien, så overvågningsmuligheden sikres eller bliver mere effektiv.

***Udvidelse af politiets overvågningsmulighed***
Den teknologiske udvikling har som beskrevet gjort eksisterende efterforskningsmidler mere indgribende - f.eks. ved at retsplejelovens bestemmelser om adgang til teleoplysningerne nu anvendes til at spore borgernes fysiske færden via positionsoplysninger i mobiltelefoner. Dette kunne have ledt til en mere restriktiv politik omkring anvendelse af disse efterforskningsmidler. I realiteten er det modsatte blevet tilfældet.

På en række områder har man inden for de sidste år valgt at slække kravene til brug af aflytning og elektronisk overvågning. For det første har man gentagne gange indført undtagelser for retsplejelovens bestemmelse om, at aflytning kun må anvendes ved forbrydelser med en straframme på mindst 6 år. Dette gælder f.eks. i forbindelse med distribution af børneporno.

Samtidig har man i et enkelt tilfælde - L194 - valgt at se bort fra det retssikkerhedsmæssige grundprincip, at borgere kun udsættes for overvågning, når der er konkret mistanke om, at de er involveret i alvorlig kriminalitet, og at borgerne efterfølgende orienteres om den overvågning, der har fundet sted.

Argumenterne for at slække kravene til brug af overvågning har typisk været, at politiet uden den elektroniske overvågning ikke vil kunne efterforske de pågældende forbrydelser, samt at forbryderne er blevet mere effektive og har fået bedre mulighed for at skjule sig ved at overgå til at anvende elektroniske kommunikation.

I realiteten synes situationen dog at være en anden. I takt med kriminelles overgang til brug af elektronisk kommunikation har politiet fået en række *nye* efterforskningsmidler, som ikke har været tilgængelige i den fysiske verden. Efterforskningsmidler, man ønsker at tage i brug - også selvom det forrykker balancen mellem staten og individet. Muligheden for at spore borgernes fysiske færden via positionsoplysninger i mobiltelefoner er f.eks. helt ny - når man i L194 udvider adgangen til at anvende disse oplysninger til også at omfatte almindelige borgere, får politiet adgang til oplysninger, som aldrig ville have været tilgængelige i den fysiske verden.

Derudover forekommer det, at beslutningen om at slække kravene til overvågning i flere tilfælde er truffet, hvor der på grund af folkestemningen eller omtale i pressen har været et politisk ønske om at "slå hårdere ned" mod en given type forbrydelser, og hvor man derfor har valgt at tillade overvågning, selvom forbrydelsens alvorlighed (strafferamme) ikke umiddelbart berettiger anvendelse af så indgribende efterforskningsmidler.

**Kan skreddet bremses?**
Meget tyder på, at den beskrevne udvikling mod øget overvågning vil fortsætte de kommende år.

I takt med teknologiens udbredelse i samfundet vil borgerne vil leve en stadig større del af deres liv "elektronisk" og dermed muliggøre en stigende overvågning. Samtidig de indbyggede kontrolmuligheder i teknologien blive stadigt mere præcise: mobiltelefoner vil kunne give positionsoplysninger med få meters nøjagtigheder osv.

I lyset af de seneste års udvikling er det næppe realistisk, at samfundet vil fraskrive sig muligheden for at anvende de øgede overvågningsmidler til efterforskning af kriminalitet. Det er f.eks. vanskeligt at forestille sig, at man ville vælge at begrænse politiets adgang til positionsoplysninger fra mobiltelefoner, fordi oplysningerne er blevet for præcise og overvågningen dermed for indgribende.

Trods intentionerne om det modsatte må det erkendes, at informationssamfundet - hvad angår kriminalitetsbekæmpelse - vil medføre øget og mere indgribende overvågning.

Stadigt er der dog en række politiske muligheder for at påvirke udviklingen.

Dels er den teknologiske udvikling ikke upåvirkelig. På en række områder er indretningen af vores kommunikationssystemer i dag et resultat af en målrettet

indsats for at *sikre* overvågningsmuligheden. Om denne indsats skal videreføres er et politisk valg.

Samtidig er det et politisk valg, om den stadige slækkelse af kravene til politiets brug af elektronisk overvågning, som vi har set inden for de seneste år, skal fortsætte.

***Skal overvågning være en designparameter?***
Hvad angår den teknologiske udvikling bør der tages politisk stilling til, om overvågningsmuligheden skal være et grundlæggende *krav* ved design af de teknologiske kommunikationsmidler.

Teknologien kan på en række områder beskytte mod de overvågningsmuligheder den skaber - f.eks. via kryptering eller anonyme tjenester (taletidskort, anonymiserings tjenester på Internet m.v.). Hvis disse teknologier tillades at blive udviklet er der mulighed for at genoprette den udvikling mod øget overvågning, som teknologien ellers giver anledning til.

Markedsudviklingen må i sig selv formodes at fremme disse teknologier, da der erfaringsmæssigt er stor opmærksomhed blandt forbrugerne om sikkerhed og overvågning. Dette forudsætter dog, at teknologierne tillades at blive udviklet, og at det ikke sættes som et grundlæggende krav til kommunikationsteknologi, at den kan overvåges.

Samtidig bør man fra politisk side være meget varsom med at kræve tilretninger af teknologierne, som forbedrer politiets overvågningsmuligheder - f.eks. lagring af ekstra data eller lagring ud over den periode udbyderne selv skal anvende data. I det øjeblik kommunikationssystemerne *tilrettes* til at muliggøre overvågning, har man reelt taget første skridt til at etablere dedikerede overvågningssystemer - systemer som ikke er etableret for at tilbyde borgerne en kommunikationsmulighed, men som udelukkende er etableret for at muliggøre overvågning.

***Hvor går grænsen for politiets indgriben?***
I forhold til politiets anvendelse af elektronisk overvågning må man frygte, at der vil ske en stadig svækkelse af kravene til anvendelse af overvågning, hvis der ikke bliver opstillet nogle fundamentale principper for, hvornår overvågning bør anvendes.

Disse krav kunne f.eks. indeholde:
- en fastlæggelse af hvor alvorlige forbrydelser, der skal være tale om, før vi som samfund vil tage overvågning i brug
- en fastholdelse af det princip, at borgere kun overvåges hvis de er under mistanke, og at elektronisk overvågning ikke anvendes til unødigt at kortlægge uskyldige menneskers færden omkring gerningsstedet (eller på nettet)

- en sikring af det grundlæggende princip om, at overvågede (efterfølgende) gøres bekendt med indgrebet, således at de pågældende evt. har mulighed for at prøve indgrebets retmæssighed ved domstolene.
- en generel afklaring af hvor mange oplysninger om borgeres færden på nettet, der bør gemmes af hensyn til evt. efterforskning, og hvor længe disse bør gemmes.

Opstilling af sådanne fundamentale principper kunne være en vej til at undgå, at samfundet gradvis skrider mod mere overvågning, som følge af at reglerne omkring anvendelse af dette efterforskningsskridt fastlægges "fra enkeltsag til enkeltsag".

## Kryptering med udgangspunkt i diskussionen om det såkaldte "Echelon"-overvågningsnetværk

*Af Professor, direktør, Peter Landrock, Ph.d.*

I dette korte indlæg prøver vi at besvare følgende spørgsmål:
Hvorfor er kryptering ikke mere udbredt end det er?
Hvilke barrierer er der for en mere udbredt kryptering?
Hvem er de væsentligste aktører på dette felt?

En række betingelser skal være opfyldt før det er praktisk muligt – og ikke mindst let og smertefrit – for danske borgere/firmaer og myndigheder at kommunikere sammen krypteret

1. Den enkelte bruger skal på sin arbejdsstation som et minimum have en software-pakke installeret som sætter ham i stand til at enkryptere sine e-mails. Denne enkryptering kan f.eks. være baseret på S/MIME standarden. Dette har de fleste brugere faktisk allerede, idet både Microsoft Outlook Express og Netscape browsere har sådanne programmer indbygget. I Microsoft kan man under ”Tools” og i Netscape under ”Options” vælge ”encrypt”, når man skal sende et enkrypteret e-mail. Nyere versioner vil endda kunne tillade såkaldt stærk kryptering, da amerikanske eksportrestriktioner på krypteringsalgoritmer er blevet lettet betydeligt. F.eks. benytter S/MIMEv.3 såkaldt triple-DES, som er praktisk ubrydelig.

2. Det er imidlertid en forudsætning, at man fra samtlige modtagere af et enkrypteret e-mail forinden har modtaget et såkaldt certifikat. Et certifikat knytter nemlig til modtageren den (offentlige) nøgle, som skal indgå i enkrypteringen. Forklaringen er ganske enkel: Enkryptering kræver, at der bruges en såkaldt sessionsnøgle, som automatisk vælges (genereres) af softwaren. Men modtagerens software kan jo ikke dekryptere, men mindre nøglen er sendt med, og i S/MIME gøres dette ved at enkryptere sessionsnøglen under modtagerens offentlige nøgle. S/MIME dekrypterer så automatisk ved et klik hos modtageren.

3. For at få et sådant certifikat skal den enkelte modtager vha. sin browser have genereret et nøglepar OG have kontaktet et CA (af uransagelige grunde i dansk lovgivning kaldes et nøglecenter, mens det i resten af verden kaldes et certificeringscenter), som udsteder et certifikat. Herhjemme har TDK og KMD oprettet certificeringscentre, og i Malmø findes desuden certificeringscentret Addtrust. Der findes web sites, som udsteder sådanne certifikater gratis til testformål, f.eks. på http://www.cryptomathic.com ved at klikke på ”labs” og dernæst ”Certification Authority”, hvor man let og smertefrit kan få udstedt et certifikat, *men*, uden nogen form for identifikation, således som et egentlig certificeringscenter må forventes at udføre det. Pointen bag et certifikat er nemlig at det sætter en bruger i stand til at kommunikere med en anden brug uden

forudindgået aftale, idet certificeringscentret har foretaget den fornødne identificering. Der er dog ikke noget i vejen for, at 2 brugere bliver enige om at få udstedt gratis certifikater uden identifikation og derefter udveksler krypteret e-mail.

4. Er man interesseret i at få en række emner belyst omkring sikker e-mail , kan det anbefales at downloade:

*Elektronisk indberetning til Finanstilsynet. Vejledning i sikker e-mail.* Finanstilsynet - 2. udgave - Marts 2001
fra http://www.finanstilsynet.dk/frame.asp?categoryID=258&menuID=238.

Denne vejledning er på 91 sider, og her har vi måske hele sagens kerne. De løsninger der forefindes i dag er simpelthen ikke brugervenlige nok, og får vi ikke lært at håndtere dette, vil digitale signaturer heller aldrig blive særlig udbredte.

5. Alternativer: Der findes også såkaldte "standalone" programmer, så muliggør kryptering og signering, f.eks. PGP, som har sin egen syntaks og derfor er inkompatibel med S/MIME. Desuden tilbyder en række firmaer på sikkerheds-området mere elle mindre avancerede løsninger baseret på såkaldte plug-ins, java-applets, chipkortintegrering etc., og sådanne løsninger kan laves meget mere brugervenlige og sikre end de løsninger der er beskrevet ovenfor. For kryptering er der imidlertid ikke så stor grund til at vælge mere sikre løsninger, da man her først og fremmest beskytter sig mod aflytning under transit.

   Desuden bør det også nævnes at SSL (TLS)-protokollen efterhånden er ret udbredt i WEB-applikationer, hvorved kommunikationen med applikationen altså automatisk bliver enkrypteret uden at brugeren skal foretage sig noget.

   Det bør også nævnes at en række firmaer har sat VPN (Virtual Private Network) op mellem dets forskellige afdelinger, som sikrer at al kommunikation mellem disse afdelinger er krypteret.

6. Aktørerne: I foråret 2000 arrangerede IT-Sikkerhedsrådet og Forsknings-ministeriet en høring med de forskellige firmaer som leverer software og eller hardwareløsninger til kryptering. Konklusionen var, at der findes en række produkter på markedet, som sætter brugeren i stand til at kommunikere sammen på sikker vis beskyttet af stærk kryptering.

   Hvis vi går nogle år tilbage var der, selv i Danmark, en diskussion i kulisserne om hvorvidt den enkelte borger skulle have adgang til stærk kryptering. IT-Sikkerhedsrådet anbefalede et klart "ja" men myndighederne og regeringen var længe om at spille ud. Først i forbindelse med en lempelse af Wassanar blev der meldt klart ud at man i det store og hele var for en sådan adgang. I mellemtiden

vendte amerikanerne henh. franskmændene rundt på en tallerken og accepterede stærk kryptering til henholdsvis eksport *fra* USA og frit brug i Frankrig. I UK derimod holder man igen med "the REGULATION OF INVESTIGATORY POWERS (R.I.P) bill", som "*will update the Interception of Communications Act, regulate covert surveillance and use of informers, and provide powers to decrypt coded e-mail*", idet man via lovgivning tvinger borgere og firmaer til at stille sessionsnøglerne til rådighed for myndighederne.

Men konkluderende må vi sige, at der efter vores mening ikke er nogen kræfter i eller uden for Danmark, der aktivt søger at hindre danske borgere i sikker kommunikation. Det, der mangler er en effektiv PKI (Public Key Infrastruktur) og mere brugervenlige produkter, problemer som det i princippet er nemt at løse, men ikke uden udgifter.

# BILAG 1

# Program

Onsdag d. 24. oktober 2001, 9 - 16 i Landstingssalen, Christiansborg

**9.00 - 9.10: Velkomst**

Ved ordstyrer, Lissa Mathiasen (S), Formand for Folketingets Retsudvalg

**9.10 - 10.00: Hvad er overvågning?**

Vi reagerer imod overvågning af os selv, men sætter samtidig overvågningskameraer op i børneinstitutionerne.
I denne emneblok diskuteres, hvad der er legitime hensyn at tage i forhold til borgerne, og skellet mellem frivillig og ufrivillig overvågning. I denne blok behandles også brugen af de elektroniske spor, vi efterlader os, når vi f.eks. bruger Dankort og mobiltelefoner.
Spørgsmål, der vil blive besvaret:

- Hvad er overvågning i lovens forstand?
- Har børn særlig behov for beskyttelse mod overvågning?
- Hvornår bliver elektroniske spor til overvågning?

**Oplægsholdere:**
Peter Blume, Professor, dr.jur. Institutleder, Retsvidenskabeligt Institut B, Københavns Universitet:

Kim Rasmussen, Kultursociolog og forskningslektor, Center for Institutionsforskning, Højvangsseminariet.

Peter Christensen, CNDO, Co-operative Network and Data Operation.

**Ordstyrer:** Lissa Mathiasen (S), Formand for Folketingets Retsudvalg.

**10.00 - 11.00: Overvågning med et kriminalpræventivt og –opklarende sigte**

Video-overvågning skaber tryghed mod vold for eksempel på banegårde, men de færreste ville vel have kameraer på villavejene og i hjemmet, hvor der begås langt flere forbrydelser.
I denne emneblok diskuteres brug af overvågning i det kriminalpræventive og opklarende arbejde. Grænserne for overvågning er ofte under pres. Men hvor meget overvågning af lovlydige borgere vil vi acceptere for at forhindre eller opklare forbrydelser? Hvilke grænser sætter menneskerettigheder og juridiske principper?
Spørgsmål, der vil blive besvaret:

- Hvad er virkningerne af kriminalpræventiv overvågning?
- Hvad synes borgerne om video-overvågning?
- Hvordan bruger Politiet elektronisk overvågning i deres arbejde?

**Oplægsholdere:**
Eva Smith, Professor, dr.jur., Formand for Det Kriminalpræventive Råd.

Niels Crone Lyngkjær, Kontorchef, Finansrådet.

Troels Ørting Jørgensen, Vicekriminalinspektør, Rigspolitiets afdeling A

**Ordstyrer:** Lissa Mathiasen (S), Formand for Folketingets Retsudvalg.

**11.00 - 11.15: Kaffepause**

**11.15 - 12.00: Overvågning med et efterretningssigte**

Staten og demokratiet har ret til beskyttelse mod anslag. Men hvor langt kan staten gå i overvågning og registrering af borgerne, før overvågningens pris bliver for stor? I denne emneblok diskuteres overvågning i efterretningstjenesternes arbejde. Hvem definerer, hvem der bør overvåges, og hvilke grænser bør der trækkes for overvågningen?

Spørgsmål, der vil blive besvaret:
- Hvilke virkemidler har PET og FE, og hvordan opfatter de grænserne for deres brug?
- Hvilke hensyn til borgernes retssikkerhed bør der tages?
- Kan kryptering være en måde for borgerne at beskytte sig mod uretmæssig overvågning? Hvorfor er det ikke mere udbredt?

**Oplægsholdere:**
Jørn Bro, Politimester i Glostrup, tidligere souschef i Politiets Efterretnings Tjeneste.

Birgitte Kofod Olsen, seniorforsker, Ph.d., Det Danske Center for Menneskerettigheder.

Peter Christensen, CNDO, Co-operative Network and Data Operation.

**Ordstyrer:** Lissa Mathiasen (S), Formand for Folketingets Retsudvalg.

**12.00 - 13.00: Frokost**

**13.00 - 14.00: Overvågning på arbejdspladser**

Privat brug af e-mail og nettet er en af de store tidsrøvere i mange firmaer, men betyder det, at chefen må holde øje med, hvad man laver på nettet eller skriver i sine e-mails?
I denne emneblok diskuteres arbejdsgiveres overvågning af ansatte. Fokus er på kameraovervågning og kontrol af e-mail og internet-brug.

Spørgsmål, der vil blive besvaret:
- Hvad må arbejdsgivere overvåge, i hvor høj grad skal de informere de ansatte?
- Hvad bekymrer de ansatte mest?

**Oplægsholdere:**
Laurits Rønn, Sektionschef, Ansættelsesretlig Sektion, Dansk Handel og Service

Bjarne Petersen, faglig sekretær, HK-handel

Janne Glæsel, advokat, Næstformand f. Datarådet

**Ordstyrer:** Hanne Severinsen (V), Formand for Folketingets Forskningsudvalg.

**14.00 - 14.20: Kaffepause:**

**14.20 - 15.50: Hvor er Folketingets indsats påkrævet?**
Mulighederne for overvågning vokser med den teknologiske udvikling. På visse områder vokser også presset for mere overvågning. Er lovgivningen fulgt med?
I denne blok diskuteres de "ømme punkter" i overvågningslovgivningen. Men også borgernes syn på overvågning inddrages. Og deres handlemuligheder.

**Samlet debat mellem politiker-panel og samtlige eksperter efter oplæg fra:**
Jon Stokholm, advokat, Formand Advokatrådet

Anne-Sofie Dideriksen, medlem af Teknologirådets Borgerpanel om overvågning

Per Helge Sørensen, forfatter, medlem af bestyrelsen i Digital Rights

Peter Landrock, professor, administrerende direktør, Cryptomathic.

**Ordstyrer:** Hanne Severinsen (V), Formand for Folketingets Forskningsudvalg.

**15.50 - 16.00: Afrunding**
Ved ordstyrer, Hanne Severinsen (V), Formand for Folketingets Forskningsudvalg.

# BILAG 2

# Borgerpanelets slutdokument
# Konsensuskonference om elektronisk overvågning
# den 17. – 20. november 2000

**Borgerpanel**

**Anne-Sofie Dideriksen**, 29 år, Ph.d. stipendiat, Århus
**Benny Kristensen**, 39 år, faglærer, Næstved
**Ditlev Granhøj Jensen**, 23 år, studerende, Odense
**Gerda Bruhn**, 45 år, sundhedsplejerske, Thisted
**Helge Bjerre**, 47 år, handelsagent, Slagelse
**Helle Landkildehus**, 35 år, socialrådgiver, Tranbjerg J
**Henrik Furbo Rasmussen**, 40 år, afdelingsleder, Hørsholm
**Inge Damgaard**, 53 år, sekretær, Faaborg
**Kurt Kristensen**, 42 år, arbejdsløs, Randers
**Marianne Stenstrop**, 33 år, folkeskolelærer, Vanløse
**Mette Eng**, 26 år, studerende, København

**Ekspertpanel**

**Anders Bjerre**, Institut for Fremtidsforskning
**Anne Kathrine Schøn**, DA
**Arne Gram**, Det kriminalpræventive Råd
**Hagen Jørgensen**, Forbrugerombudsmand
**Henrik Waaben**, Datatilsynet
**Jan Carlsen**, Institut for datasikkerhed
**Janne Glæsel**, Bech-Bruun og Trolle advokatfirma
**John Strand**, Strand Consult
**Jørgen Hoppe**, HK
**Kim Munch Lendal**, Dansk Handel & Service
**Kim Rasmussen**, Højvangsseminariet
**Klaus Rasborg**, Roskilde Universitetscenter
**Linda Nielsen**, Københavns Universitet, Retsvidenskabelig Institut
**Oluf Jørgensen**, Danmarks Journalisthøjskole
**Per Helge Sørensen**, Digital Rights
**Peter Blume**, Københavns Universitet, Retsvidenskabelig Institut
**Peter Christensen**, EDB-fagets fagforeningen, PROSA
**Steffen Stripp**, PLS-Rambøl
**Søren Baggesen**, Roskilde Universitetscenter
**Trine Rode**, Aalborg Universitet, Institut for kommunikation
**Yih-Jeou Wang**, Dansk Industri

# Introduktion

Teknologirådet har nu gennemført konsensuskonferencen med titlen: ”Elektronisk Overvågning” med et borgerpanel bestående af 11 kvinder og mænd.

Borgerpanelet har haft to forberedelses-weekender, hvor vi har gennemdrøftet hele problematikken og udmøntet den i en række spørgsmål til ekspert-besvarelse.

Efter indstilling fra borgerpanelet har Teknologirådet i samarbejde med en planlægnings-gruppe udpeget 21 eksperter til at besvare panelets spørgsmål. Efterfølgende har eksperterne såvel skriftligt som senere mundtligt under konferencen på Christiansborg forholdt sig til vores spørgsmål.

Og endelig har borgerpanelet så udmøntet arbejdet med elektronisk overvågning i dette slutdokument, som der gennem diskussion er opnået konsensus om.

* * *

Elektronisk overvågning er en sammensat problematik bestående af mange forskellige aspekter som for eksempel videoovervågning af gader, butikker, tank-stationer og transportmidler, overvågning af arbejdspladser, registrering af e-mails og Internet, samt registrering af helbredsoplysninger både i offentligt og privat regi.

Desuden har overvågning mange forskelligartede konsekvenser af både personlig og samfundsmæssig karakter. Der kan være fordele og ulemper ved overvågning og både økonomiske, psykologiske og medmenneskelige relationer kan blive påvirket.

Mange interessemodsætninger er på spil, og der er store økonomiske interesser involveret. Samtidig udvikler overvågningsteknologien sig med stormskridt, hvad der yderligere vanskeliggør et samlet overblik over emnet.

For at strukturere arbejdet har borgerpanelet inddelt emnet i følgende seks arbejds-temaer: "Menneskelige konsekvenser af elektronisk overvågning". "Konsekvenser for samfundet og fællesskabet af elektronisk overvågning". "Fremtid og udvikling". "Retssikkerhed vedrørende elektronisk overvågning". "Registrering og brug af oplysninger om personer". "Overvågning på arbejdspladsen".

Under disse seks arbejdstemaer har borgerpanelet fået eksperternes input. Disse er indgået som værdifuld baggrundsviden i det videre arbejde, der nu foreligger i form af dette slutdokument.

Borgerpanelet vil dog ikke undlade at gøre opmærksom på, at de besvarelser som ekspert-panelet i første omgang gav på vores spørgsmål generelt var af temmelig overordnet karakter. Dette bekræfter vores indtryk af, at elektronisk overvågning, og de problem-stillinger der knytter sig til dette, er meget vanskelige at overskue, hvilket de derfor også må være for politikerne.

Eksperternes vanskeligheder med at give konkrete svar afspejler sig i borgerpanelets slutdokument, hvor det har været svært at give absolutte anbefalinger. Udviklingen kræver, at der hele tiden må følges med rent lovgivningsmæssigt efterhånden som teknologierne bliver udviklet.

Mange af borgerpanelets anbefalinger pointerer derfor vigtigheden af fortsat debat, åbenhed i forvaltningen og den enkelte borgers kontrol med brug af personlige data.

Som almindelige borgere håber vi med dette dokument at bidrage til den videre diskussion og udvikling af politik på området.

## Menneskelige konsekvenser af elektronisk overvågning

**Problemstilling**
Da der tilsyneladende ikke er forsket meget i konsekvenser af elektronisk overvågning, er der ingen klar viden om, hvilken indflydelse det har på os som mennesker.

Når det handler om børn, gælder der nogle helt særlige problemstillinger, fordi de udsættes for en massiv overvågning hvis for eksempel forældre udstyrer børnene med mobiltelefoner, personsøgere med mere for at kunne kontrollere dem. Børn er afhængige af forældres og pædagogers holdning til overvågning indtil de er 15 år. Selvom der er mange børne-organisationer, der beskæftiger sig med børns vilkår, har dette ikke udmøntet sig i nogle generelle retningslinier eller lovgivning, der tager specielt hensyn til børns rettigheder i forhold til overvågning. Børn har altså ikke noget valg for at undgå overvågning for eksempel i institutioner, hvis forældre og pædagoger har vedtaget det.

**Vurdering**
Vi vurderer, at elektronisk overvågning har indflydelse på et menneskes liv. Overvågning har konsekvenser både for det menneske, der bliver overvåget, og for det menneske, der udfører overvågningen. Konsekvenserne er ikke altid synlige, og overvågning kan måske have langtidsvirkninger.

For det menneske, der bliver overvåget, kan konsekvenserne bl.a. være afmagtsfølelse og resignation, der udløses af, at man ikke har mulighed for at fravælge at blive iagttaget. Man kan også føle usikkerhed, fordi man ikke kan overskue, hvorfor man overvåges, og fordi man ikke ved, hvad der sker med billederne og oplysningerne.

Utryghed kan for eksempel vise sig ved, at man tilpasser sin adfærd for at sikre sig, at man ikke kommer under mistanke. Man flytter så at sige ind i et privat og offentligt glashus og udsættes for at blive kigget efter i sømmene. Den sociale kontrol erstattes af en teknisk "gennemlysning" af ens person og handlinger. Man kan miste sin selvrespekt og følelsen af at være et myndigt menneske, fordi andre gives mulighed for at vurdere, om det man gør, er rigtigt eller forkert, eller om det man gør, er godt nok. Der er risiko for, at overvågning mindsker menneskers ansvarsfølelse. Man fokuserer på risikoen for at blive opdaget i stedet for at overveje, om det man gør, er forkert.

Omvendt kan det for den, der overvåger, være ubehageligt at blive pålagt at bedømme andre menneskers forseelser, ligesom det kan blive en belastning at blive pålagt at kontrollere kollegaers elektroniske kommunikation. Når man overvåger, kan man komme i et dilemma, når man skal vurdere, om en forseelse skal forfølges. Det menneske, der overvåger, kan også føle utilstrækkelighed og afmagt, fordi muligheden for at reagere direkte på det, man opdager, ikke nødvendigvis er til stede, hvis man sidder fysisk langt væk.

Videoovervågning kan skabe falsk tryghed, fordi man kan forledes til at tro, at kameraets tilstedeværelse er en beskyttelse i sig selv. Dette kan være tilfældet på togstationer, hvor man kan tro, at der sidder et menneske med mulighed for at handle i tilfælde af, at der for eksempel sker et overfald.

Det er vores vurdering, at det er uheldigt, hvis børn mister muligheden for at have hemmeligheder for de voksne. En massiv brug af overvågning kan forhindre, at børn får mulighed for at lære af egne fejl, uden nødvendigvis at få skældud af de voksne. Når børn overvåges, kan det medføre, at de tilpasser sig det, de ved, at de voksne ønsker, ligesom det kan betyde at de bliver bedømt på andres præmisser. Det kan påvirke deres identitets-dannelse.

Meget overvågning opfylder de voksnes behov for kontrol. Vi vurderer, at meget overvågning i virkeligheden er forældrenes og ikke børnenes behov. Mange forældre er ikke vidende om, at overvågning kan hæmme børns identitetsudvikling, når overvågningen medfører, at børnene føler, at der er restriktioner lige om hjørnet.

**Anbefalinger**

- Der bør generelt rejses en debat, som skaber bevidsthed om, at den elektroniske overvågning ikke i sig selv er en garanti for tryghed, og at overvågning ikke kan erstatte den sociale kontrol.

- Det anbefales, at der laves undersøgelser, der belyser, hvilke psykologiske følgevirkninger elektronisk overvågning har.

- Det anbefales, at der laves undersøgelser, som belyser, hvad der sker med børns identitetsdannelse og øvrige psykologiske udvikling, når de er under elektronisk overvågning.

- Det er panelets indtryk, at ingen af de eksisterende instanser varetager børns rettigheder i forbindelse med lovgivning på dette område. Det bør der rådes bod på. Der er behov for at oplyse og rådgive forældre, institutioner og deres ansatte samt børn, om fordele og ulemper omkring overvågning af børn.

# Overvågningens konsekvenser for samfundet

**Problemstilling**
Hvordan udvikler elektronisk overvågning sig i fremtiden ?
Hvordan kan samfundet styre udviklingen og hvordan kan den enkelte borger sikre sig indflydelse på denne?
Hvordan påvirker elektronisk overvågning samfundet?

**Vurdering**
Fremtiden rummer mange muligheder for øget brug af elektronisk overvågning. På den ene side giver det mange positive muligheder for at lette vores hverdag. På den anden side indeholder det en risiko for en uacceptabel grad af kontrol af borgerne fra myndigheder og private virksomheders side. Denne problemstilling kalder vi "Det digitale dilemma".

Allerede i dag råder teknologi- og kommunikationsvirksomhederne over utroligt mange, endnu ikke udnyttede overvågningsteknologier, ofte forklædt som services. Alt bliver teknisk muligt.

Som eksempler på kommerciel brug af overvågningsteknologi og services kan for øjeblikket nævnes mobiltelefoner med lokationsbestemte services. Mobiltelefonen kan fx henvise til den nærmeste iskiosk. Et andet eksempel er "superproviders" – sammensmeltninger af tele-medie- og finansielle virksomheder, der muliggør samkørsel af kundeoplysninger. Begge dele kan gøre kunderne afhængige af udbyderne, og i meget høj grad gøre kundernes forbrugeradfærd gennemsigtig. Et fremtidigt eksempel kunne være, at man får indopereret en chip i skulderen, så personen er identificerbar, kan overvåges og eksempelvis ikke behøver dankort eller id-kort.

Dette rejser det klassiske spørgsmål om, hvorvidt leverandørerne skaber et nyt behov eller opfylder et eksisterende behov. Den enkeltes personlige og forhåbentligt bevidste forbrugsvalg kan have betydning for, hvilke af de kommercielle overvågningsteknologier, der bliver taget i brug, og hvordan.

Det er tydeligt, at udbredelsen af elektronisk overvågning og den lette tilgængelighed øger presset for at indføre overvågning på flere og flere områder. Når fx en butik indfører videoovervågning, kan man forestille sig, at nærliggende butikker tvinges til at gøre ligeså, for at undgå, at butikstyveri flytter til deres område.

Vores vurdering er, at et stærkt demokrati er essentielt for at kunne styre og kontrollere udviklingen. Herunder er det vigtigt, at borgerne sikres indsigt i den offentlige forvaltning, hvilke informationer myndighederne har om os, og hvad de reelt bliver brugt til. Der må stilles lignende krav til private virksomheder.

Borgerne skal sikres en privat sfære, en urørligheds zone, hvor deres individuelle forskelligheder kan trives, og hvorfra deres demokratiske aktivitet kan tage sit afsæt. Man kan diskutere, hvor grænserne for den private sfære bør gå. Vores vurdering er, at indenfor hjemmets fire vægge er alt privat. Udenfor hjemmet, fx i butikscentre eller på stationer, som alle har adgang til, bør man dog også respektere privatlivets fred.

Et stærkt demokrati bør ikke have kløfter mellem forskellige grupper i befolkningen. Det er vigtigt, at udviklingen indenfor elektronisk overvågning ikke skaber yderligere skel. Hermed mener vi, at der ikke må skabes nye barrierer for den almindelige borgers mulighed for at udøve sine demokratiske rettigheder og pligter.

Man kan frygte, at overvågning forskubber fokus fra reglens begrundelse til kontrol af, om reglen bliver overholdt. Lader man fx være med at stjæle i en videoovervåget butik, fordi man ved, at man bliver opdaget, er fokus flyttet fra det væsentlige: At man skal respektere den private ejendomsret.

Vi vurderer, at etikken bør være med til at sætte grænserne for, hvor langt vi vil gå individuelt og samfundsmæssigt med hensyn til overvågningsteknologi. Derfor er det nødvendigt med en fortsat debat af etiske normer og værdier for anvendelsen af elektronisk overvågning. I debatten er det vigtigt at skelne mellem produktions-overvågning af maskiner og person- og stedovervågning.

Vi vurderer, at debatten som minimum bør omfatte emner som:

- Erstatter overvågning tillid og fællesskab med mistillid og egoisme?
- Skal vi have kontrol i stedet for moral og god opdragelse?
- Fjerner vi de menneskelige relationer og erstatter dem med elektronik, for eksempel et kamera i stedet for en vagt eller kontrollør, en chip i stedet for den menneskelige omsorg, blot fordi det er billigere?
- Hvordan tackler vi spændingsfeltet mellem den krænkende overvågning og den forebyggende overvågning?
- Hvad er det for en type samfund vi vil have?

Vi vurderer, at det er vigtigt, at denne debat bliver ført så bredt som muligt i samfundet.

Vi må konstatere, at en del af den nuværende overvågning er indført uden forudgående folkelig debat. Vi må sikre, at den nye teknologi vurderes inden den indføres - og ikke omvendt. Grænserne for, hvad vi vil acceptere, kan skride, hvis vi ikke træffer bevidste valg om overvågningens formål og teknologiens anvendelse. Det er vigtigt, at vi ikke indfører teknologier, blot fordi de er til rådighed. Vi skal desuden undgå at symptombehandle menneskeskabte problemer ved hjælp af teknologi.
Vi skal være bedre til på forhånd at gennemskue konsekvenserne af at indføre ny teknologi. Der er i dag en tendens til, at fokusere på fordelene. Der mangler derfor en afvejning af fordele og ulemper for både overvågeren og de overvågede.

Overvågningsteknologien udgør i sig selv ikke en trussel. Der må skelnes mellem relevant og overflødig eller krænkende overvågning. Et eksempel på relevant overvågningsteknologi er fotofælder, som afslører fartsyndere, og kun dem. Omvendt kan overvågning af personale og kunder i butikker, der ikke har gjort noget forkert, opleves som krænkende. Sindelagskontrol, hvor man registrerer holdninger i stedet for adfærd, er under alle former uacceptabelt. Et eksempel kunne være registrering af e-mail korrespondance mellem personer af en bestemt politisk observans.

Vi ønsker at blive beskyttet mod overdreven kontrol og overvågning, og vi ønsker selvbestemmelse med hensyn til, hvilken overvågning vi udsættes for. Det enkelte menneske har dog individuelle grænser og dermed individuelt ansvar for at sige fra, når den enkeltes grænse er nået. Vi må acceptere, at nogen, fx i detailhandelen, har et dobbeltsyn på os, som både lovlydige kunder og potentielle butikstyve. Men vi skal ikke gøre den opfattelse til vores egen. Vi skal fastholde tilliden til os selv.

**Anbefalinger**

- For at undgå, at overvågning udvikler sig til en trussel mod individet og samfundet, skal der sikres et stærkt og levende demokrati.

- Det er vigtigt med en løbende etisk debat om, hvilket samfund vi ønsker. Denne debat skal specielt omfatte samfundets grundlæggende værdier. Værdidebatten kan være en rettesnor til at modvirke en udvikling, hvor grænserne for hvilken overvågning vi accepterer, umærkeligt og ubemærket flytter sig.

- Vi anbefaler, at man overalt i samfundet prioriterer omsorg og opdragelse højere end kontrol og overvågning.

- Vi anbefaler bedre oplysning til borgerne om problemerne med sikkerhed i forbindelse med brug af Internet, e-mails og mobiltelefon, om rettigheder til indsigt i persondata, registrering og samkøring jævnfør persondataloven, samt om rettigheder i henhold til øvrig lovgivning om overvågning.

- Vi anbefaler åbenhed i den offentlige forvaltning og gennemsigtighed i private virksomheders aktiviteter indenfor registrering og samkøring.

## Lovgivning og retssikkerhed vedrørende registrering og brug af oplysninger samt elektronisk overvågning

**Problemstilling**
Det har bekymret borgerpanelet, hvorvidt de teknologiske muligheder overhaler lovgivningen på de områder, som vedrører elektronisk overvågning. Hvordan kan man sikre, at lovgivningen er på højde med de forandringer, den teknologiske udvikling medfører. Retssikkerheden på området skal sikres.

Borgerpanelet har desuden interesseret sig for, hvem der har og bør have rettighederne til information og brugen af denne med henblik på at undgå misbrug.

**Vurdering**
I forbindelse med persondataloven må man tage i betragtning, at den retter sig mod et område i rivende udvikling. Vi vurderer, at kendskabet til og forvaltningen af person-dataloven ikke altid er tilstrækkelig i de virksomheder og blandt de myndigheder, der arbejder under ansvar for loven.

Indsamling og registrering af oplysninger må kun ske med saglige formål. Den, der indsamler og/eller registrerer, afgør hvad der er sagligt. I tvivlstilfælde afgør Data-tilsynet, hvad der er saglige formål. Det rejser problemstillingen om, hvad der kan fortolkes som sagligt.

Borgerpanelet er opmærksom på en undtagelse vedrørende informationspligt i person-dataloven om patientdata til forskningsbrug. Undtagelsen betyder, at der kun i særdeles begrænset omfang er pligt til at informere personer, når identificerbare data om dem bruges i forskningsprojekter.

Det er værd at overveje, hvad der kan blive den nedre grænse for, hvilke lovovertrædelser, der kan medføre straf, når man ved hjælp af tv-overvågning kan opdage og dermed straffe flere bagatelagtige lovovertrædelser end før. Vi vurderer, at der foreligger et dilemma i forhold til bagatelagtige lovovertrædelser: Man kan stille spørgsmålstegn ved det rimelige i at bruge resurser på at forfølge alle sådanne lovovertrædelser.

Vi vurderer, at der er huller i lovgivningen om handlepligt, fordi loven er rettet mod andre forhold, end de der eksisterer i dag. Loven blev lavet for at fastlægge en persons handlepligt i forbindelse med fx en trafikulykke, hvor man umiddelbart er tilstede. Nu kan man som følge af muligheden for at opsætte overvågningsudstyr befinde sig langt fra det sted, hvor en forbrydelse eller en ulykke sker. Hvad betyder disse nye forhold for vores handlepligt? Har man en anden slags ansvar?

Den tryghed, overvågning giver, når det anvendes præventivt, rummer også muligheder for krænkelse af den enkelte. Vi vurderer, at den enkeltes retssikkerhed kan krænkes, fordi en omvendt bevisbyrde kunne komme til at gælde. Man ville være skyldig indtil det modsatte var bevist. Man kunne for eksempel komme under mistanke, eller ligefrem blive erklæret skyldig i en forbrydelse, fordi overvågningsteknologi gør det muligt at fastslå ens blotte tilstedeværelse i nærheden af et gerningssted.

Vi vurderer, at der kan der opstå problemer med lovgivningen angående registrering og brug af oplysninger i tilfælde, hvor firmaer lægges sammen over landegrænser. Indenfor EU er medlemslandenes lovgivning relativt ens, men der er store forskelle mellem lovgivningen i EU og lovgivningen i de såkaldte tredje lande som for eksempel USA. Man kan forudse store udfordringer i lovgivningsarbejdet på dette område.

Det ser ud til, at den digitale signatur er på vej. Den kan skabe øget mulighed for, at den enkelte borger kan få sig et bedre overblik over de offentligt registrerede oplysninger. Vi vurderer imidlertid, at den vil kunne medføre, at staten i princippet har øget mulighed for at overvåge borgerens aktiviteter.

Der findes privatlivssikrende teknologi, som proxyservere og lignende, der kan sikre ens anonymitet fx på nettet. Der er tilsyneladende ikke stor efterspørgsel på nuværende tidspunkt. Der savnes en diskussion af, i hvilket omfang samfundet er interesseret i at anvende en sådan teknologi.

Vi vurderer, at udviklingen af de teknologiske muligheder for, hvad vi kan få at vide om vores helbred, vil kunne sætte persondataloven under pres, fx. i forbindelse med

forsikringsselskabers virke. Selskaberne kan forventes at ville gøre brug af disse oplysninger i forbindelse med risikovurdering. Det er derfor vigtigt, at man fastholder gældende praksis om skriftligt samtykke i forbindelse med forsikrings-selskabers indhentning af ens helbredsoplysninger. Vi ser desuden et problem, hvis forsikringsselskaber skal have ret til indblik i personers dna-materiale. Vi finder det vigtigt, at forsikringsselskaberne fortsat ikke kan bruge dna-materiale.

Udviklingen viser, at tele-, medie-, forsikrings-, bank- og kreditvirksomheder samles i store enheder. Man kan formode, at helhedsløsninger, hvor vi tilbydes mange ydelser af samme enhed, bliver almindelige. Man kan forudse et pres på de love, som regulerer brugen og samkøringen af registrerede kundeoplysninger.

**Anbefalinger**

- Når man indfører en ny lovgivning, skal man for eksempel tage samfunds-økonomiske og miljømæssige hensyn. Ud fra vores vurderinger anbefaler vi generelt, at man ligeledes tager et hensyn til, hvad en given lovgivning har af konsekvenser for registrering og brug af oplysninger.

- Persondataloven og andre love som vedrører overvågning bør til stadighed revideres.
- Med hensyn til begrebet saglighed i forbindelse med persondataloven er det vigtigt med åbenhed og debat om Datatilsynets afgørelser om, hvad der er sagligt.

- Vi anbefaler, at de virksomheder og myndigheder, som arbejder under ansvar for persondataloven, får nøjere kendskab til lovens indhold.

- Vi anbefaler et krav om samtykke ved al brug af identificerbare data til forskning.

- Love vedrørende handlepligt bør revideres og føres ajour i forhold til den teknologiske udvikling.

- Opsætning af overvågningsudstyr kan medføre, at den enkeltes retssikkerhed krænkes. Man bør afveje, om den gevinst, der er ved at sætte udstyret op, modsvarer de eventuelle krænkelser den enkelte kan påføres. Vi efterlyser mere debat på dette område.

- Vi anbefaler, at Danmark aktivt arbejder for et større samarbejde om lovgivning i internationalt regi angående registrering og brug af person-oplysninger. Ligeledes anbefaler vi de danske myndigheder at holde et vågent øje med, om international lovgivning på området vil kunne udvande dansk lovgivning, der skal sikre den enkelte borgers integritet.

- Vi anbefaler, at man ved en eventuel indførelse af den digitale signatur tager hensyn til borgerens muligheder for selv at holde øje med sine egne oplysninger.

- Vi anbefaler, at man arbejder på at udbrede kendskabet til og indføring af privatlivssikrende teknologi.

- I forbindelse med det forventede øgede pres på persondataloven angående forsikringsselskabers brug af helbredsoplysninger anbefaler vi, at dette problem følges nøje fra politisk hold og suppleres med en vedvarende etisk debat.

- Ved sammenlægning og fusioner er der mulighed for samkøring af registrerede personoplysninger i stor stil, hvorved der skabes mulighed for massiv og aggressiv markedsføring. Vi anbefaler derfor, at de relevante myndigheder holder øje med, at lovgivningen er gearet til at håndtere dette pres.

## Overvågning på arbejdspladsen

**Problemstilling**
Der er på arbejdsmarkedet uenighed om, hvordan arbejdsmarkedets parter i fællesskab skal forholde sig til elektronisk overvågning på arbejdspladsen. Det handler om flere forhold. Først og fremmest handler det om, at man fra arbejds-giverside mener, at ledelsesretten er rammen for hvordan og hvor meget der overvåges. Medarbejderside fremhæver, at elektronisk overvågning er medvirkende til at skabe utryghed på arbejdspladserne, dels på grund af den direkte påvirkning fra overvågning, og dels fordi spillereglerne vedrørende elektronisk overvågning er uklare.
Vi mener, at disse forhold har en negativ indflydelse på det psykiske arbejdsmiljø, og at dette vil blive et stigende problem i takt med den øgede brug af elektronisk overvågning.

Ovenstående problemstilling omhandler TV - overvågning, scanning og læsning af e-mails, kontrol af internetbrug, herunder downloading og kontinuerlig skærm-aflæsning. Ydermere kan man forestille sig, at der i fremtiden kan ske større udbredelse af kommunikation ved hjælp af videotelefon med mere på arbejdspladsen.

**Vurdering**
For medarbejderen er privatsfæren på arbejdsmarkedet allerede etableret, da det ikke er tilladt automatisk at registrere medarbejderes telefonsamtaler, samt registrere, hvem der ringes til. Da den teknologiske udvikling har medført en ændring af arbejdsgangen og kommunikationen, kan overvejelserne så være, om dette forbud skal udvides til også at gælde scanning og læsning af personlige e-mails med mere Vi vurderer, at hvis dette skal ske, skal der være en klar adskillelse mellem, hvad der er privat kommunikation, og hvad der er en del firmaets dokumentation, der skal arkiveres og skal være tilgængelig for relevante personer i firmaet.

Med hensyn til skærmovervågning af arbejdsgangen skal denne være motiveret af nødvendigheden for opretholdelse af firmaets drift. I hvert tilfælde må overvågnings-løsningen holdes op mod alternative muligheder.

Hjemmearbejdspladsen er en anden problemstilling. Spørgsmålet er, om overvågning af medarbejderes brug af computere her bør accepteres, da arbejdet udføres i det private hjem.

Udviklingen på arbejdsmarkedet, hvor blandt andet postbudes og hjemmehjælperes arbejde overvåges ved hjælp af scannere, rejser en problemstilling om tryghed og tillid, både for ansatte og brugere. Det bør derfor nøje overvejes, hvornår sådanne tiltag er hensigtsmæssige.

Videoovervågningen er nødvendig i visse produktionsmiljøer af hensyn til almindelig sikkerhed for medarbejderne og produktionen. Ved røveritruede virksomheder, såsom pengeinstitutter, posthuse, døgnkiosker og tankstationer, kan der være en kriminalpræventiv virkning. Den kan komme medarbejderne til gode i form af en følelse af øget tryghed, og den kan have betydning for efterforskning og opklaring af en forbrydelse.

Videoovervågning kan være en måde at komme svind til livs på, men det er ikke nødvendigvis den mest effektive. Alternative muligheder kan eksempelvis være inddragelse af medarbejderne i planlægningen af arbejdsgange, virksomhedens fysiske indretning med videre. I forbindelse med overvågning bør betydningen af overvågningsfrie zoner, håndtering af data, placering af kameraer nøje overvejes i samarbejde med de ansatte.

**Anbefalinger**

- For at sikre en korrekt og lovlig opsætning af video anbefaler vi en ordning om statsautorisation af forhandlere og montører af overvågningsudstyr.

- Ved behov for foranstaltninger til forebyggelse af svind på steder, hvor der ikke kommer kunder, for eksempel lager, indlevering og baglokaler, anbefaler vi, at der benyttes andre metoder end videoovervågning i arbejdstiden.

- Vi anbefaler arbejdsmarkedets parter, at de udarbejder et sæt regler på området, som gøres til lov af Folketinget, og dermed er et ufravigeligt udgangspunkt for indførelse og regulering af elektronisk overvågning. Hvis ikke denne mulighed udnyttes af parterne, anbefaler vi, at Folketinget udarbejder lovgivning på området.

- I forbindelse med disse forhandlinger bør betydningen af overvågningsfrie zoner, håndtering af data, placering af kameraer med mere nøje overvejes. I hvert tilfælde må overvågningsløsningen holdes op mod alternative muligheder.

- Vi anbefaler, at hvis der skal ske en begrænsning af virksomhedens mulighed for kontrol af e-mails, skal der være en klar adskillelse mellem, hvad der er privat kommunikation, og hvad der er en del af firmaets dokumentation, der skal arkiveres og være tilgængelig for relevante personer.

# Teknologirådets udgivelser 2000 - 2001

Alle Teknologirådets udgivelser kan læses og hentes gratis fra Rådets hjemmeside, www.tekno.dk

## Rapporter

**Beriget mad – mulighed eller trussel?** Resumé og ekspertindlæg fra konference på Christiansborg den 13. september 2001. Teknologirådets rapporter 2001/7.

**Det aldrende samfund – grund til bekymring?** Resumé og redigeret udskrift af høring i Folketinget den 20. april 2001. Teknologirådets rapporter 2001/6.

**Biobrændsel og transportsektoren.** Resumé og redigeret udskrift af høring for Folketinget 2. maj 2001. Teknologirådets rapporter 2001/5.

**Trafik og kørselsafgifter.** Konsensuskonference afholdt af Teknologirådet i samarbejde med Transportrådet. Teknologirådets rapporter 2001/4.

**Erfaringer fra statslige IT-projekter – hvordan gør man det bedre?** Rapport og anbefalinger fra en arbejdsgruppe under Teknologirådet. Teknologirådets rapporter 2001/3.

**Unge og Rusmidler.** Resumé og redigeret udskrift af høring for Folketinget den 24. januar 2001. Teknologirådets rapporter 2001/2.

**Kloning til behandling.** Resumé og redigeret udskrift af høring for Folketinget den 22. november 2000. Teknologirådets rapporter 2001/1.

**Industriens brug af kemikalier – oplæg til strategisk sporskifte i den politiske indsats**. Teknologirådets rapporter 2000/10.

**Overvågning.** Slutdokument og ekspertindlæg fra konsensuskonferencen 17.-20. november 2000. Teknologirådet 2000/9.

**Terapeutisk Kloning.** Resumé og redigeret udskrift af høring i Folketinget den 22. november 2000. Teknologirådet 2000/8.

**Allergi.** Handlingsplan for forebyggelse af overfølsomhed og allergiske sygdomme i Danmark 2001-2005. Teknologirådets rapporter 2000/7.

**Støj og teknologi**. Slutdokument og ekspertindlæg fra konsensuskonferencen 12. - 15. maj 2000. Teknologirådet 2000/6.

**Byøkologi**. Resumé og redigeret udskrift af høring i Folketinget den 29. maj 2000. Teknologirådet 2000/5.

**Kommunen på nettet**. Rapport fra projektet om elektronisk selvbetjening i det offentlige oktober 1999- april 2000. Teknologirådets rapporter 2000/04.

**Gensplejsede fødevarer**. Udskrift af oplægsholdernes manuskripter fra konferencen om gensplejsede fødevarer på Christiansborg den. 4 april, 2000. Teknologirådet 2000/03.

**Xenotransplantation**. Resumé og redigeret udskrift af høring i Folketinget den 23.februar 2000. Teknologirådet 2000/02.

**Fremtidens TV og Radio**. Resumé og redigeret udskrift af høring i Folketinget den 1. februar 2000. Teknologirådet 2000/01.

**Den digitale doktor** – om IT-anvendelse i praksissektoren. Debatoplæg. Teknologirådet 2000/nov.

**EUROPTA** - European Participatory Technology Assessment. Participatory Methods in Technology Assessment and Technology Decision-Making. Rapport. Teknologirådet 2000.

## Nyhedsbrevet fra Rådet til Tinget

Nr.164 11/01: Stejl debat om beriget mad
Nr.163 10/01: Udstøder teknologien ældre?
Nr.162 10/01: Kroppen som identifikation
Nr.161 10/01: Open Source Software er ikke slået igennem
Nr.160 09/01: Styr på medicinsk udstyr?
Nr.159 09/01: Dyr biobrændsel til transport
Nr.158 07/01: Betal med mobiltelefonen
Nr.157 05/01: GMO-debat i krydsild
Nr.156 05/01: Mening med road pricing?
Nr.155 03/01: Fare for nye IT-fiaskoer
Nr.154 03/01: Kemi: Stop fodslæberi
Nr.153 03/01: Huse med eget elværk
Nr.152 02/01: Behov for stamcelle-politik
Nr.151 01/01: Vækst, Gener og Open Source
Nr.150 12/00: Overvågning på glidebane
Nr.149 11/00: Færre bøvser - bedre klima
Nr.148 11/00: Det usikre kulstofkredsløb
Nr.147 11/00: Mere frugtbar jord - mindre drivhuseffekt
Nr.146 11/00: Huller I kyotoaftalen
Nr.145 11/00: Kyotoaftalen vakler
Nr.144 11/00: Kickstart til allergi-indsatsen

Nr.143 11/00: Lette miljøgevinster overses
Nr.142 08/00: Fire bud på IT-sikkerhed
Nr.141 08/00: Xenotransplantation
Nr.140 08/00: Alternativer til kloning.
Nr.139 08/00: Usikre gevinster for net-kommuner (også oversat til engelsk)
Nr.138 07/00: Staten bør satse på byøkologi
Nr.137 06/00: Schh... du larmer - om Teknologirådets projekt om støj (også oversat til engelsk)
Nr.136 05/00: Gensplejsede fødevarer
Nr.135 05/00: Xenotransplantation
Nr.134 01/00: Danmark eksporterer miljøproblemer til udviklingslande

## BIOSAM informerer

BIOSAM nr.4 01/00: Organ-grise - Risici, regler og realisering
BIOSAM nr.5 06/01: Fire års kloningsdebat

## Teknologidebat

TD 4/2001 – Bæredygtigt forbrug?
TD 3/2001 – Uhmmm, vitaminer
TD 2/2001 – Fremtidens undervisning
TD 1/2001 – Digitale dialoger/ Årsberetning 2000
TD 4/2000 – Atjuu, allergien er over os
TD 3/2000 – Schhh, du larmer!
TD 2/2000 – Fremtidsbilleder/ Årsberetning 1999
TD 1/2000 – Den digitale doktor