Elektronisk overvågning

Slutdokument og ekspertindlæg fra konsensuskonference
den 17.- 20. november 2000

Teknologirådets rapporter 2000/9

Elektronisk overvågning

Borgerpanelets spørgsmål og slutdokument samt udskrift af oplægsholdernes manuskripter ved konsensuskonferencen på Christiansborg den 17., 18. og 20. november 2000

Projektledelse i Teknologirådets sekretariat:
Søren Gram

Projektmedarbejder:
Anne Weber

Omslag: Camilla Hjerl, Selle 16
Tryk: Vester Kopi

ISBN: 87-90221-52-4
ISSN: 1395-7392

Rapporten bestilles hos

Teknologirådet
Antonigade 4
1106 København K
Telefon 33 32 05 03
Fax 33 91 0509
E-mail tekno@tekno.dk

Rapporten findes også på Teknologirådets hjemmeside www.tekno.dk

Du kan desuden downloade det introduktionsmateriale, som journalist Peter Hesseldahl har skrevet til borgerpanelet på www.tekno.dk

Teknologirådets rapporter 2000/9

Forord

Overvågning på arbejdspladsen, overvågning i butikkerne, overvågning af daginstitutionen, overvågning ved brug af internet, mobiltelefon og dankort, overvågning på gader, tankstationer og i busser, osv. osv. Med den hastige udbredelse af elektronisk overvågning er der i stigende grad behov for en samlet vurdering af overvågningsteknologiens muligheder og konsekvenser for den enkelte borger og for samfundet.

Hvilke problemer kan overvågningsteknologien løse og hvilke skaber den? Hvor langt er vi som samfund parate til at gå i brugen af overvågningsteknologi? Hvordan kan vi forvente, at udviklingen former sig, og hvor vidt vil den føre os? Det er nogle af de spørgsmål Teknologirådet satte fokus på ved en konsensuskonference om elektronisk overvågning, der blev afholdt på Christiansborg den 17., 18., og 20. november 2000.

Hvornår oplever den enkelte borger elektronisk overvågning som tryghedsskabende, og hvornår overskrides en personlig grænse, så overvågning i stedet giver den enkelte utryghed? Sådanne spørgsmål kan hverken eksperter eller politikere besvare fyldestgørende. Derfor har Teknologirådet spurgt et borgerpanel til råds.

Konsensuskonferencer er en af Teknologirådets metoder, der har borgerinddragelse i højsædet. Konsensuskonferencens overordnede mål er at bygge bro mellem borgere, eksperter og politikere, og at bidrage til at styrke en åben, offentlig og demokratisk debat i samfundet.

Et borgerpanel har på to forberedelsesweekender i efteråret 2000 forberedt en række spørgsmål om elektronisk overvågning; spørgsmål som de inviterede eksperter søgte at besvare på konferensen. På baggrund af eksperternes svar, har borgerpanelet debatteret emnet og opnået konsensus om en række anbefalinger til politikerne. Borgernes stillingtagen og anbefalinger udgør det slutdokument, du finder i denne rapport. Rapporten indeholder også en udskrift af eksperternes indledende oplæg på konferencen.

Konsensuskonferencen om elektronisk overvågning blev tilrettelagt i et samarbejde mellem Teknologirådet og en planlægningsgruppe bestående af:

Peter Christensen, PROSA
Jacob Lyngsø, IT-Brancheforeningen
Peter Blume, Københavns Universitet, Det Retsvidenskabelige Institut
Lars Barfoed, Finansrådet
Jean Fischer, Roskilde Universitetscenter

Desuden deltog Carl Christian Larsen som proceskonsulent for borgerpanelet og ordstyrer på konferencen.

Teknologirådet vil gerne benytte lejligheden til at takke alle involverede for samarbejdet.

Teknologirådet, december 2000
Søren Gram
Projektleder

Indholdsfortegnelse

Borgerpanelets slutdokument

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

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 planlægningsgruppe 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, tankstationer 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 arbejdstemaer: "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 ekspertpanelet i første omgang gav på vores spørgsmål generelt var af temmelig overordnet karakter. Dette bekræfter vores indtryk af, at elektronisk overvågning, og de problemstillinger 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 børneorganisationer, 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 identitetsdannelse.

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 produktionsovervågning 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 persondataloven 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 Datatilsynet, hvad der er saglige formål. Det rejser problemstillingen om, hvad der kan fortolkes som sagligt.

Borgerpanelet er opmærksom på en undtagelse vedrørende informationspligt i persondataloven 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 proxy-servere 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 forsikringsselskabers 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 samfundsøkonomiske 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 personoplysninger. 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 arbejdsgiverside 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 skærmaflæsning. 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 overvågningsløsningen 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 overvågningsfri 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.

Borgerpanelets spørgsmål til eksperter

1. Menneskelige konsekvenser af elektronisk overvågning

a) Hvad er konsekvenserne for børn og voksne ved forskellige typer af elektronisk overvågning?
b) Hvilke psykologiske konsekvenser har elektronisk overvågning?
- Hvordan påvirker elektronisk overvågning børns udvikling og identitetsdannelse ?
- Findes der undersøgelser der belyser hvordan voksnes adfærd og psyke påvirkes af overvågning (ved videoovervågning, brug af internet, kreditkort mm.)?

2. Konsekvenser for samfundet og fællesskabet af elektronisk overvågning?

Hvordan påvirker elektronisk overvågning samfundet/fællesskabet og hvilke konsekvenser har denne påvirkning?
- Hvordan påvirker elektronisk registrering af virkeligheden vores ansvarsfølelse og sociale normer – herunder hvordan påvirkes relationer indenfor familien og mellem familien og samfundet?
- Hvordan forbereder vi os til at leve i en virkelighed med registrering og elektronisk overvågning?
- Hvilke forhold ved indførsel af elektronisk overvågning bør vægtes højere end økonomi (i for eksempel sundheds- og socialsektoren)?
- Er overvågning symptombehandling?

3. Fremtid og udvikling

Hvordan udvikler elektronisk overvågning sig i fremtiden, og hvordan kan samfundet styre denne udvikling?
- Hvad er skrækvisionen, og hvad er drømmevisionen?
- Hvilke muligheder åbner teknologien for elektronisk overvågning indenfor de næste fem år?
- Hvad er producentens rolle i udviklingen?
- Har brugen af elektronisk overvågning en selvforstærkende effekt?
- Hvordan kan individet/samfundet overskue og styre udviklingen?

4. Retssikkerhed vedrørende elektronisk overvågning

Hvordan sikres at lovgivningen og administrationen er på højde med udviklingen, således at det enkelte menneskes retssikkerhed tilgodeses?

- Hvordan forhindres misbrug af oplysninger indsamlet uden noget umiddelbart formål (elektroniske spor)?
- Hvilke muligheder er der for at regulere og kontrollere registrering af elektronisk indsamlede oplysninger, opbevaring af dem, kommerciel udnyttelse og samkøring af disse?
- Hvilket behov vil der være for at regulere lovgivningen, når selv "bagatelagtige" lovovertrædelser opdages?
- Hvis elektronisk overvågning skaber en forventning om forøget sikkerhed for de overvågede (fx på plejehjem), medfører det så nogle særlige ansvarsmæssige forhold for dén hvis den hvis job det er at overvåge?
- I hvilket omfang samarbejdes der omkring national og international lovgivning (fx i EU, OECD, FN) i forbindelse med elektronisk overvågning, og hvad betyder det for dansk lovgivning?
- Er der særlige retsmæssige forhold der gælder for elektronisk registrering af børn?

5. Registrering og brug af oplysninger om personer

a) Hvem har og hvem bør have rettighederne til information og brugen af denne?

- Hvor meget ved private virksomheder og offentlige myndigheder og hvad bruger de det til – nu og i fremtiden?
- Hvad kan forsikringsselskaber få adgang til og registrere nu og i fremtiden?
- Hvad kan sundhedssektoren få adgang til og registrere nu og i fremtiden?
- Hvor langt er det offentlige fremme med hensyn til digital signatur?
- Hvad sker der med registrerede personlige oplysninger når offentlige og halv-offentlige institutioner bliver privatiserede/udliciterede?

b) Er der en grænse mellem personlig frihed og fælles bedste?

- Hvilke konkrete muligheder er der nu og bør der være for at privatpersoner kan kontrollere brugen af deres personlige oplysninger?
- Hvor lidt registrering har samfundet brug for, for at kunne opretholdes?
- Hvor meget registrering kan samfundet bære og stadig være et demokrati?

6. Overvågning på arbejdspladsen

Hvilke fordele og ulemper er der ved elektronisk overvågning af mennesker på en arbejdsplads?

- Hvad er fagforeningernes og arbejdsgiverne holdning til overvågning af medarbejdere?
- Hvad er formålet med elektronisk overvågning på arbejdspladsen?
- Hvilke problemer ser fagforeningen og arbejdsgiveren?
- Hvilke løsninger ser arbejdsgiveren og fagforeningen?

Udskrift af ekspertoplæg

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, Højvangsseminaret
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

Tema 1: Menneskelige konsekvenser af elektronisk overvågning

Oluf Jørgensen, Afdelingsforstander i informationsret, Danmarks Journalisthøjskole

Spørgsmål:
Hvad er konsekvenserne for børn og voksne ved forskellige typer af elektronisk overvågning?

"Der har altid været kontrol. Tidligere dominerede den uformelle kontrol. Den er indbygget i socialt samvær og virker mellem folk, der mødes ansigt til ansigt. Den er stadig vigtig, men i det moderne samfund er megen kontrol kommet på distance og bygger på persondata.

Persondata er blevet anvendt længe før IT. Der kræves persondata ved patientbehandling, skatteopkrævning, tildeling af sociale ydelser, fakturering og betaling, politimæssig efterforskning m.v. IT-anvendelse betyder ikke principielle ændringer, så længe anvendelsen handler om bestemte persondata, fx ved konkret mistanke om fejl eller ulovlighed. IT betyder blot, at arbejdet kan gøres meget hurtigere.

IT giver muligheder for nye former for kontrol. Kontrollen kan fx rettes mod al færdsel eller al kommunikation på et område. Masseoplysninger kan sammenkobles for at opspore mulige, hidtil ukendte fejl og ulovligheder. Kontrollen bliver mere finmasket og effektiv. Kontrollen får dermed karakter af overvågning". (Kilde: "Persondataret" af Oluf Jørgensen, Systime, november 2000).

Udtrykket Store Bror ser dig, stammer fra Orwells roman 1984. Den beskriver et samfund, hvor magthaverne eller "systemet" overvåger næsten enhver aktivitet. Store Bror- billedet passer på visse typer overvågning i dagens samfund. Andre billeder passer bedre på andre typer overvågning: Lille Bror, Den Søde Søster, Den Økonomiske Far og Den Bekymrede Mor.
Visse former for elektronisk overvågning i dagens samfund har karakter af Store Bror-overvågning. Det gælder formentlig efterretningsvæsenernes overvågning. Vi ved utrolig lidt om den. Hvis formodningerne om efterretningsvæseners globale overvågning af elektronisk kommunikation (Echelon) holder stik, så ser Store Bror næsten alt. Andre overvågninger hører hjemme i samme kategori, fx visse arbejdsgivere, der som daglig rutine tjekker, hvad de ansatte foretager sig ved computerne. Det gør tre af fire amerikanske arbejdsgivere oplyser FTFs blad Fællesrådet.

Samkøring af registre for at opspore økonomiske ulovligheder kan minde om Store Bror, men i dagens samfund er denne type overvågning meget mere afgrænset. Det samme er politiets overvågning ved konkret efterforskning, og forretningers overvågning af butikslokaler. Denne afgrænsede overvågning kalder jeg Lille Bror-overvågning.
Den Søde Søsters overvågning har en anden karakter. Den er omklamrende og klistret. Et godt eksempel på denne type overvågning er kategorisering af borgerne i særlige

livsstilsgrupper eller interessegrupper med henblik på direkte markedsføring. Kære Caroline. Vi er glade for at kunne give nogle særlige tilbud til dig. I den direkte markedsføring camoufleres reklamen som en personlig henvendelse. Den søde søster kan også opleves i omsorgs-, social- og sundhedssektoren. Det er nok et spørgsmål om tid, før den søde søster også her vil bruge elektronisk overvågning som basis for tilbud om forbedring af livskvaliteten.

Den Økonomiske Far benytter overvågning for styrke indtjening og minimere tab. Forretninger vil ikke tage unødvendige risici ved kreditgivning. Derfor tjekker de kundens kreditværdighed. Pengeinstitutter danner sig et overblik over kunders økonomiske stabilitet. Forsikringsselskaber danner sig et overblik over kunders skadesrisici. Den Bekymrede Mor benytter overvågning for at passe på. Der kan ske indbrud i hjemmet. Der kan ske overfald på torve og pladser. Der kan være arvelige sygdomme i familien. Måske kan vi forebygge ulykker og sygdom. Hellere tage én gentest for meget end én for lidt, vil den bekymrede Mor tænke om nogle år.

Elektronisk overvågning er indbygget i daglige rutiner ved arbejde, indkøb, færdsel mv. Den er ofte usynlig - kontrollanterne er anonyme og på lang afstand. De fleste mærker ikke overvågningen direkte. Maskeringen fuldføres i sproget. Der tales typisk ikke om kontrol og overvågning, men om sikkerhed, kvalitetsudvikling, varetagelse af kundernes interesser, coaching af medarbejdere mv.

Maskeringen slører, men ændrer ikke ved realiteterne. Elektronisk overvågning har konsekvenser.

Store Bror-overvågning betyder sikkert, at terrorister ikke bruger elektronisk kommunikation. Om der er andre virkninger, ved jeg ikke. Overvågning på arbejdspladsen: Ved klare meldinger vil ansatte indrette sig og undlade uønsket computerbrug. Ved uklare meldinger skabes usikkerhed og stress.

Lille Bror-overvågning afslører nogle ulovligheder. Ved klare forhåndsinformation forebygges ulovligheder.
Den søde søster skaber afhængighed for nogle. Eller med andre ord: Den søde søster klistrer.
Den Økonomiske Far har kontante virkninger. Nogle får kredit, andre får ikke. Nogle kan tegne forsikring, andre kan ikke eller må betale mere.
Den Bekymrede Mor-overvågning betyder måske, at nogle sygdomme og ulykker undgås. Noget kriminalitet flytter til områder, der ikke er overvåget. Generelt set vokser bekymringerne. Den Bekymrede Mor bygger på bekymring, men giver samtidig grund til mere bekymring.
Generelt set kan overvågning true det enkelte menneskes integritet. Personlig integritet handler om styrke og muligheder til at være sig selv og bestemme over egne forhold. Retten til at bestemme over egne data er et vigtigt element. Den personlige integritet svækkes, når myndigheder og forretninger overvåger og disponerer over borgerens data, uden at informere og uden at spørge. Borgerens selvbestemmelsesret kan aldrig være absolut, men jo mere styr borgeren har på egne data, desto stærkere er den personlige integritet.
Personlig integritet betyder ikke, at den enkelte borger skal bygge en mur om sit privatliv. Det er værdifuldt og livsnødvendigt for det enkelte menneske at have samvær med andre

og dele sine glæder og sorger. Det er også værdifuldt og nødvendigt at have kontakter med myndigheder, forretninger, foreninger mv. Respekt for den personlige integritet betyder, at det enkelte menneske selv må tage stilling til, hvem han vil dele sit liv med.
Alle mennesker har ret til beskyttelse. Børn har også rettigheder, der kan krænkes af overvågning. Hensynet til den personlige integritet kan ikke varetages på samme måde for børn som for voksne. Børn skal have en vis alder og modenhed, før de selv kan tage vare på egne interesser. En ung, der er fyldt 15 år, kan selv råde over egne persondata. For børn og unge under 15 år, må forældrene som hovedregel tage stilling.. Forældre har ansvaret for beskyttelsen af deres børn. Hvis forældrene groft misrøgter dette ansvar, må sociale myndigheder gribe ind.

Persondataloven giver vigtige rettigheder til borgerne. Det er afgørende for beskyttelsen af den personlige integritet, at loven ikke kun bliver en vedtagelse på et stykke papir, men at den også bliver en del af virkeligheden.

Kim Rasmussen, Kultursociolog og forskningslektor, Center for institutionsforskning, Højvangsseminariet

Spørgsmål:
- Hvordan påvirker elektronisk overvågning børns udvikling og identitetsdannelse?
- Findes der undersøgelser der belyser hvordan voksnes adfærd og psyke påvirkes af overvågning (ved videoovervågning, brug af internet, kreditkort mm.)?
- Hvilke psykologiske konsekvenser har elektronisk overvågning?

Det korte svar - der omfatter begge spørgsmål - er, at der mig bekendt **ikke** er lavet undersøgelser herhjemme, der kan svare på spørgsmålene.
Jeg har i det mindste ikke fundet sådanne i de databaser, hvor jeg har søgt
eller hørt sådanne refereret blandt de bibliotekarer og kollegaer jeg har talt med.

Dette kan jo undre. Hvordan kan det gå til, at vi ved så lidt om de menneskelige konsekvenser, når man tænker på, hvor omfattende den elektroniske overvågning efterhånden er blevet?

For vi er jo alle overvågede, - på posthuset, i banken, på togstationen, i taxaen, i centret, som internetbrugere, som e-mail-afsendere, osv.

og vi overvåger selv fra tid til anden, - fx. gennem TV, hvor fx "skjult kamera" vækker latter, hvor "docusoaps" kalder på nyfigenhed, eller gennem web-kameraer, via tlf./mobil-tlf. osv.

Når der ikke kan refereres til danske undersøgelser, **betyder det så, at der ikke kan siges noget** om forholdet mellem overvågning, og hvordan overvågning indvirker på det enkelte menneskes psyke?

Nej. Det er min opfattelse, at der ud fra bestemte forudsætninger, godt kan siges noget alment og generelt om psykologiske konsekvenser. Samtidig vil jeg understrege, at der med **psykologisk ,** primært tænkes på, hvad vi **føler** og hvad vi **tænker, når vi oplever overvågning,** og at konsekvenser ikke må forstås alt for simpelt som et årsag-virknings forhold, hvor mennesket reagerer mekanisk og passivt på overvågning.

For det første: Vi kan **alle bidrage til at beskrive og fortælle om overvågnings-fænomenet** og dets virkning på os, fordi det ikke er et snævert afgrænset og specielt fænomen, som kun få har oplevet, men et fænomen, der findes bredt og alment.

For det andet: Der er ingen grund til specielt at skelne mellem børn og voksne i denne sag. **Børns følelser og oplevelser adskiller sig ikke væsentligt fra voksnes**, hvad angår, at blive overvåget og observeret,
eller hvilke dilemmaer man kan komme i, hvis andre konfronterer én med deres observation.

Hvad der er anderledes er, at hvor de voksne kan sige fra, når de overvåges på arbejdspladsen eller andre steder, dér er børnene uden egentlige midler til at kæmpe imod.
Da børn i dag ikke befinder sig på gader og veje, men er afleveret i børneinstitutioner og tilbringer en stor del af dagen på et ofte ret begrænset område, der ikke er særlig svært at overvåge, så er de tvunget til at lade sig overvåge:
- nogle endda dobbelt-overvåge: dels nærovervåget af pædagogerne, dels fjernovervåget af forældre og andre, hvis det bliver en udbredt tendens at anbringe web-kameraer i børneinstitutioner.

For det tredje kendes overvågningsfænomenet fra alment accepterede teorier **om social kontrol.** Det er min opfattelse, at man **til en vis grad** godt kan **overføre denne viden** på fænomenet: elektronisk overvågning. Blot man husker at teori er teori, og ikke forveksler virkelighedens og psykens komplicerede verden med teoriernes forenklinger.

Hvad kan der så siges, mere alment teoretisk om de menneskelige og psykologiske konsekvenser?

1) For det første:
Overvågning - også elektronisk overvågning - er **relationsmæssigt fænomen og bz-polært fænomen**. Der er altså **mindst to parter i spillet.**

En der overvåger	**og**	**en der bliver overvåget.**
(en aktiv part)		(en tilsyneladende passiv part)

De fleste er tilbøjelige til at tænke sig ind i den overvågede parts situation, - måske fordi de fleste af os af egen erfaring bedst kender til denne side.

Men: Der er **psykologi i "begge ender"** af overvågningsfænomenet,
og
der er **psykologi i "spillet" mellem de to parter** .

Overvågning har konsekvenser for begge parter.

Den der overvåger:	**Den der bliver overvåget**:
kan føle sig magtfuld,	Kan føle sig afmagtsfuld,
kan føle man har kontrol,	Kan føle man ikke har kontrol
kan føle man ser og registrerer det man gerne vil se,	Kan føle sig observeret, Kan fortrænge det eller gøre modstand

Sådan vil det almindeligvis være,
- både når overvågningen foregår, så man synligt kan se og observere hinanden - ansigt til ansigt. Men også ved anonym elektronisk overvågning, gælder dette.

Og dog - tingene kan hurtigt vendes om: bankrøverne gemmer sig bag briller, strømper og hætter,

og voldmændene kan begå deres overfald på de overvågede toiletter, ved at dække kamera-erne til. Når det sker, hvem er det da, der er magtfulde og hvem er det da der er afmagtsfulde?

Ved **elektronisk overvågning gøres overvågningsrelationen automatisk og upersonlig**. Der indskyder sig noget, imellem den der overvåger og den overvågede.
Overvågerens ansigt bliver anonymt, upersonligt, følelsesløst, - magten bliver ansigtsløs,

Den overvågede kan gøre sig abstrakte fantasier om overvågeren,
- hvorfor bliver man overvåget?
- hvor meget overvåges?
- hvad kan ses og registreres?
- hvad skal det bruges til?
- har man ret til det?
- kan man ikke slippe for det? osv. osv.

I visse sammenhænge kan man føle det stærkt ubehageligt med **den elektroniske overvågnings tavse og utrættelige observerende linse**,
I andre kan man måske føle sig mindre presset, mindre tynget, mindre overvåget, end hvis det var en person, der holdt én under observation, - også selvom man reelt måske er mere registreret og overvåget, fordi overvågningen kan zoomes, oplagres, genses osv.

De psykologiske konsekvenser **blandt de overvågede** kan spænde **fra:**

de afmagtsfølelser, og de tilpasningstanker, der ligger i spørgsmålet: Jamen, hvis man ikke har noget at skjule, hvad så?

og **til konsekvenser såsom**: vrede, frustration, indignation, aktiv modstand, aktiv modhandlen. For de overvågede er ikke altid passive.

Men også hos **de der overvåger**, kan de psykologiske konsekvenser varierer:
- alle der har lavet observationsstudier af menneskelige relationer vil vide, at det er særdeles anstrengende at overvåge og observere over længere tid.

Der er altså tale om psykologiske konsekvenser i begge ender af overvågningsrelationen.

Der er også tale om lidt forskellige konsekvenser afhængig af overvågningens form:
om den foregår direkte mellem mennesker, i kontakt med hinanden eller om den er elektronisk,

2) Det andet almene, der kan siges om de psykologiske konsekvenser af elektronisk overvågning er, at konsekvenserne **afhænger af i hvilken sammenhæng overvågningen optræder**.
Her tænker jeg ikke kun på hvilket sted den foregår (fx. om det er på offentligt område eller privat), men også på hvilke behov, der ligger til grund, og hvilke erfaringer de implicerede parter gør.

- de psykologiske konsekvenser af ikke at blive overvåget, når man er syg, kan være fatale for såvel den syge, som for de, der har ansvar for at drage omsorg for den syge.
Den syge kan føle, at ens sygdom ikke bliver taget alvorligt nok,
at de professionelle ikke bekymrer sig nok om en.
De ansvarlige kan ved svigtende overvågning med rette bebrejdes for ikke at overvåge godt nok.

- de psykologiske konsekvenser af ikke at blive overvåget, når man er gammel og svag, eller når man er stærkt handicappet eller stærkt udviklingshæmmet - kan være, at man lever i stor angst og evige bekymringer. Og ved svigt kan de ansvarlige og de pårørende komme ud i samvittighedskvaler, selvbebrejdelse o.lign.

- de psykologiske konsekvenser af ikke at overvåge industri-spildevand, salmonella, gift og kemikalie-depoter, grundvandet, osv. kan blive fatalt for os alle, fordi vi kan blive truet på vores helbred. Og de ansvarlige/ overvågerne kan med rette føle og tænke, at de har svigtet deres ansvar og pligt.

Måske kan man sige det sådan: **når man selv har valgt at ville overvåges**,
fordi man eksempelvis er syg,
fordi man er eksempelvis er gammel,
da kan det have meget negative psykologiske konsekvenser **ikke** at blive overvåge. Men samtidig kan overvågningsteknologien også skabe en falsk tryghedsfølelse, hvis man stoler for meget på den.

Derfor må overvågningsfænomenet og overvågningsteknologien vurderes ud fra den konkrete sammenhæng, den altid vil indgå i. Ellers risikerer man, at diskussionen bliver for abstrakt og for almen.

Teknologi - såvel som overvågningsteknologi , er ikke noget entydigt, men har altid flere facetter. Det er i høj grad den konkrete sammenhæng og de konkrete omstændigheder, der afgør konsekvenserne.

3. Det sidste jeg vil sige noget om og inddrage, **drejer sig om video-overvågning af børn og børneinstitutioner.**

Her er der altså tale om en helt konkret og specifik sammenhæng. Dette fænomen findes mange steder i USA, og er også kommet her til landet.

Her er tale om en udvikling, der endnu ikke er kommet ret langt, men som måske vil blive mere udbredt som årene går og de nye teknologiske muligheder byder sig til og børnehaver i udlicitation bliver til service-varer, der skal sælges til forældrene, idet de samtidig søger at dække forældrenes behov på moderigtigt vis.

Hvad er de psykologiske konsekvenser af dette fænomen?
Vi ved det ikke, for det er ikke undersøgt.

Det rejser dog både nogle etiske spørgsmål og nogle demokratiske:
Har børnene ingen ret til privathed, når de er i institution?
Har børn ingen ret til at være medbestemmende om deres eget liv i børneinstitutionen?

Hvem har ret til at bestemme, at der skal video-overvåges i børnehaven?

I relation til psykologien, kan vi antage:

- at forældrene **der overvåger**, føler:
at deres behov for at vide,
at deres barn har det godt, bliver opfyldt

- at de får indsigt i barnets institutionsliv

at de der fjern-overvåges :
nærovervågerne / pædagogerne
- fortrænger deres viden om, at de principielt er under konstant opsyn,
og at **børnene** kun sporadisk er opmærksomme på overvågningen

- at forældrene føler, at de forstår, det de ser,
- at børnene kun momentvis vil være opmærksomme på at de overvåges, indtil de gentage gange bliver konfronteret med beskrivelser af det, forældrene mener at have set
- Dernæst kan børnene begynde at blive i tvivl om deres egen oplevelse, de kan føle sig misforstået, mistroet, usikre,
- De kan miste deres selvtillid, hvis deres egne oplevelser betvivles eller afvises

Men får forældrene da ikke indblik i børnenes liv? Ikke efter min opfattelse.

Lad mig afslutningsvis give et eksempel, der kan illustrere, lidt af det, der er på spil, når voksne ser noget andet, end det børn ser. Eksemplet er hentet fra en undersøgelse, jeg selv og min kollega Søren Smidt har lavet, om hvad unge omkring 18-20 års alderen husker, når de tænker tilbage på deres tid i børnehave: En ung kvinde fortæller:

"Jeg kan huske en dag, hvor Jens og jeg børstede tænder sammen. Jeg kom til at tabe min tandbørste ned i toilettet, og jeg blev så ulykkelig, for jeg var så bange for at få skæld ud. Men Jens blev min redning. Han dykkede hele armen ned efter den, og så blev jeg glad igen. Men i det samme kom pædagogen forbi ude på gangen, og så det. Så fik vi begge en skideballe for at lege med toilettet. Vi blev sat på en stol, og måtte først rejse os fra stolen, når de voksne sagde til".

Eksemplet viser noget om forskellen på, hvad børns oplever, og hvad voksne ser.
Eksemplet viser også, at sporene efter voksnes fejlagtige fortolkning er blivende.
Det er sådanne konsekvenser, man bl.a. kan frygte med fjernovervågning.

Med video-overvågning af børns liv i børneinstitutioner, er der tale om et voldsomt indgreb indført uden demokratisk debat, og uden at børnene umiddelbart kan sætte sig imod det. Samtidig risikerer man, at dette skridt vil være med til, at børn opfatter det som almindeligt og selvfølgeligt at blive overvåget.
Med indføring af videoovervågning i børneinstitutioner sættes konceptet for moderne børnepasning og forældrenes behov OVER børns ret til at blive betragtet som mennesker i egen ret, og med ret til at blive hørt og forstået på egne præmisser.

Hvad der her er sagt om de psykologiske konsekvenser ved elektronisk overvågning, er sagt på et overvejende alment teoretisk og ikke særlig præcist grundlag. Dette gør det kun så meget mere påkrævet, at overvågningsfænomenet og dets konsekvenser undersøges og udforskes mere specifikt.
Tak for ordet.

Tema 2: Konsekvenser for samfundet og fællesskabet af elektronisk overvågning

Linda Nielsen, Københavns Universitet, Retsvidenskabeligt institut C

Spørgsmål:
- Hvordan påvirker elektronisk registrering af virkeligheden vores ansvarsfølelse og sociale normer - herunder hvordan påvirkes private relationer indenfor familien og mellem familien og samfundet?
- Hvilke forhold ved indførsel af elektronisk overvågning bør vægtes højere end økonomi (i for eksempel sundheds - og symptombehandling)?
- Er overvågning symptombehandling?

INDLEDNING

Det er vanskeligt at behandle hele det store og forskelligartede område, som elektronisk overvågning og elektronisk registrering af virkeligheden dækker over, som ét samlet spørgsmål. Derfor fokuseres i det følgende på tre centrale problemområder, som efter min opfattelse udgør kernespørgsmål.

For det første hvilke grunde, der kan føre til, at sådan overvågning eller registrering kan forekomme hensigtsmæssig eller ligefrem ønskelig - og hvorfor elektronisk overvågning eller registrering af virkeligheden kan være problematisk eller ligefrem uacceptabel. For det andet hvilke elementer, der må indgå i en vurdering af, om en konkret overvågning eller registrering kan anses acceptabel eller ej. For det tredje en vurdering med en illustration af nogle områder, der efter min opfattelse kan karakteriseres som uproblematiske områder@, nogle områder der må karakteriseres som uacceptable, og endelig nogle, der indeholder et dilemma.

1. HENSYN OG MODHENSYN I RELATION TIL OVERVÅGNING

1.1. Hensyn - hvorfor overvåge eller registrere?

De hensyn, der fører til at der etableres eller ønskes etableret overvågning eller registrering omfatter i hvert fald følgende:

a. Forebyggelse af forbrydelser

Der installeres fx overvågningskameraer i pengeinstitutter, på stationer, i forretninger mv. med det hovedformål at sikre mod tyveri og at forebygge overfald. Fartkontrol er et andet eksempel på overvågning, der tilsigter at forebygge overtrædelse af lovgivningen - nemlig hastighedsgrænserne. Samkøring af forskellige registre kan have et lignende formål, fx at sikre mod socialbedrageri. Samtidig kan disse foranstaltninger siges at tilgodese de, der

overholder reglerne og tilgodese retssamfundet ved at det fx bliver sværere at udføre socialbedrageri, tyveri osv.

b. Give tryghed

Overvågning på fx stationer og andre offentlige steder kan give de, der opholder sig på de pågældende steder en tryghedsfornemmelse ved fx overfald eller tyveri, hvor der dels føles en vis sikkerhed ved, at der sker overvågning, dels bliver mulighed for hurtig hjælp. En anden form for tryghed kan opstå, hvor fx en dement plejehjemsbeboer ved hjælp af en chip bliver registreret, når den pågældende bevæger sig udenfor et givet område. Endelig kan forældre føle tryghed ved fx at kunne følge deres børns dagligdag i børnehaven el.l.

c. Forskning

Registrering af virkeligheden udgør en del af fundamentet for forskning. Det har derfor i forskningsmæssig sammenhæng stor betydning at kunne registrere en række oplysninger og at benytte disse oplysninger i forskningsmæssig sammenhæng. Et eksempel herpå er den forskning, der baserer sig på blodprøver, vævsprøver mv., der er på hospitalerne, og som kan give anledning til en række vigtige forskningsmæssige resultater. Disse resultater kan være vigtige for den fremtidige viden og dermed mulighederne for sygdomsbekæmpelse, forebyggelse osv. Der findes masser af andre eksempler også indenfor andre videnskaber for vigtigheden af at give registrere og benytte oplysninger om virkeligheden.

d. Journalistisk øjemed

Der er en stigende tendens til at benytte skjult kamera til at afsløre metoder og situationer, der kan forekomme uhæderlige eller på anden måde problematiske. Eksempler er metoder i forsikringsverdenen, opførsel blandt politikere, samværs med børn, hvor sagkyndige vurderer samværssituationen osv.

e. Underholdning

AOvervågning@ el.l er blevet populært i relation til underholdning. Et gammelkendt eksempel er skjult kamera. Aktuelle eksempler er videooptagelser af personer, der selv har indvilliget i det, fx i hjemmet og med mulighed for at følge med over internettet - eller i form af videooptagelser af en række frivillige, der lader sig installere i en særlig bolig med kameraer og mikrofoner installeret - ABig Brother@ hedder det endda!

f. Andet

Andre formål med elektronisk overvågning eller registrering af virkeligheden er fx varetagelse af offentlige serviceopgaver og kontrolopgaver, arbejdsgiveres udøvelse af kontrolfunktioner ved hjælp af overvågning eller registrering af ansattes e-mails, internet-brug osv.

1.2. Modhensyn - hvorfor kan overvågning/registrering være uacceptabel?

De modhensyn, der kan føre til, at elektronisk overvågning eller registrering af virkeligheden ikke anses acceptabel er især knyttet til følgende forhold, som kan siges at være af etisk karakter:

a. Selvbestemmelse

Et af de bærende etiske principper er retten til selv at bestemme grundlæggende forhold - ikke mindst vedrørende ens person. Dette fører til, at den enkelte person selv i et vist omfang må bestemme, om og i givet af hvem, man vil overvåges. Princippet kan dog ikke gennemføres fuldt ud, hvis man vil have overvågning på offentlige steder, i banker, butikker mv. Der må derfor foretages en afvejning, hvor spørgsmål om privatliv og integritet bliver centrale.

b. Retten til privatliv

Beskyttelse af privatlivet er fundamental, men det er vanskeligt at give en præcis definition af, hvilke rettigheder der flyder af dette princip. I det følgende opdeles retten til privatliv i spørgsmål om personlig integritet, social integritet og boligen.

- personlig integritet

I begrebet personlig integritet ligger en forestilling om, at der er noget ved en person, som skal være beskyttet mod andre mennesker. Det hører med til at være menneske, at der er visse aspekter af ens tilværelse, man ønsker at Ahave for sig selv@, som Aikke kommer andre ved@ osv. Det benævnes ofte i engelsksproget litteratur som Aprivacy@. I dansk sammenhæng er det også beskrevet som Aurørlighedszonen@ (Løgstrup). Dette får betydning for, hvornår overvågning og registrering anses uacceptabel.

S social integritet

Den sociale integritet benyttes her om den enkelte persons beskyttelsesbehov i forhold til omgivelserne. Nøgleordene er beskyttelse mod urimelig social kontrol og beskyttelse mod hvad andre mennesker får at vide om ens person, herunder optagelser på video o.l. samt videregivelse af personfølsomme oplysninger.

S boligen

ABoligen er ukrænkelig@ står der i Grundlovens ' 72. Dette udtrykkes også af og til ved princippet: AMy home is my castle@. Dette fører til, at overvågning har en helt anden karakter i forhold til privatlivets fred, end overvågning på offentlige steder, hvor man i forvejen må være indstillet på, at andre kigger på en.

c. Beskyttelse mod Aovervågningssamfundet@

Selvom hvert enkelt element af elektronisk overvågning og registrering af virkeligheden kan forekomme acceptabel, kan det samlede billede alligevel blive, at samfundet ændrer karakter.

I takt med at elektronisk overvågning og registrering af virkeligheden bliver almindelig - og almindeligt accepteret - er der derfor en risiko for, at den samlede mængde af denne overvågning og registrering fører til en samfundsstruktur, som kan få uheldige konsekvenser. Hvis den enkelte person er registreret og overvåget i meget udstrakt grad kan den mulighed for gennemsigtighed og kontrol med den enkelte persons liv, der herved opstår, dels give anledning til misbrug, dels give anledning til et samfund, hvor den enkelte person ikke længere føler at kunne bevæge sig i fred og frihed.

2. ELEMENTER, DER MÅ INDGÅ I VURDERINGEN

Der er en række spørgsmål, som man efter min opfattelse bør stille sig, hvis en bestemt overvågning kommer på tale.

2.1. Hvad er formålet med den elektroniske overvågning/registrering?

- Beskytte mig
  - mod overfald, tyveri, at betale for de andres tyveri eller snyd osv.
  - mod at personen selv (fx som dement) bringer sig i en farlig situation
  - mod at barnet er ked af det i børnehaven og gerne vil hentes

- Kontrollere mig
  - for at se om den pågældende overfalder, stjæler, snyder, kører for stærkt osv.
  - for at se om barnet har det godt i børnehaven

- Forskning
  - med henblik på bedre viden til brug for eksempel
  - sygdomsforebyggelse og behandling, samfundsforskning,

- Underholdning
  - tv-programmer, familien selv sender et program ind
  - overvågning, hvor hovedpersonen er informeret på forhånd
  - skjult kamera

- Andet
  - statistiske formål
  - journalistiske formål
  - ???

De fleste er formentlig villige til at acceptere videre brug af overvågning for at blive beskyttet end for fx at blive brugt til underholdningsformål.

2.2. Hvem foretager overvågningen/registreringen?

S Det offentlige

S En institution el.l.

S Arbejdsgiveren

S Familien

S Andre

Vurderingen vil være forskellig alt efter, hvem af de nævnte, der står for overvågningen.

2.3. Hvad viser overvågningen/registreringen om mig?

S Mine almindelige data
- S navn, adresse telefonnummer
- S cpr-nummer

S Personfølsomme oplysninger
- S Helbred
- S Sociale forhold
- S Straf

S Kørsel
- S Hastighed
- S Passagerer i bilen

S Indkøb
- S Tyveri
- S Indkøbsvaner

S Net-surf-vaner
- S Børneporno o.l.
- S Yndlingsemner
- S Hyppighed

- S Personlige gøremål
  - S Adfærd i hjemmet
  - S Adfærd i offentlige rum

Hvordan sker den?

- S - I anonyme registre
- S - I registre med navns nævnelse
- S - I samkørte registre
- S - Ved videooptagelser, der slettes
- S - Ved videooptagelser, der gemmes

S Hvor foregår den?

- S - På offentlige steder - veje osv.
- S - I banker, indkøbscentre, detention o.l.
- S - På arbejdspladsen
- S - I børnehave, skole, vuggestue

S Hvad er alternativet?

- S Ingenting
- S Anden form for opmærksomhed

3. Vurdering

Nogle områder kan udelukkes som absolut værende i strid med retten til privatliv og integritet: Eksempelvis kontrolovervågning i eget hjem samt kontrol over familielivet.

Andre synes generelt accepterede og acceptable (selvom det kan være irriterende): Eksempelvis fartovervågning på vejene og videoovervågning i banker.

Atter andre er svære, fordi de indeholder både beskyttelsesønske og omsorg på den ene side, men evt. kontrolforanstaltninger og Atvang@ på den anden side: Eksempelvis elektronisk overvågning af senildemente. Og hvad med video fra børnehaven?

Herudover er der det helt generelle spørgsmål, hvad der sker med vores samfund, hvis det bliver helt almindeligt at registrere elektronisk og foretage elektronisk overvågning. Når alt bliver så gennemsigtigt, bliver det så for svært at Avære i fred@, og kan der blive tale om misbrug? Hvor skal grænsen sættes - og af hvem?

I hvert fald må der tages hensyn til børn og andre - som ikke selv kan samtykke. Det må også altid overvejes, om der er bedre alternativer end overvågning, fx omsorg eller andre måder at indrette plejesituationen på, så de senildemente med mindre indgribende foranstaltninger sikres mod at gå ud og bringe sig i farlige situationer. I det hele taget bør man altid overveje om man ved overvågningen sætter noget teknisk i stedet for

menneskelig omsorg. Og om man risikerer en Afokusforskydning@ på en uheldig måde fra overholdelse af regler, fordi man synes de er acceptable - eller måske endda fornuftige - til sikring mod at undgå overvågningskontrollen - eller måske endda forsøg på at Asnyde@ den. En sådan fokusforskydning kan have heldig indflydelse på opfattelsen af retssamfundet. Endelig bør der være et konstant vågent øje for, at vi ikke ender i et overvågningssamfund, hvor det bliver for nemt at kontrollere og for svært at Avære i fred@ - privatlivet og familielivet bør fredes.

Søren Baggesen

Spørgsmål:
- Hvordan forbereder vi os til at leve i en virkelighed med registrering og elektronisk overvågning?

Til en begyndelse må jeg slå fast, at jeg ikke på nogen måde er ekspert på noget der har med elektronisk overvågning at gøre (det jeg er ekspert på er sådan noget som dansk litteratur i første halvdel af det 19. århundrede, og det er jo noget ganske andet). Men styregruppen har ment – og nok med rette – at det spørgsmål jeg er blevet bedt om at svare på, er der ikke rigtig nogen som overhovedet er eksperter på, og så har de altså spurgt mig om jeg ville prøve. Det har jeg sagt ja til, fordi det tvinger mig til at formulere nogen tanker om emnet jeg har gået og gjort mig. Det er min baggrund, og det må spørgerne have med når de overvejer om de kan bruge mine svar til noget.

Det er altid godt at tage udgangspunkt i egne erfaringer, og jeg har faktisk oplevet i en periode at få min telefon systematisk aflyttet af politiet. Det var i tresserne hvor jeg engagerede mig i det der bredt blev kaldt "Vietnambevægelsen". Det vi lavede der hvor jeg var med, var først og fremmest en annoncekampagne og ellers læserbreve og offentlige møder og demonstrationer. Den slags var – og er – lovlige politiske aktiviteter og dem må politiet hverken telefonaflytte eller registrere. Derfor var vi naturligvis godt forargede over at politiet lyttede med når vi talte i telefon sammen, men bortset fra det tog vi det roligt. Det vil sige vi fortsatte med at bruge telefonen nøjagtig så meget og så lidt som vi ville have gjort uden politiets medvirken.

Det er vel i sig selv en slags svar, i hvert fald hvis jeg tilføjer: "Gå hen og gør ligesådan". Men jeg vil godt udvide svaret med en sentens som fører lidt videre: "PET er ikke Stasi, men det er ikke PETs fortjeneste, det skyldes udelukkende at Danmark ikke er DDR". Jeg er ikke i tvivl om at vi – samfundet, myndighederne – kunne have en bedre kontrol med overvågerne end vi har i øjeblikket. Men det ville ikke i sig selv garantere for noget som helst. Ethvert samfund vil have sit PET og det der sikrer at det ikke udvikler sig

til Stasi er ikke parlamentariske udvalg, men de helt overordnede rammer som PET skal fungere i.
Det vil sige at det måske vigtigste svar jeg har at give på spørgsmålet, er at vi skal gøre os klart at det bedste og til syvende og sidst måske eneste værn vi har, imod de værste skadevirkninger af det overvågningssamfund vi er ved at bevæge os ind, er at vi opretholder demokratiet som rammen om samfundet. Nu kan man godt have sine bekymringer om demokratiets fremtid i Danmark, men det er en anden og meget stor problematik som jeg vil lade ligge. Det skal forstås sådan at jeg ikke opfatter overvågningen og mulighederne for overvågning som noget der i sig selv er en trussel mod demokratiet. Det farlige er at hvis demokratiet skrider, så vil de teknologiske muligheder for kontrol med borgerne gøre det meget nemmere for magthaverne at opretholde deres herredømme.

Derfor er det vigtigt, at vi i vores overvejelser over hvordan vi forbereder os til at leve i en virkelighed med registrering og elektronisk overvågning, skelner mellem to slags kontrol - jeg vil kalde dem "adfærdskontrol" og "sindelagskontrol". Adfærdskontrol har man når politiet ser til at annoncekampagner, protestmøder og demonstrationer ikke udvikler sig til terrorbomber og postrøverier (Blekingegadebanden er et både skræmmende og manende eksempel). "Sindelagskontrol" har man når nogen (politiet, Stasi) holder øje med at borgerne ikke får grimme og skadelige tanker om samfundets indretning, og sørger for sanktioner mod dem som har den slags tanker. Forskellen er vist klar nok, men grænsen mellem de to er ikke helt så nem at trække, der eksisterer ikke hårfine grænser, grænseområder er altid gråzoner. Det kan måske være rimeligt at kræve, at ansøgere til stillinger i børnehaver og fritidshjem fremlægger en ren straffeattest, så man kan sikre sig imod ansættelse af en person der er straffet for uterlighed mod børn. Men vi skal passe på ikke at anse det for så rimeligt at det ligger uden for enhver diskussion, for hvad bliver så det næste som måske kan være rimeligt? At vi ikke ansætter skolelærere der kunne mistænkes for at ville "indoktrinere ungdommen med kommunistiske idéer"? Det var faktisk tæt på i halvfjerdserne.

Tilbage til dengang min telefon blev aflyttet. Det menneske som blev mest berørt af det var min mor. Ikke fordi hun havde noget at frygte, hun var ikke engageret i politiske aktiviteter som politiet overhovedet kerede sig om, og i øvrigt ringede hun til os for at høre hvordan vi havde det – og ungerne? – og fortælle os om hvordan de havde det derhjemme i Struer hvor jeg kommer fra. Præcis af den grund var det både klart og rigtigt at hun for alvor måtte blive oprørt. Hvad hun oplevede var at politiet brutalt og umotiveret krænkede hendes privatlivs fred. Det var ikke bare mine, vietnamaktivistens, samtaler der blev aflyttet, det var også hendes. Ikke fordi der var nogen der ville lytte til dem, men fordi hun snakkede med en som nogen ville aflytte.

Som sagt mener jeg at det var både klart og rigtigt, at mor var den som blev mest oprørt. Krænkelsen af privatlivets fred ved overvågning, enhver overvågning, er størst for dem der bliver overvåget uden at der er nogen grund til overvåge dem, og uden at nogen vil overvåge dem. Samtidig er det den form for overvågning som de fleste af os bliver mest udsat for. For det er jo den slags overvågning jeg kommer ind under hver gang jeg træder

ind gennem døren til Kvickly, og dermed træder ind i synsfeltet for det elektroniske øje der sidder oppe under loftet i velsagtens enhver Kvickly.

Det vil jeg godt udbrede mig lidt om. Først ved lige at bede jer overveje forholdet mellem "os" og dem" i den her sag. Det har nemlig slået mig ved at læse alle de spørgsmål igennem som er blevet stillet til ekspertpanelet ved den her konsensuskonference, at der er en hel klar fordeling mellem "os" og "dem" i dem. "Vi" er de overvågede, "de" er dem der overvåger os. Det er jeg ikke spor overrasket over. For det første er det jo i det store og hele rigtigt at det forholder sig sådan; for det andet ligger det vel i hele oplægget; og for det tredje vil det under alle omstændigheder være den position vi spørger fra i den her sag, for det er den der bekymrer os. Alligevel synes jeg vi skal gøre os klart, at helt så klart er det ikke med "os" og "dem". Vi er også overvågere, eller i hvert fald bliver overvågningen også gennemført på vores vegne. Det er klart med sådan noget som PET (og den afdeling af politiet der holder øje med pædofil-siderne på nettet, og dem der lytter til samtaler i narkomiljøet o.s.v.), dem har vi, fordi vi har indset at det er nødvendigt at have dem, vi har dem for vores egen trygheds skyld. Men i sidste ende gælder det vel også for det elektroniske øje i Kvickly, om ikke på anden måde så i hvert fald på den at vi tror på at det kan begrænse butikstyverier, dvs. begrænse Kvicklys spild, og dermed holde priserne nede – vi ved jo godt at det på den ene eller anden måde bliver os der kommer til at betale for de videoer de andre stjæler fra hylderne.

Derfor er det vigtigt at vi overvejer det der med "os" og "dem" – og at vi gør det præcis ud fra det forhold, at vores situation er den samme som mors, altså at vi – folk flest for det meste – bliver overvåget uden at der er nogen som helst grund til at overvåge os. Det tvinger os nemlig til at se det dilemma i øjnene der består imellem den overvågning vi ønsker, og den vi vil finde os i. Hvis det var sådan – eller er sådan for nogen af os – at der er et nøjagtigt sammenfald mellem de to, så var der ikke noget dilemma. Men helt så enkelt er det nok ikke, det kan nemt falde sig, at vi kunne ønske overvågning på steder hvor vi ikke selv ønsker at blive overvåget, og hvor der heller ikke er nogen grund til at overvåge os, for vi foretager os ikke noget vi ikke må der.

Lad mig tage et eksempel. For et par år siden var der en urmager på gågaden i Holstebro som var meget plaget af at nogen forsøgte at smadre hans udstillingsvinduer, sandsynligvis for at stjæle af varerne bag dem. Derfor søgte han om lov til at sætte et par videokameraer op, så fortovet foran hans butik blev overvåget. Det var vi mange som godt kunne se rimeligheden i, men kommunen vægrede sig, og det var vi også mange som gav vores tilslutning til. For selvfølgelig havde urmageren en klar og anerkendt interesse i at beskytte sin butik, men gågaden i Holstebro er offentligt rum, og der vil vi have lov at færdes uden at nogen holder systematisk og elektronisk øje med os. Hvis jeg står med min kone under armen og kigger på smykker som vi ikke kunne drømme om at købe, så er det selvfølgelig lige meget at der hænger et kamera og glor på. Men hvis jeg står med en anden mands kone under armen og kigger på de samme smykker, så er det noget andet. Vi gør ikke noget ulovligt, men vi ønsker ikke at blive holdt øje med i den situation.

Jeg ved ikke hvad udfaldet af den her sag er blevet, så meget har den ikke interesseret mig. Men det der er klart i det her tilfælde, nemlig at det drejer sig om privat overvågning af offentligt rum, det er mindre klart i andre tilfælde. Hvis urmageren ønsker

at sætte kameraer op inde i sin butik, så er det meget nemmere for ham, for det er hans private ejendom. Men er en butik også et privat rum? og er et supermarked? er Bilka og OBS? er et butikscenter som Fisketorvet i København? Juridisk set er de – går jeg ud fra, for de er jo hver for sig privatejede. Men i praksis er de ikke. Ikke alene bliver vi inviteret indenfor, eller rettere nærmest presset til at komme der. Der er også ved at ske det – og det har ejerne bestemt ikke noget imod – at den slags butikker får besøg af mange som egentlig ikke kommer der for at handle, men bare for at opleve. Det kaotiske rykind da Fisketorvet åbnede. viste jo klart nok at det her var iscenesat og blev opfattet som en oplevelse, og ovre på mine kanter i hvert fald bliver det mere og mere almindeligt, at folk planlægger en tur til Bilka i Holstebro som en familieudflugt i weekenden. De klarer nok nogle indkøb når de alligevel er der, men det er ikke det der får dem til at tage af sted. Bilka bliver målet for det man i gamle dage ville kalde en skovtur, og selv om jeg er ved at blive så gammel at jeg opfatter det som sært, så kan jeg godt se at det måske ikke er helt skidt, for på den måde kan familierne få en udflugt sammen også om vinteren. Men altså: Bilka er et rum som vi opfatter som et offentligt rum, men som er under konstant privat overvågning.

Det er her dilemmaet kommer ind. For på den ene side giver det en vis tryghed at vide at Bilka er overvåget, på den anden vil vi godt kunne tage på udflugt uden at vi bliver holdt øje med. Jeg tror ikke at problemet er stort for ret mange, og de bliver vel hjemme alligevel, uden at Bilkas omsætning tager skade af det. De fleste af os har givetvis vænnet os til det, som det hedder.

Men netop derfor kan det godt være umagen værd at tænke lidt over, hvad det er vi har vænnet os til. Har vi bare lært os selv at sådan er det og det behøver vi ikke at tage os af, for egentlig er det ikke os de holder øje med, det er dem der er grund til at holde øje med? eller får det på en eller anden måde indflydelse på den måde vi opfatter en familieudflugt på, og den måde vi opfører os på når vi er på udflugt?

Jeg tænker på sådan noget som vores holdning til butikstyverier, det er jo først og fremmest dem som begrunder overvågningen. De butikker og indkøbscentre som bliver udflugtsmål er indrettet på den måde at alle varerne ligger fremme og byder sig til så fristende som muligt, det er derfor de bliver udflugtsmål. Meningen med det er at vi skal lade os friste, vi skal tage varerne og vi skal tage dem selv, og det er ikke kun for at spare penge til personale at det er sådan, det er en del af indkøbsoplevelsen. Derfor er de også udstyret med overvågningskameraer, og chips af en slags i varerne, og elektroniske sluser vi skal igennem for at komme ud, for det er jo også meningen at vi skal betale for varerne. Bilka inviterer os inden for med åbne arme fordi vi er potentielle kunder, og i samme øjeblik vi træder ind, holder de øje med os for vi er også potentielle butikstyve. Mottoet her – som overalt hvor vi bliver overvåget - er Lenins gamle diktum: "Tillid er godt, men kontrol er bedre!"

Det er dette dobbeltsyn på os vi har vænnet os til – og bliver nødt til at vænne os til i stadig højere grad. Spørgsmålet er om det gør noget ved os. Det spørgsmål er blevet rettet på forskellig måde og under forskellige overskrifter til denne konference, og der er nogen som nok er mere eksperter på det end mig, som skal prøve at besvare det. Men jeg vil godt prøve også, og prøve konkret med udflugten til Bilka som eksempel. Her kan spørgsmålet stilles på denne måde: hvordan lærer vi ungerne som vi tager med på udflugt,

hvad det er for en situation vi bringer dem i? For de bliver jo også fristet, og det er så nemt lige at få en barbiedukke ned i rygsækken og tage den med, så der er noget at lege med når man kommer hjem. Spørgsmålet er så hvordan vi lærer dem at det må de ikke? Det rigtige svar er vel stadig, at vi skal lære dem at det må de ikke, fordi det er forkert at stjæle. Det er bare ikke så nemt, for så er der en masse andet som også skal forklares. Og er det nemme svar ikke at sige til dem, at det må de ikke, for det bliver opdaget og så kommer butiksdetektiven og tager dem?

Det er, men jeg, den situation vi skal forberede os på. Og så skulle jeg altså prøve at svare på hvordan vi gør det. Jeg kan ikke se bedre end at vi må gøre det ved: på den ene side at gøre os situationen klar, og på den anden side at nægte at anerkende den. Bilkas dobbeltsyn på os som potentielle kunder og potentielle butikstyve, må vi vænne os til og finde os i. Hvis vi indser det – og ikke bare skyder det fra os som en ubehagelig realitet – så kan vi også forholde os til det. Og det kan vi gøre ved ikke at anerkende det, ved ikke at tage det til os som vores eget syn på os selv. Bilka stoler ikke på vores egen indre kontrol, de har ingen tillid til os. OK – så må vi sørge for at vi opretholder tilliden til os selv. Jo mere ydre kontrol vi får, jo mindre indre kontrol har vi brug for. Bortset fra at vi har brug for den for vores egen skyld. Vi kan godt holde fast i nogen normer for ordentlig opførsel, selv om Bilka ikke tror vi kan, fordi der er nogen der ikke kan. Vi kan godt opdrage vores børn til at lade være med at hugge barbiedukken, fordi det er forkert at stjæle, og ikke fordi overvågningskameraet opdager at de gør det.

Tema 3: Fremtid og udvikling

Per Helge Sørensen, Forfatter, Digital Rights

Spørgsmål:
- Hvad er skrækvisionen?

Forestil dig et samfund. Et samfund, hvor alle borgere fra barnsben får indopereret en lille kamera bag hornhinden.

Et kamera, som konstant optager hvad den enkelte borger ser. Hvor han går hen. Hvilke personer han møder. Hvilke bøger har køber – og overvejer at købe. Hvilke aviser han læser og hvad han se i Tv. Hvilke foreninger han deltager i.

Forestil dig at billederne bliver sendt til en stor database gemt i kælderen under politigården. En database, hvor det er muligt fra sekund til sekund at følge den enkelte borgeres bevægelser – at se med over skulderen - og hvor billederne bliver gemt et halvt år tilbage i tiden.

Forestil dig, at det hele sker i kriminalitetsbekæmpelsens navn. For at forbrydere ikke bare kan bevæge sig rundt i vores samfund og begå kriminalitet, uden at politiet bag efter har en mulighed for at opklare det. Ikke mindst sker det for at sikre politiets mulighed for at opklare overgreb mod børn. Her er det jo uden billederne fra kameraet helt umuligt at fastslå, hvad der er foregået. Børn er vanskelige vidner. Gentagne gange er det lykkedes forbrydere at gå fri, fordi det ikke har været muligt at få en tilstrækkelig sikker sag stablet på benene. Og billederne i databasen er jo ikke mindst i den anklagedes egen interesse, hvis han vitterligt er uskyldig – for så kan de jo bevise hans uskyld.

Billederne er naturligvis beskyttet. Det er ikke hvem som helst, der kan få adgang til dem. Kun mod en dommerkendelse kan politiet få lov til at åbne databasen og få adgang til billederne fra en borgers kamera. Og for at få en dommerkendelse skal borgeren være mistænkt for en alvorlig forbrydelse. Mord. Seksuelle overgreb. Forbrydelser med en straframme over 6 år.

Eller det skulle man i hvert tilfælde oprindeligt. Det er godt nok begyndt at skride en smule. I takt med at kameraerne er blevet udbredt, har politiet fundet ud af, at der foregår langt flere ulovlige ting end man oprindeligt havde forestillet sig. Folk mødes i et væk og planlægger forbrydelser. Misbruger deres fysiske bevægelsesfrihed til at begå snart den ene, snart den anden forbrydelse. Butikstyveri, svindel, indbrud, vold og overgreb.

Hurtigt er der kommet er voksende pres for at tillade adgang til billederne i databasen i andet end de mest alvorlige forbrydelser. For det kan vel ikke være rigtigt at de kriminelle skal udnytte systemet til undgå politiets efterforskning. At de skal misbruge samfundets retssikkerhedsgarantier til at skjule deres kriminalitet. Gradvist er betingelserne for at politiet kan få adgang til databasen blevet slækket. Lidt efter lidt har man udvidet kredsen af forbrydelser, som kunne berettige en dommerkendelse til databasen. Ja faktisk er man for nyligt begyndt at diskutere at tage den fulde konsekvens og give politiet mulighed for at få en dommerkendelse i forbindelse med alle forbrydelser, som bliver begået i den fysiske verden.

Men stadig vil det jo kun være forbrydere, der bliver overvåget. Så længe du ikke foretager dig noget ulovligt, er der ingen der får adgang til dine billeder. Det er jo ikke sådan, at politiet vil sidde og kigge med på må og få. Surfe i uskyldige menneskers billeder. Det ville de jo for øvrigt slet ikke have ressourcer til. Det er jo millioner af billeder der er tale om.

Så længe du blot holder dig på den rigtige side af loven, har du intet at frygte. Så vil billeder blive optaget, lagret i databasen og efter et halvt år blive slettet igen. Ingen vil nogensinde kigge på dem. Du behøver faktisk slet ikke at føle dig overvåget.

Hvis du er uskyldig kan du trygt glemme alt om kameraet. Og hvis du ikke er... Så er det måske meget godt at politiet kan kigge med.

En skræk... vision?
Er ovenstående en skrækvision? Det er det nok i virkeligheden ikke.

Skrækken er der ganske vist ikke noget galt med. Det samfund, der beskrives, er vel for de fleste temmelig skræmmende. Det er visionen det halter med. En vision skal være noget, der ligger et stykke ude i fremtiden. Noget der endnu ikke er realiseret. Og det er her det går galt. For det samfund, der beskrives, er ikke så langt fra at være det samfund, vi er ved at skabe på Internettet.

På Internettet har vi naturligvis ikke kameraer bag hornhinden, når vi surfer. Men det er heller ikke nødvendigt. For når vi går på Internettet, bliver der automatisk genereret - og gemt - en lang række oplysninger om os, som gør det muligt at følge vores færden på nettet. Oplysninger om hvornår vi har været på. Om hvilke hjemmesider vi har besøgt. Hvem vi har sendt mail til og modtaget mails fra.

For den person, der får adgang til disse oplysninger vil det være muligt at følge os fra sekund til sekund. Se hvilke personer vi kommunikerer med. Hvilke aviser vi læser på nettet og hvilke Tv programmer vi ser. Hvilke bøger vi køber – og overvejer at købe. Hvilke nyhedsgrupper vi deltager i. Hvilke chat-rooms vi besøger.

Efterhånden som en stadig større del af vores dagligdag sker via nettet bliver det muligt at følge vores liv fra sekund til sekund via disse oplysninger. Lige så nøjagtigt, som hvis vi havde et kamera bag hornhinden. Eller måske endnu mere?

De vigtige spørgsmål er, hvor længe disse oplysninger bliver gemt, hvem der kan få adgang til dem og under hvilke betingelser. Og det er lige præcis her, at det Internetsamfund, vi er ved at skabe, kommer skræmmende tæt på skrækvisionen. For i det øjeblik at talen falder på kriminalitetsbekæmpelsen – ikke mindst efterforskningen af børneporno på nettet – har vi været meget gavmilde med at give adgang til oplysningerne.

For det første har vi valgt at lempe kravene for at politiet kan foretage aflytning på nettet i forhold til de krav vi tidligere har stillet i forbindelse med telefonaflytning. Selvom en overvågning af en person på nettet på mange måder er langt mere indgribende end en simpel telefonaflytning er vi - i takt med at vi er blevet opmærksomme på, at også forbrydere nyder godt af Internettets effektive kommunikationsform - begyndt at slække på kravene.

I første omgang er det særligt børneporno, det har været i fokus. Selvom vi som samfund ikke takserer distribution af børneporno til mere en maksimalt 2 års fængsel – altså under de 6 år, som hidtil har været betingelsen for at få en dommerkendelse - har vi valgt alligevel at give politiet adgang til aflytning på nettet.

Desværre er dette nok kun første skridt på vejen. Som man noterede sig i Justitsministeriets udvalg om IT-kriminalitet så "må der løbende på baggrund af udviklingen i kriminalitetsformerne tages stilling til, om der er behov for at udvide adgangen til indgreb i meddelelseshemmeligheden til flere straffebestemmelser". Eller som et mindretal i udvalgte fremførte: der bør "åbnes mulighed for, at domstolene kan afsige kendelse om indgreb i meddelelseshemmeligheden i alle situationer, hvor der reelt ikke er andre efterforskningsmuligheder."

Og det er ikke kun i Danmark, man mener, at politiets muligheder for at overvåge borgerne skal forbedres. I Europarådets udkast til en konvention om IT-kriminalitet (Cyber-Crime) fra den 2. oktober 2000 lægges der op til, at politiet skal kunne få realtids adgang til oplysninger om brugeres færden på nettet i forbindelse med ”alle forbrydelser begået via en computer” . Med det Internetsamfund, der er ved at opstå omkring os, er der næppe mange forbrydelser, som vil falde uden for denne kategori...

Men lempelse af betingelserne for adgang til overvågningsdata er ikke det eneste punkt, hvor vi nærmer os skrækvisionen ovenfor. For selvom computersystemerne genererer og gemmer en lang række oplysninger om os, når vi surfer på nettet, så synes vi stadig ikke, at det er helt nok.

F.eks. er det meget ubelejligt, at mange Internetudbydere faktisk sletter en masse data, når de ikke længere selv har brug for dem. Data, som ville give politiet mulighed for at se, hvad brugerne har foretaget sig på nettet i den sidste tid, hvis det skulle blive nødvendigt.

I Danmark (og i en række andre lande) overvejer vi derfor at stille krav i lovgivningen om, at Internetudbyderne skal gemme disse data et halvt år tilbage i tiden, således at politiet kan få adgang til dem i forbindelse med efterforskningen.

Og så er vi jo lige præcis i den samme situation som i skrækvisionen. At vi gemmer en række oplysning om alle borgernes færden et halvt år tilbage i tiden – udelukkende med det formål at politiet kan overvåge de få borgere, som mistænkes for at begå noget ulovligt.

Men skulle vi så ikke også se at få anskaffet os de kameraer?

Anders Bjerre, Instituttet for Fremtidsforskning

Spørgsmål:
- Hvad er drømmevisionen?

København, 17. november 2030
Til 30-års jubilæet for Teknologirådets konsensuskonference om overvågning 17. nov. 2000

Lillebror ser alt!

Først vil jeg gerne takke Teknologirådet for at tage initiativ til at gentage deres konference om overvågning her 30 år efter, i 2030.
Og specielt jeg har jo særlig grund til at takke for det.

Som så mange andre kunne jeg dengang, i år 2000, se både positive og negative sider af udviklingen i overvågning.

Uanset mine egne holdninger var jeg blevet bedt om at indtage det "politisk ukorrekte" standpunkt - at tale for det positive i overvågning. Så at sige at være djævelens advokat.
Og det er jo altid med en vis frygt, man påtager sig den rolle. Bliver man hængt ud i pressen?

Men nu, 30 år efter, er det jo tydeligt at jeg holdt på den rigtige hest!

Dengang i år 2000 havde man angsten for overvågningssamfundet. For at man skulle blive manipuleret. For at "Storebror ser alt" - de skjulte magthavere, der ville kontrollere os yderligere.
Men den nye virkelighed er langt mere åben. Samfundet er transparent.
Det er lillebror, der ser alt - det er os alle sammen.
Og det har givet en helt anden og mere demokratisk magtbalance i samfundet.

Vi har måttet sluge et par kameler undervejs. Er det nødvendigt med så meget registrering?
Hvad er der blevet af privatlivet?
Men man vænner sig jo efterhånden til nye kulturformer.
Glæder sig over forandringerne og de nye muligheder.

Historisk er åbenhed såmænd ikke så fjern. I landsbysamfundet vidste alle alt om alle. Ingen havde eget soveværelse, og på das sad man flere på række. Privatliv var en by i Rusland.
Men i småborgerlighedens tidsalder lukkede man sig mere og mere inde. Alt var facade. Skjorten måtte godt være laset, bare skjortebryst, flip og manchetter var fine - man skjulte sig bag masker. Folk lukkede sig inde med deres tanker og drifter, som de på trods af Freud og hans disciple troede var så specielle at de måtte skjules for andre! Dette fokus på privatlivets hellighed var jo aldeles latterligt og småborgerligt forkrampet.

Tiderne ændrede sig heldigvis igen. Man kunne se det i brugen af mobiltelefoner. Folk udbredte sig højlydt om de mest private ting mens de sad i S-toget. Hvor var problemet?

Nogle unge mennesker fandt ud af at skabe opmærksomhed eller endda tjene penge ved at sætte web-cams i deres hjem. Så kunne man se en af stripperkongens piger via nettet - eller almindelige unge pars udskejelser i soveværelset. TV gjorde folk til stjerner hvis de lod Big Brother se alting.

Men det virkede kun en kort overgang. Så forskellige er vi mennesker jo heller ikke. Alle pudser næse, alle tisser, alle har et seksualliv og nogle har fordøjelsesproblemer. Hvor interessant er det? Overvågning blev hurtigt uinteressant!

Jeg er overvåget af alverden - og jeg kan overvåge alverden alt det jeg lyster.

Resultatet er blevet et langt mere åbent, menneskevenligt og demokratisk samfund end nogensinde før i verdenshistorien.

Pointen er jo netop at jeg også selv kan overvåge alting - ligesom alle andre kan.

Der er ikke nogen egentlig skjult overvågning - for hvordan skulle man kunne skjule det? Hvis FN eller Microsoft eller Peter eller Fatima overvåger os, så finder vi nok ud af det. Alting er synligt for alle! Man kan ikke snage i det skjulte - overvågerne er selv synlige!

Og det hele ligger frit tilgængeligt i databaserne i al eftertid.

Hvis man bliver mistænkt for en forbrydelse, så vil man blive overvåget med tilbagevirkende kraft - politiet gennemgår databaserne, og kan rekonstruere ens mindste gøren og laden de sidste mange år. Eller en journalist gør det. Eller ens nabo.

Hvis man tæver sin treårige dreng, så må man regne med at han trækker beviserne frem som 15-årig og lægger sag an.

Jo, "Lillebror ser alt". Om ikke andet, så når han er blevet stor.

Alt i alt må man hellere opføre sig anstændigt overfor andre mennesker.

Den nye åbenhed er magthavernes mareridt. Alle de rænkespil der trivedes i fortiden. Rænkespil på Christiansborg, rænkespil i direktionskontorerne, i marketingbureauerne. De var ude på at snøre os - og de vandt spillet, for de havde flere informationer end os andre. Der var kampagner med fordrejede virkelighedsbilleder.
Hvis vi bare spiste XX, så blev vi rige og smukke!
Hvis vi bare stemte på NN, så var problemerne væk!

Manipulationerne trives på lukkethed - men blev dræbt af den nye kultur.
Folkestyre, frihed og anstændighed trives på åbenhed!

Den ultra-liberalistiske individualisme glemte at frihed for alle forudsatte frihed under ansvar.
De var imod overvågning på vejene - så hellere trafikdrab.
De var imod overvågning af betalinger - så hellere svindel og skattesnyd.
De var imod overvågning i hjemmene - så hellere incest, hustruvold og jalousidrab.
De var imod overvågning på gaden - så hellere voldtægt og mord.

Den nye tids ånd giver individet langt større reel frihed, for den er baseret på den enkeltes frihed under respekt for fællesskabet.
Du kan gøre hvad du vil, så længe du ikke tramper på andre.
Men ve dig hvis du ikke respekterer andre - du bliver opdaget.

Alt på nettet bliver overvåget. Også overvågerne.
Søger de at skjule sig, så bliver de hacket. De bliver *altid* hacket! "Information wants to be free", som hackerne sagde. Informationerne kommer altid frem. Altid.

Der er kameraer overalt i det offentlige rum - og i de fleste private. Det er stort set gratis - og giver enorme fordele. Det intelligente hjem kan hjælpe med stort set alting, for det er koblet op på alverdens databaser og kunstige intelligens.
Ulemper er der ingen af. Når man ellers først har vænnet sig til at ha' kamera på overalt.

Det var ikke alle, der syntes det var smart i starten. Mange var faktisk modstandere!
Men altså. Hvis man ikke har webcam i badeværelset skal man selv huske at bestille mere tandpasta når tuben er ved at være tom - og hvem gider det?!

Andre kan se hvordan vi bruger vores penge. And so what ?
Alle har da lov at ha' nogle laster - og lasternes sum er som bekendt konstant. Hvis de ikke kan ses, så ligger de nok i fantasien!

Man skal tænke på at vi er omgivet af intelligente systemer. Og de kan kun hjælpe os hvis de har information om os.
Jo mere information, jo bedre kan det hjælpe - og jo mere diskret kan det fungere.
Der er jo ikke noget overnaturligt ved en elektronisk butler - den skal være forbundet med alverdens databaser og analysecentre for at virke optimalt. Så det er den selvfølgelig!

Min families e-butler kender vores vaner. Vi behøver ikke selv at holde køleskabet fyldt - der er altid basisvarer i huset. Vi skal selv sige til hvis vi vil ha' særlige retter til middag, men i det daglige bruger vi bare butlerens forslag.
Vi skal ikke selv vedligeholde huset - det bliver klaret af det system, ejendomsmægleren installerede i sin tid.

Og tænk hvis man selv skulle vælge hvad man ville se i fjernsynet! Det er jo helt urealistisk!
Dengang i år 2000 havde mange måske kun 8-10-12 kanaler at vælge mellem - det kunne man godt overskue. Men nu ligger der millioner af programmer jeg kan hente hjem en aften. Hvordan skulle jeg selv kunne vælge mellem dem? Det er da nødvendigt at systemet har overvåget hvad jeg tidligere har været glad for og så foreslår mig noget godt til i aften.

Kort og godt: Jeg ville drukne i valg hvis jeg ikke var støttet af min e-butler - og den er støttet af hele verdens info-systemer.

Jeg kan huske engang i 2015. Jeg genlæste Hemingways "Den gamle mand og havet". I ugerne derefter blev jeg overdænget med reklamer for fiskeudstyr og for tropiske sørejser! Men nu er systemerne heldigvis smarte nok til straks at se at det ikke interesserer mig. Hvordan skulle de vide det uden at overvåge min mimik når jeg læser?

Da systemerne først var blevet hjælpsomme, pålidelige og så diskrete som den perfekte kammertjener, så var vi mange, der godt ville ha' webcams overalt. Jo før, jo bedre!

De ganske få, der ikke havde webcam overalt, kom til at fremstå som lidt suspekte. Hvad havde de mon at skjule? Rygterne gik! Den sikreste måde at aflive rygterne var selvfølgelig at åbne for det hele - så alle har webcam hjemme nu.

Vi har alle chip-implantater. Chips i overarmen, der overvåger os. Det gav en masse ballade i sin tid da systemet blev indført - men det er altså ret smart!
Tænk - i gamle dage, da skulle man ind til lægen for at få checket helbredet - blodprøver skulle sendes på laboratoriet - svar ugen efter, hvis de ikke var blevet forbyttet!
Nu bliver man bare overvåget, og lægen ringer hvis problemer - det er ret meget lettere!

Og det var værre endnu i gamle dage!

Hvis man kørte galt og fik kraniebrud - hvis man fik hjertestop eller insulinchok - hvordan skulle man så tilkalde en læge? Jo, man skulle lige vågne op og ringe på mobilen - det lyder grotesk - og folk døde da faktisk også af det!
Nu ringer chippen selv op, fortæller hvad du fejler og hvor du er - og straks er ambulancen på vej.

Og i øvrigt er de chips ret praktiske. Ellers skulle man jo selv åbne dørene !
Og hvordan skulle folk kunne finde en, hvis man ikke man kunne spores ved sin chip?

Selvfølgelig er der ulemper. Du kan ikke satse på at gå uset rundt i storbyen.
Hvis hende der fra julefrokosten vil finde dig - så finder hun dig!
Men altså - det betyder bare at man må være helt ærlig når man møder gamle kammerater eller gamle kærester.
"Det var hyggeligt dengang, nu ser mit liv anderledes ud, der er ikke plads til dig".
Mindre hykleri, mere ærlighed.
Hvis man har problemer med ærlighed, så var det måske lettere i gamle dage.

Hvad har vi mistet ved den globale overvågning?

Vi har mistet muligheden for at begå tyveri, snyde og bedrage andre uden at blive opdaget, for at tæve og voldtage i det skjulte. Vi har mistet muligheden for at køre hensynsløst og for at begå skattesvindel.
Alt dette kan man kalde tab af frihed - men helt ærligt !

Vi har i en vis forstand mistet "privatlivets fred".
Men det har vi jo egentlig ikke. Vi bliver jo ikke forstyrret af overvågningen.
Og vi har jo ikke mistet vores personlighed - vores venskaber eller fjendskaber. Vi kan stadig være glade med vennerne - der er plads til både stille stunder og til fest og ballade.

Faktisk har vi jo stadig alt det liv, vi har lyst til - det kan bare ikke skjules for andre. Hvis vi har særprægede seksualvaner kan det ikke skjules, men på den anden side er der ingen der interesserer sig for det længere.
Det vi har mistet er måske især illusionen om at vi er så unikke.

Vi har mistet nogle myter - men vundet nogle realiteter.

Hvad har vi vundet?

Vi har vundet friheden fra en masse konkrete problemer i samfundet. Affekt-vold er selvfølgelig ikke forsvundet, men kriminaliteten er stærkt reduceret.
Så der er mindre vold og ingen tyverier. Ingen plat, skattesnyd, forsikringssvindel.

Generelt har åbenheden givet personlig ansvarlighed - man kan ikke dække sig under at være "firmaets mand". Man kan ikke producere landminer og bare fortælle folk at man er proces-ingeniør i metalindustrien - det med minerne kommer frem.

Produktsikkerheden er forbedret - der er åbenhed om forløbet, om tests osv. for forbrugere, journalister og offentlige myndigheder - men hvis konkurrenter kigger over skulderen, så bliver de opdaget - og dømt for industrispionage!
Alt i alt er etikken kommet helt i top næsten overalt. Virksomheder kan samarbejde åbent, tingene glider lettere, og forbrugerne er tryggere ved resultaterne.

Men vi er ikke bare blevet fri for de ting vi frygtede.

Vi er også sluppet for det, vi knap nok vidste at vi frygtede.

Det civile samfunds genkomst og den nye personlighed

Vi kan møde fremmede med åbenhed. Vi går langt mere tillidsfuldt gennem verden - vi behøver ikke at skjule vore egne hensigter, for det vil være nytteløst, og tilsvarende behøver vi ikke at frygte andre menneskers skjulte sider. De kan have sære drømme og forestillinger - lige som vi selv - men risikoen for at de bliver voldelige er meget lille.

Det kan virke grotesk at nogle stadig kan drømme om gamle dage.

Dengang i år 2000 frygtede man tabet af tilliden i "det civile samfund". Flere og flere vendte ryggen til hvis der blev begået overgreb på gaden. Flere og flere lukkede sig ind i deres små huler. De kørte i bil til arbejde hvor de kun mødte ligesindede i samme socialklasse. Så kørte de hjem igen, åbnede garagedøren med fjernbetjeningen og gik ind til sig selv. De mødte aldrig "anderledes" mennesker. I USA havde man lukkede byer med vagtmænd, omgivet af pigtråd og minefelter. Francis Fukuyama skrev en bog om tabet af tillid - "Trust". Han mente at det åbne samfund var baseret på gensidig tillid - den fundamentale tillid til fremmede, indtil det modsatte var bevist. Og den var ved at blive nedslidt i det moderne liv. Samfundet ødelagde sine egne forudsætninger.

Også i Danmark boede folk mere og mere adskilt efter socialklasse og baggrund. Og færre og færre brugte folkeskolen. Samfundet var lige så stille ved at gå i stykker. Fællesskabet på vej ud.

Tilliden til fremmede var på vej ned. Det var ikke bare "de fremmede" - dem, der var en tak mere sorthårede og talte med accent. Utrygheden ved dem var bare et symptom på den almindelige utryghed - de var så at sige oplagte symboler.
Nej, det var fremmede mennesker i almindelighed, der var farlige. At møde fremmede på en mørk vej. At lade sine børn komme sent hjem - man måtte hellere køre dem i bil.

Mandlige pædagoger skulle have anstandsdame med i puslerummet. Og kameraet i vuggestuen var der specifikt for at overvåge om de var kriminelle. Det mindede om kriminalitet, det var symbolet på mistænksomhed.

Nu er der kameraer overalt - chips overalt - alt registreres. Der er tryghed og åbenhed.
Vi har bevæget os fra magthavernes overvågning af de mange til alles åbenhed overfor alle.
Vi har bevæget os fra kontrol til selvkontrol, fra overherredømme til demokratisk civilisation.

Der er langt bedre mulighed for tillidsfulde møder, på tværs af alder, køn og etnicitet. Vi søger ikke længere tryghed bag hjemmets lukkede døre, men finder den i åbne møder med andre mennesker. Kulturen blomstrer i den spontane glæde over forskellighederne - det er let at vise forskelligheder, for vi kan alligevel ikke skjule dem!

Demokratiet blomstrer sammen med kulturen - for demokrati forudsætter åbenhed og tryghed.

Og ligeværden blomstrer i takt med den øgede tryghed. Svage grupper færdes frit.
Vi kan lade børnene lege med hinanden på gaden, i haverne, i skovene. Børnene har faktisk fået større frihed og mindre tæt overvågning - for de kan leve i børnenes verden.

Vi har nok alle fået en mere åben personlighed.
Vi er stadig unikke individer med umistelige rettigheder og uerstattelige, personlige relationer til vore nærmeste.

Men vi kan ikke regne med at udføre kriminelle handlinger i det skjulte, og i det hele taget er der ikke plads til så meget hykleri.

John Strand, Strand Consult

Spørgsmål:
- Hvilke muligheder åbner teknologien for elektronisk overvågning indenfor de næste fem år?

Lad mig starte med at minde om at det ikke er muligt at give noget entydigt svar på ovenstående spørgsmål. Et svar vil være helt afhængigt af hvilken teknologi man vælger at fokusere på. Jeg har i mit svar valgt at fokusere på IP/Internet teknologien, og især det mobile aspekt af denne teknologi. Årsagen hertil er, at jeg mener denne teknologi i højere grad vil præge udviklingen de næste fem år, og at den vil komme til at spille en rolle i stort set alle forbrugers dagligdag.

Lad mig således dele ovenstående spørgsmål op i to:

1. Hvad er hoved linjerne i den teknologiske udvikling inden for IP/Internet teknologien de næste fem år?

2. Hvilke konsekvenser har denne udvikling for muligheden for elektronisk overvågning?

Hvad er hoved linjerne i den teknologiske udvikling inden for IP/Internet teknologien de næste fem år?

IP/Internet teknologien åbner mulighed for adgang til Internettet fra forskellige typer terminaler. Traditionelt har terminalen været computeren, men også fjernsynet bruges flere steder som Internet terminal. Men altovervejende går udviklingen i retning af trådløs adgang til Internettet, altså adgang via mobiltelefonen.

Denne udvikling betyder at mobiltelefonens funktion udvides fra primært at håndtere taleopkald til at være en terminal, der giver adgang til en mængde andre tjenester. I fremtiden vil denne mobile terminal, samt det tilhørende SIM kort vil være bindeleddet mellem forbrugeren og en leverandør af telefoni og tjenester.

Indtil videre er det fortsat teleselskabet der varetager rollen som leverandør (kaldet Service Provider). Det er teleselskabet der sender forbrugeren regningen for de samtaler der føres på telefonen, og for de tjenester som hentes via terminalen på Internettet. Men vi begynder at se etableringen af en helt ny type virksomheder, der i højere grad er tilpasset denne nye virkelighed. Fordi tjenester ud over taleopkald forventes at blive dominerende i fremtiden søger teleselskaber, at alliere sig med f.eks. medievirksomheder, der kan levere indhold i

form af underholdning og nyheder til selskabets kunder. Og fordi det er teleselskabet, der kommer til at stå for afregningen med kunden, bliver der også behov for alliancer med finansvirksomheder, der kan håndtere denne del af kunderelationen. Alt i alt vil vi i fremtiden se en helt ny type leverandører, der er en sammensmeltning af Tele, Medie og Finansvirksomheder. Denne nye type leverandører har vi døbt Super Providers, og de kan bedst sammenlignes med et supermarked, der også repræsenterer en sammensmeltning af tidligere separate og enkeltstående butikker.

Disse Super Providere bliver knudepunkter i fremtidens trådløse samfund. De har relationen til kunden og de har den nødvendige infrastruktur. Som sådan vil de også udgøre magtbaser, der selvsagt kan både bruges og misbruges.

Derfor er politikernes udfordring også at se at denne udvikling, ikke længere er et telepolitisk anliggende men et mediepolitisk anliggende. UMTS / 3G mobiltelefoni er ikke blot en ny og smartere form for telefoni. Det er et helt nyt medie.

Disse Super Providers bliver i stand til at tilbyde kunden en bred vifte af tjenester og ydelser. Men frem for alt åbner teknologien op for muligheden for, at levere skræddersyede løsninger til hver enkelt kunde. Som en slags virtuelle bibliotekarer vil Super Providerne kunne tilbyde at lokalisere kunden og levere information og tjenester for kunderne, på grundlag af kundernes personlige profil og præferencer.

Hvilke konsekvenser har denne udvikling for muligheden for elektronisk overvågning?

Teleselskaberne/Super Providerne ligger som udgangspunkt inde med en række oplysninger om kunden: Navn, adresse, lokation, og IP/Internet adfærd. Og hvis udviklingen fortsætter som antaget kan de komme til at ligge inde med endnu flere kundeoplysninger. Denne udvikling repræsenterer et dilemma – et digitalt dilemma i relation til begrebet overvågning.

Ordet overvågning er negativt ladet og giver næsten automatisk associationer i retning af George Orwell og hans skræmmebillede af fremtiden. Men der er også flere eksempler på at denne overvågning bliver anvendt i samfundets tjeneste. I forbindelse med skudepisoden i Lufthavnen i Kastrup for nogle år siden, var det overvågningen af en rockers mobiltelefon der førte til at den pågældende med sikkerhed kunne placeres i Lufthavnen på gerningstidspunktet. Samme type overvågning betød at Statsanklageren kunne så tvivl om dele af Kurt Thorsens forklaring i retten omkring hans adfærd en bestemt dag.

Udviklingen går i retning af, at jo flere oplysninger en kunde er villig til at overgive om sig selv til leverandøren, desto bedre er leverandøren i stand til levere ydelser og tjenester, der passer til kundens behov og personlige profil. Muligheden er at de informationer vi, som

forbrugere og kunder giver videre til leverandørerne benyttes til at gøre vores hverdag meget nemmere. Det bliver muligt at checke ind på et hotel og finde at minibaren indeholder vores favoritdrikke, fjernsynet er indstillet til vores favoritkanaler og på mobiltelefonen ligger en liste over restauranter og underholdningssteder i nærheden, som matcher vores personlige smag.

Ingen enkeltperson, uanset lokalkendskab vil være i stand til at servicere kunden på samme måde som sådanne digitale bibliotekarer, der hurtigt og effektivt søger information på basis af hvad vi som kunder fortæller om vores (eller vores families) præferencer. Men for at Super Providerne kan blive i stand til at levere denne høje grad af service må de nødvendigvis komme til at ligge inde med store mængder informationer om kunden:

Kunde:	Navn, adresse, alder, køn
Kundeprofil:	Psykografisk profil, demografisk profil, historisk adfærd
Lokation:	Hvor kunden er hvornår (denne information er tilgængelig i real-time)
Teknologi:	Hvilken telefon og anden teknologi kunden benytter sig af
Økonomi:	Historiske transaktioner, type af kreditkort, kreditværdighed

Denne viden er i sagens natur personlig, men også mange penge værd for leverandørerne og naturligvis er der en risiko for at denne viden misbruges. Og hvis den misbruges vil resultatet være at vores privatliv bliver lige så privat som et postkort.

Det er denne situation der skaber det digitale dilemma: Jo flere oplysninger vi som kunder er villige til at give desto bedre en service er leverandøren i stand til at yde. Men jo flere oplysninger vi giver, desto større er naturligvis muligheden for elektronisk at overvåge vores færden. Vi kan naturligvis fravælge at afgive oplysninger, og således påberåbe os privatlivets fred, men så afskriver vi også de betydelige muligheder for en høj service, som leverandøren ellers kunne tilbyde. Når og hvis vi siger nej til at give oplysninger om os selv, siger vi i sagens natur også nej tak til at blive serviceret i det omfang som det ellers var muligt.

Det er nærliggende at konkludere at den fremtidige IP/Internet teknologi inden for mobiltelefoni og mobilt Internet åbner op for en betydelig mulighed for overvågning af forbrugeren. Jeg vil personligt, vælge en mere positiv vinkel og minde om at netop denne afdækning af kunden gør leverandøren i stand til at levere produkter og tjenester af en høj kvalitet. En sådan afdækning kan sidestilles med den, der finder sted når vi går til lægen eller søger vejledning hos en katolsk præst. Begge vil kun være i stand til at yde hvad der forventes af dem, hvis de får adgang til at afklare personlige forhold.

Det falder os helt naturligt at give personlige oplysninger og lade os monitorere, når vi forstår hvorledes disse oplysninger kan komme os til gode. Vi kalder det kundeservice. Når og hvis vi ikke forstår formålet med at indhente oplysninger, er vi tilbøjelige til at kalde det overvågning. Jeg tror der er mange mennesker, for hvem det endnu ikke er helt klart hvilke servicemuligheder IP/Internet teknologien åbner op for. De mennesker er mere tilbøjelige til at tale om overvågning end kundeservice. Jeg medgiver, at det med den teknologiske udvikling kan være svært at skelne mellem overvågning og service. Og netop derfor vil det være en skam hvis en manglende forståelse for teknologiens muligheder for at yde kunden service skal gøre udfaldet.

Ord forklaring:

SIM-kort. Et SIM-kort er den lille chip, som giver kunden adgang til mobilnettet. SIM-kort indeholder en række sikkerhedsfunktioner, og det er muligt at lagre oplysninger som adresser og telefonnumre på SIM-kortet

UMTS. [Universal Mobile Telephony System]. UTMS er afløseren for GPRS og GSM, og forventes indført i Danmark i 2002. En række lande i Europa har afholdt auktioner over rettighederne til UMTS-licenserne. Disse auktioner har indbragt lande som England og Tyskland mange milliarder kroner til skattekasserne. Grunden til at UMTS-rettighederne er så eftertragtede er, at båndbredden på dette net kan komme helt op på 2 Mbit og at UMTS bygger direkte på Internets IP-protokol. Dette betyder, at det vil blive muligt at sende TV, Internet, radio, telefoni og meget mere over det trådløse net. Dette er også grunden til at en så bred vifte af interessenter har vist interesse for auktionerne - både teleselskaber, IT-firmaer, medieselskaber, Internet Providere m.fl.

GSM. [Global System for Mobile Communication]. GSM er den mest udbredte standard for mobiltelefoni i dag. GSM blev udviklet i 1990 og afløste i Danmark standarden NMT. GSM findes i flere forskellige versioner, nemlig GSM 900, 1800 og 1900. GSM 1800 er den mest udbredte standard i Danmark og Europa, hvorimod GSM 1900 er mere udbredt i USA.GSM 900 er især velegnet til landområder hvor store geografiske områder skal dækkes, men hvor belastningen ikke er så stor.

Web sider:
http://www.privacy.net/
http://www.strandconsult.dk/

Yih-Jeou Wang, Dansk Industri

Spørgsmål:
- Hvad er producentens rolle i udviklingen?

Jeg skal sige tak for indbydelsen til at komme i dag og sige et par ord om industriens holdninger til elektronisk overvågning, herunder hvordan vi ser på fremtiden og udviklingen.

Det vil være naivt at tro, at vi kan afskaffe elektronisk overvågning. Og jeg tror heller ikke, at det vil være særligt klogt. Elektronisk overvågning er i dag en integreret del af danske virksomheders produktionsapparat om det så er til sikringsformål eller til fjernstyring og kontrol af apparater og maskiner i virksomhederne.

Og det er med dette udgangspunkt, at vi fra industriens side gerne vil forsøge at nuancere debatten om elektronisk overvågning, der ofte i den offentlige debat får en negativ og hysterisk klang.

Lad mig slå fast: Elektronisk overvågning er allerede i dag et faktum. Det er en integreret del af dansk produktion på mange forskellige niveauer. Uden elektronisk overvågning, kontrol og styring, ville vi have store problemer med produktiviteten og effektiviteten i virksomhederne.

Virksomhederne er i dag dybt afhængig af, at den elektroniske infrastruktur fungerer og er stabil.

Virksomhederne i dagens Danmark er dybt afhængig af at kunne høste effektiviseringsgevinster gennem intelligente apparater og maskiner, der måske befinder sig fysisk på forskellige geografiske lokationer. Effektiviseringsgevinster, der bygger på, at man via elektroniske netværk har mulighed for at overvåge, at kontrollere.

Virksomhederne har derfor ikke interesse i at overvåge sine medarbejdere, som det påstås i den offentlige debat. Det er medarbejderne, der i arbejdsprocessen overvåger.

Og set i lyset af, at f.eks. et af hospitalernes væsentligste opgaver er overvågning af patienter, mener jeg at mange af "skrækvisionerne" bør modereres kraftigt. Jeg vil gå så langt som at påstå, at elektronisk overvågning i sidste ende er med til at redde menneskeliv.

Jeg tror, at virksomhederne nu og i de kommende år vil bruge elektronisk overvågning i stor stil – ikke til at kontrollere mennesker, men til at kontrollere og overvåge apparater –

som led i de løbende effektiviseringer, der sker i virksomhedens produktionsapparat til glæde for dens konkurrencekraft.

Omvendt er jeg meget enig i den kritik, der er rejst i den offentlige debat om virksomheder, der skjult overvåger den elektroniske kommunikation, som medarbejdere udfører, om det så er telefonsamtaler eller e-poster.

Der tror jeg, at vi fra virksomhedsside skal holde den etiske fane højt: Vi skal sikre gennemskuelighed i den måde, hvorpå vi bruger elektronisk kommunikation, herunder hvem, der har mulighed for at se og høre hvad på arbejdspladsen. Og ikke mindst at det er kendt for alle! Der bør ikke være skjulte overvågningsaktiviteter, som i sidste ende kan gå hen og ødelægge et ellers tillidsfuldt samspil på en arbejdsplads mellem ledelsen og den enkelte medarbejder.

Når det så er sagt, så har jeg dog nogen gange svært ved at forstå, hvorfor kritikere af overvågning på arbejdspladsen fokuserer så kraftigt på elektronisk kommunikation, som i mine øjne ikke er principielt forskellig fra al mulig anden kommunikation på arbejdspladsen.

Elektronisk kommunikation, om det så er telefonsamtaler, faxer eller for den sags skyld e-poster, er kommunikation, som medarbejderen udfører i virksomheden, for virksomheden og i en professionel sammenhæng. Den enkelte virksomhed har derfor et naturligt behov for og også en ret til at få adgang til breve og e-poster, som medarbejderen har sendt eller modtaget på arbejdspladsen.

Og praksis er ofte, at andre medarbejdere i en kollegas fravær går ind og læser posten for netop at sikre, at alle aktiviteter kan fortsætte, selvom en enkelt medarbejder er syg, er på ferie eller på anden måde er fraværende i kortere eller længere perioder.

Under alle omstændigheder bør der være åbenhed omkring disse spørgsmål, som bør være et emne, der drøftes løbende mellem ledelsen og medarbejderne i virksomhederne.

Tak for ordet.

Klaus Rasborg, Roskilde Universitetscenter

Spørgsmål:
- Har brugen af elektronisk overvågning en selvforstærkende effekt?
- Hvordan kan individet/samfundet overskue og styre udviklingen?

Det er jo store spørgsmål, som der ikke gives nogle enkle svar på. Ikke desto mindre vil jeg i det følgende forsøge at indkredse nogle mulige svar. Til det formål kan det være nyttigt, i første omgang, at se lidt nærmere på, hvad det er for nogle samfundsmæssige mekanismer, der - set ud fra en sociologisk synsvinkel - kan siges at ligge til grund for det moderne "overvågningssamfund."

På et overordnet plan kan fremkomsten af nye former for overvågning, disciplin og kontrol ses som forbundet med fremkomsten af det moderne, industrielle (kapitalistiske) samfund. Den engelske sociolog Anthony Giddens skelner mellem fire forskellige grundlæggende institutioner, som han mener spiller en central rolle i det moderne samfund, nemlig *kapitalisme*, *industrialisme*, *overvågning* og *militærmagt*.[1] I det følgende vil jeg fokusere på overvågningsdimensionen, selv om den selvfølgelig ikke kan adskilles fra de tre øvrige dimensioner.

Med *overvågning* tænker Giddens på det moderne "overvågningssamfund", sådan som det især er blevet analyseret af den franske idéhistoriker og kulturanalytiker Michel Foucault (1926-1984).[2]

For Foucault er det moderne samfund ikke slet og ret ensbetydende med fremskridt og øget oplysning - det *disciplinerer* også sine borgere. Foucault opfatter *fængslet* som et mønstergyldigt eksempel på dette, idet fængslets overvågning, strenge disciplin og kontrol af de indsatte efter hans opfattelse også kendetegner en række andre centrale institutioner i det moderne samfund: kernefamilien, skolen, fabrikken, kasernen og sindssygehospitalet.

I det moderne samfund sættes videnskaben og fornuften i højsædet. Men netop derfor søger det moderne samfunds "fængselslignende" institutioner også at afgrænse og

---

[1] Anthony Giddens: *Modernitetens konsekvenser.* København: Hans Reitzels Forlag, 1994 [1990], s. 53ff.

[2] Michel Foucault: *Overvågning og straf. Det moderne fængselsvæsens historie.* København: Rhodos, 1977 [1975].

udelukke alt hvad, der modsætter sig fornuftens herredømme og den etablerede samfundsorden: de gale, de kriminelle, de arbejdsløse osv.

Derfor kommer *indespærring*, *overvågning* og *kontrol* efter Foucaults opfattelse til at spille en central rolle i det moderne samfund. Set med Foucaults briller gennemsyres det moderne samfund af overvågningsstrategier, magtrelationer og disciplineringsteknikker, som tager sigte på at normalisere alt hvad, der måtte afvige fra samfundets fremherskende normer og værdier. Magten bliver "allestedsnærværende", dvs. den kan ikke entydigt lokaliseres og afgrænses til bestemte samfundsmæssige institutioner som f.eks. stat eller virksomheder. Magt, overvågning og kontrol udgør ifølge Foucault en kompliceret "strategisk situation" i det moderne samfund.

Som illustration af, hvordan fængslet kan fungere som en overvågningsteknologi, benytter Foucault det såkaldte *Panoptikon* (fra gr. *pan*, al + gr. *optikon*, vedr. synet), som var et sindrigt fængselssystem, der i midten af det 19. århundrede blev udviklet af den engelske filosof og jurist Jeremy Bentham (1748-1832).[3] Det særlige ved Panoptikon var, at det var bygget op på en sådan måde, at nogle få fangevogtere på én og samme tid var i stand til at overvåge og kontrollere samtlige indsatte: "Panoptikon" er en cirkulær cellebygning med et observationstårn i midten. Fra dette centrale sted foregår overvågningen. Tårnet er indrettet sådan, at der er fri udsigt til alle celler, samtidig med at det på grund af et sindrigt skodde-system er umuligt at se ind i observationstårnet. Fra dette sted kan man se alt, uden selv at blive set".[4] Panoptikon var med andre ord baseret på et overvågningsprincip, hvor det er *de få*, der overvåger *de mange*.

I sin oprindelige udformning vandt Panoptikon ikke nogen større udbredelse, men i det 19. århundrede blev række af dets grundlæggende principper benyttet i forbindelse med bygningen af fængsler i USA, England samt en række europæiske lande.[5]

I dagens samfund kan f.eks. videoovervågning af butiksarealer, parkeringskældre, offentlige toiletter m.m. ses som en videreudvikling af det panoptiske overvågningsprincip, idet den ny videoteknologi muliggør, at forholdsvis få personer/kameraer kan overvåge og kontrollere et i princippet uendeligt antal mennesker. Sociologisk set må en sådan øget overvågning af det offentlige rum antages at øge den sociale kontrol, dvs. samfundets kontrol med vores gøren og laden. På det individuelle plan kan dette føre til øget

---

[3] Foucault, s. 176-201.

[4] Joachim Wrang: *Cellen og øjet - om overvågning, forbrydelse og straf*. Århus: Klim, 2000, s. 27.

[5] F.eks. kan det nævnes, at de panoptiske principper angiveligt har spillet en rolle i forbindelse med opførelsen af Statsfængslet i Vridsløselille, jf. *Cellen og øjet*, s. 22

selvovervågning og selvkontrol, idet vi i stigende grad bliver bevidste om, at vi kan blive stillet til regnskab for enhver af vores handlinger.

I det senmoderne mediesamfund antager overvågningen stadig nye former. Den rivende udvikling af de elektroniske kommunikationsmidler (videoteknologier, tv-satellitter, computer, Internet, mobiltelefon osv.) har gjort verden til en "global landsby", hvor vi i stigende grad løsrives fra vores bundethed til rummet, stedet og lokaliteten.

På Internettet kan man 24 timer i døgnet følge med i tilværelsen hos folk, der har ladet deres bolig forsyne med web-kameraer. I tv-serier som f.eks. *Robinson* forvandles almindelige, anonyme danskere med et slag til kendte og feterede "mediepersonligheder", hvis liv alle interesserer sig for og følger med i. Den foreløbige kulmination på denne ekstreme voyeurisme er tv-serien *Big Brother*, som nu også introduceres i Danmark. Hér kan man live på Internettet, samt i daglige tv-sammendrag, følge med i alt hvad et antal personer, der bor sammen i en bolig overplastret med videokameraer, foretager sig - morgen, middag og aften. På tankevækkende vis er disse nye voyeuristiske tendenser beskrevet i filmene *The Truman Show* og *Ed-tv*.

Hvor Panoptikon var baseret på, at det er *de få*, der overvåger *de mange*, synes der altså i stigende grad at være tale om, at det er *de mange*, der overvåger *de få*. Den engelske sociolog Zygmunt Bauman taler derfor om, at blikket i stigende grad bliver *synoptisk* (fra gr. *syn*, med, sammen + gr. *optikon*, vedr. synet).[6]

Forudsætningen for disse nye overvågningsprincipper er, som det allerede vil være fremgået, de nye informationsteknologier. Og det er klart, at jo mere avancerede disse nye teknologier bliver, desto mere kan overvågningsteknikkerne forfines.

En øget tv-overvågning kan, som nævnt, være med til at øge mistilliden og utrygheden blandt mennesker, idet den gør enhver til en potentiel lovovertræder. Den øgede selvkontrol, der meget vel kan tænkes at være følgen, er på tankevækkende vis beskrevet af en ung mand, der - aldeles grundløst viste det sig siden hen - på baggrund af videooptagelser blev fyret fra sin arbejdsplads i Brugsen, angiveligt fordi han havde stjålet nogle cigaretter: "Jeg er bevidst om det hele tiden. Hvis jeg kommer til at lægge noget uden for kameravinklen, så tror de måske, at jeg har stjålet. Så jeg sørger for at vise kameraet det hele. Jeg tror, at den følelse vil sidde i mig resten af livet. ... Jeg tager det også med hjem. Kan aldrig rigtig slappe af, fordi jeg spekulerer over, om jeg har gjort noget forkert i løbet af dagen." [7]

---

[6] Zygmunt Bauman: *Globalisering. De menneskelige konsekvenser*. København: Hans Reitzels Forlag, 1999 [1998].

[7] Pernille Tranberg: ANår kameraet tager fejl", artikel i *Politiken,* d. 26/1-2000, 3. sek., s. 5.

Omvendt er der også dem, der peger på eventuelle positive effekter af de nye overvågningsteknologier. Et af hovedargumenterne er her, at en øget tv-overvågning dels kan forebygge kriminalitet, dels kan lette opklaringen af begåede forbrydelser: "Erfaringerne fra ind- og udland viser, at tv-overvågning har en forebyggende virkning over for en række former for kriminalitet. Samtidig har det vist sig, at tv-overvågning bidrager til at opklare forbrydelser, som ellers ville forblive uopklarede."[8]

De nye overvågningsteknologier synes med andre ord at have et janusansigt. På den ene side kan det ikke udelukkes, at de - i hvert fald på kort sigt - kan have en præventiv effekt; på den anden side kan de - stik mod hensigten - føre til øget selvkontrol og mistillid mellem mennesker: "Tv-overvågning befinder sig altså i et spændingsfelt mellem forebyggelse og krænkelse. Spørgsmålet er, hvor balancepunktet er."[9]

Selv hvis argumentet om tv-overvågningens gunstige effekter i forhold til forebyggelse og opklaring af kriminalitet skulle have noget på sig, kan man ikke desto mindre spørge, om ikke der er tale om en *teknologisk* løsning på *sociale problemer*. Altså at problemer, der måske i højere grad skyldes en utilstrækkelig social integration i det civile samfund - familien, skolen og lokalsamfundet - søges løst ved at indføre stadig mere avancerede overvågningssystemer. Samtidig kan man frygte, at en eventuel kriminalitetsforebyggende effekt som følge af tv-overvågning blot vil betyde, at kriminaliteten flytter andetsteds hen. Hermed kan der sættes en uendelig spiral i gang, hvor vi, i et forsøg på at være på højde med kriminalitetsudviklingen, lader stadig flere områder overvåge.

Denne selvforstærkende tendens kan fremmes yderligere som følge af: "... disse "tryghedsforanstaltningers" kommercialisering og den produktudvikling osv., der ligger heri, samt at én "kunde" hele tiden skaber en ny, nemlig naboen, nabobutikken, nabosommerhuset, nabogaden, eller hvad det nu er, pga. frygten - som kan være helt reel - for overflytning fra det mere til det mindre sikrede. Skræmmevisionen for enden - hvis der findes en ende? - af denne udvikling er de med mure og porte beskyttede boligområder i Nord- og Sydamerika, butikscentre der er opbygget efter principper hentet fra gammeldags fængselsteknologi, biler der minder om tanks osv. I dette samfund har opdelingen mellem

[8] Eva Smith: ATV-overvågning i spændingsfeltet mellem forebyggelse og krænkelse", i: *TV-overvågning. Mellem forebyggelse og krænkelse*. Det Kriminalpræventive Råd, Marts, 2000, s. 4.

[9] Eva Smith, s. 4.

"vindere" og "tabere" udviklet sig til det fuldkomne. Tilværelsen er gennemgribende "privatiseret" og offentlige "frie" rum er afskaffet."[10]

Hvis vi med andre ord blot lader den (overvågnings-)teknologiske udvikling "løbe løbsk", og ukritisk tror på, at nye teknologier er gode, blot fordi de er nye, så kan der være grund til at formode, at brugen af elektronisk overvågning vil have en selvforstærkende effekt. Og hvis vi ukritisk tror på, at sociale problemer, som måske har deres rødder et helt andet sted, kan løses ad teknologisk vej, så kan der være grund til at formode, at brugen af elektronisk overvågning vil have en selvforstærkende effekt.

Hvis vi derimod vover, at anfægte "udviklingen", og insisterer på, at de mange nye avancerede teknologier, vi omgiver os med i det moderne samfund, i sidste instans er skabt af os selv, og derfor også kan kontrolleres af os - selvom det nogle gange kan synes som om, at de er ved at tage magten fra os - så er der åbnet op for en diskussion af, om vi ønsker at leve i et samfund, hvor overvågning spiller en stigende rolle. Hermed er vi fremme ved det andet spørgsmål om, hvad vi kan gøre for bedre at kunne overskue og styre udviklingen.

På et overordnet plan kan man sige, at det må dreje sig om, at styrke den demokratiske diskussion af, i hvilken retning vi ønsker at vort samfund skal udvikle sig. I forbindelse med sin teori om "risikosamfundet" peger den tyske sociolog Ulrich Beck på, at borgerhøringer og borgerpaneler - altså ting, der til forveksling minder om konsensuskonferencer - vil kunne være med til at styrke den folkelige indflydelse, og til at forbedre den demokratiske beslutningsproces i forbindelse med de komplicerede spørgsmål om indførelsen af nye teknologier, som vi ofte har svært ved at overskue konsekvenserne af (overvågningsteknologi, genteknologi, bioteknologi m.v.).[11]

En forudsætning for, at sådanne fora til styrkelse af den demokratiske diskussion skal kunne have nogen effekt er imidlertid, at beslutningerne ikke er taget på forhånd, at der brydes med eksperternes "monopol" på sandheden, og at der er en åben dialog mellem de deltagende parter.

På et mere konkret plan må det dreje sig om, at blive enige om nogle kriterier, hvorudfra vi kan vurdere fordele og ulemper ved de nye teknologier. Et udgangspunkt

---

[10] Flemming Balvig: *RisikoUngdom. Ungdomsundersøgelse 1999*. Det Kriminalpræventive Råd, København, 1999, s. 239f.

[11] Ulrich Beck: *Risikosamfundet. På vej mod en ny modernitet.* København: Hans Reitzels Forlag, l997 [l986]; Ulrich Beck: *Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung*. Frankfurt/M: Suhrkamp, 1993.

kunne her være Det Kriminalpræventive Råds fem anbefalinger i forbindelse med tv-overvågning:[12]

1. Overvåg ting og steder - ikke personer
Kravet er her, at tv-overvågningen på den ene side skal have en forebyggende eller opklarende effekt, og på den anden side skal medføre større tryghed. Det kan f.eks. dreje sig om overvågning i pengeinstitutter og posthuse, butikker og indkøbscentre, tankstationer og togstationer.

2. Klare retningslinier når udstyret er installeret
! *Brug af materialet*
Hvad gør man, hvis man "finder noget" på båndene? Og hvem må se dem?
! *Opbevaring*
Hvordan skal videobåndene opbevares?
! *Overdragelse til "tredjepart"*
Til hvem og under hvilke betingelser kan man overdrage båndene?
! *Sletning*
Hvornår skal båndene slettes?
Her drejer det sig altså om krav, der kan styrke retssikkerheden.

3. Fire centrale aspekter bør overvejes
! *Det præventive aspekt*
Har tv-overvågning en kriminalpræventiv effekt? I givet fald, hvori består den?
! *Opklaringsaspektet*
Bidrager tv-overvågning til opklaring af kriminalitet?
! *Tryghedsaspektet*
Giver tv-overvågning en øget tryghed? Er den reel eller falsk?
! *Krænkelsesaspektet*
Kan tv-overvågning være personligt krænkende? Og hvor går grænsen?

Her drejer det sig altså om, at afveje det præventive aspekt på den ene side mod krænkelsesaspektet på den anden side.

4. Man bør skelne mellem fire områder for overvågning
! *Forretninger og erhverv*
! *Arbejdspladsen*
! *Den private sfære*
! *Det offentlige rum*

[12] Det følgende er baseret på anbefalingerne i: *TV-overvågning. Mellem forebyggelse og krænkelse*. Det Kriminalpræventive Råd, Marts, 2000, s. 6-9.

En mindre empirisk undersøgelse, som Statens Information/Gallup har lavet for Det Kriminalpræventive Råd, viser, at 60 pct. af danskerne er positive over for, at der kommer mere tv-overvågning. Går man nærmere ind på forskellige typer af tv-overvågning, viser der sig imidlertid betydelige forskelle i danskernes holdninger: "Som tommelfingerregel kan man sige, at jo tættere kameraet kommer på den enkelte person, des mindre positiv er holdningen til tv-overvågning."[13]

Således stiller langt den overvejende del af de adspurgte sig "overvejende positivt" til tv-overvågning af banker, tankstationer og togstationer (henholdsvis 93, 90 og 88 pct.). Derimod er det kun er en mindre del, der stiller sig "overvejende positivt" til tv-overvågning af omklædningsrum, på arbejdet og på offentlige toiletter (henholdsvis 11, 18 og 20 pct.).[14]

5. Man bør bevare den sunde fornuft

Det anbefales her, at man bevarer den kritiske indstilling til brugen af tv-overvågning, og at man i den forbindelse benytter de fire ovenstående anbefalinger som grundlag for en nærmere afklaring.

Den ovennævnte undersøgelse viste også, at der i befolkningen er et udbredt ønske om, at området bliver reguleret. Et problem i denne forbindelse er imidlertid, at den teknologiske udvikling ifølge sagens natur tenderer til hele tiden at være ét skridt foran lovgivningen og det politiske system. Så meget desto vigtigere er det imidlertid, at vi søger at fastholde en demokratisk kontrol med den teknologiske udvikling, således at den ikke tager magten fra os. Det er klart, at der her også ligger en stor opgave for fagforeningerne med hensyn til at stille krav til, begrænse, eller eventuelt søge helt at eliminere tv-overvågning på arbejdspladsen, overvågning af de ansattes e-mails, brug af Internet m.v.

Lad mig afslutningsvis forsøge at sammenfatte ovenstående overvejelser i nogle få, enkle punkter:

! Det gælder om, at fastholde den kritiske sans. Nye teknologier er ikke nødvendigvis gode, blot fordi de er nye.

! Det gælder om, at afveje fordele mod ulemper. Kun hvis de eventuelle fordele vejer tungest, kan man overveje at indføre overvågningsteknologier. Samtidig bør man overveje, om sociale problemer - som f.eks. kriminalitet - kan løses ad teknologisk vej.

---

[13] Det Kriminalpræventive Råd, s. 12f.

[14] Det Kriminalpræventive Råd, s. 13.

! Det gælder om, at styrke den folkelige indflydelse og forbedre den demokratiske dialog i forbindelse med indførelsen af nye teknologier. F.eks. har man på det genteknologiske område vedtaget en toårig tænkepause.
! Sidst, men ikke mindst, bør vi overveje, hvad det er for et samfund, vi ønsker at leve i. Ønsker vi et samfund baseret på mistillid, kontrol og afstand mellem mennesker? Eller ønsker vi et samfund baseret på tillid og fællesskab?

Tema 4: Retssikkerhed vedrørende elektronisk overvågning

Jan Carlsen, Instituttet for Datasikkerhed

Spørgsmål:
- Hvordan forhindres misbrug af oplysninger indsamlet uden noget umiddelbart formål (elektroniske spor)?

Kommunikation mellem mennesker er en nødvendighed. Til brug herfor er der gennem generationer udviklet forskellige hjælpemidler, der kan formidle denne kommunikation hurtigt og over fysiske afstande mellem parterne. Som eksempler herpå fra nyere tid kan nævnes telegrafen, telefonen, radio og TV og sidst, men ikke mindst internettet.

Når internettet anvendes som hjælpemiddel er det vigtigt at forstå, at selvom der sidder en person som afsender af et budskab i den ene ende og tilsvarende en person som modtager i den anden ende, så formidles budskabet af via flere forskellige computere undervejs. Selv om der ikke er en person i den sidste ende af forbindelsen, så er personen erstattet af en computer, der kan udføre de handlinger (eks. fremfinde informationer og returnere disse) som afsenderen har bedt om.

Uanset eksemplerne er der tale om en række computere, der samarbejder for at omsætte afsenderens anmodning til noget for computerne forståeligt, at dirigere det gennem et verdensomspændende netværk til den rette modtager for der at iværksætte den ønskede anmodning og returnere svaret til afsenderen igen.

Disse computere (der kan være mange forskellige ting fra eksempelvis mobiltelefoner, palme tops, pc'ere og til store main-frame computere) har en ting til fælles - det er teknologi, der kan (og vil) gå i stykker eller fejlfungere. Dette er en kendt sag og derfor udfolder såvel producenterne som brugerne heraf store anstrengelser for at undgå dette og dersom dette ikke er muligt, da hurtigst muligt at kunne genoprette situationen med så lille forsinkelse og med så små tab af informationer som muligt.

For at kunne gøre dette, er det nødvendigt for de computere der er involveret heri, at lagre de informationer de modtager og skal sende videre. Skulle informationerne så gå tabt undervejs til eller i næste led i kæden, kan de fremskaffes fra det foregående.

Også hos modtageren foretages der en registrering af, hvad der er foregået ud fra ovennævnte hensyn, men også andre forhold kan have indflydelse herpå. Der kan således være tale om:

- lovgivningskrav (et banalt eksempel fra Danmark hvor f.eks. bogføringsloven stiller krav til registreringer, hvis der er penge involveret),

- kommercielle krav og ønsker, hvor mange forhold kan gøre sig gældende:

    - eksempelvis kan det være en rent praktisk ting at vide, hvem der har rekvireret en given ydelse, og hvortil regningen skal sendes/debiteres

    - et behov for at vide, hvor mange og hvorfra forespørgsler kommer af hensyn til kapacitetsberegninger af udstyret

    - tilsvarende kan der også være af interesse at vide hvem der forespørger en given ydelse med henblik på at sælge eller videreformidle informationer herom til andre eller beslægtede virksomheder. Eksempelvis kan information om, hvem der har bestilt vielsesringe have interesse for brudekjolesælgere, ejendomsmæglere, møbelsælgere, babyudstyrsforretninger etc. Her findes mange eksempler fra stort set alle brancher.

    - ønsket om at kunne give en bedre service kan også ligge bag registreringer. Mange dot.com firmaer arbejder p.t. på at lære dine vaner at kende, således at de hurtigt kan lede dig frem til det du måtte ønske - eller måske give dig et godt tilbud på en nyudkommen bog, som formodentlig har din interesse, baseret på dine tidligere køb.

Konklusionen på dette er, at computere registrerer informationer af mange forskellige grunde, til brug for mange forskellige formål fra fejlretning, af lovgivningsmæssige krav, af forretningsmæssige årsager o.s.v. Det er også, hvad computere er skabt til - at registrere, lagre og fremfinde informationer, samt sætte disse i et nyt sammenhæng. Det kan derfor ikke undre, at når man er på internettet efterlades der masser af spor mange forskellige steder over hvem man har kommunikeret med og i princippet også hvad man har foretaget sig.

Præcis hvor disse informationer ligger, hvor længe og hvem der måtte have adgang til dem kan der ikke svares på. I nogle tilfælde vil det være op til modtageren alene at bestemme hvad der skal gemmes og hvor længe, samt hvem der må få adgang hertil, i andre tilfælde kan det være underlagt lovgivningsmæssige eller frivillige bestemmelser. Det kan derfor være meget forskelligt fra den ene gang til den anden.

Man kan inddele informationerne i 4 kategorier:

1. Oplysninger der afgives frivilligt og bevidst - eksempelvis kreditkortnummer i forbindelse med et køb, navn og adresse og evt. e-mailadresse hvis man ønsker noget tilsendt. Der kan naturligvis være mange flere oplysninger i denne kategori.

Oplysninger af denne type vil administreres af modtageren, der bestemmer over dets anvendelse. Der kan være lovgivningsmæssige bestemmelser der regulerer dette (afhængigt af pågældende lands bestemmelser) eller virksomheden kan have indgået i et forbrugerbeskyttelsesprogram, der fastsætter sådanne regler. I sidstnævnte tilfælde vil dette normalt kunne ses på web'ens hovedside.

Man bør nok notere sig, at selv om informationerne måtte være underlagt lovgivning eller andre begrænsninger ad frivillig art, er dette ingen garanti for at disse informationer kan komme til uvedkommendes kendskab eller kunne misbruges af 3. part. Årsagerne hertil kan skyldes manglende sikkerhed på web-sitet, fejl, sjuskeri eller bevidst misbrug.

2. Oplysninger som udveksles mellem afsender- og modtagercomputer er bl.a. oplysninger om browser og version, operativsystem, oplysninger om domæne og om hvorfra man er blevet henvist til dette sted (hvor man har været sidst).

3. Evt. oplysninger (Cookies) der sendes fra modtagerens computer til afsenderen og placeres på harddisken i dennes computer. Indholdet heraf bestemmes af den website man besøger (her benævnt modtageren) og vil i de fleste tilfælde være harmløse informationer og som websitet bruger til senere at kunne genkende den besøgende. Brugeren kan selv bestemme, hvorvidt sådanne cookies skal afvises.

4. De oplysninger som web-sitet kan registrere på basis af brugerens adfærd på web-suiten. Eksempelvis hvad er det brugeren ønsker oplysninger om, hvad interesserer brugeren, hvor længe er brugeren på hvilke sider, hvad ønsker brugeren nærmere information om o.s.v.

Alle disse informationer kan såvel bruges og misbruges af modtagerne uden at brugeren der har efterladt disse spor, har nogen indflydelse herpå, og som oplægget til dette indlæg spørger, hvorledes undgår man det?

For at foregribe begivenhedernes gang må man nok konkludere, at dette ikke kan lade sig gøre, men risikoen herfor kan reduceres. Konklusionen er baseret på følgende:

1. Al færden på Internettet afsætter spor. På grund af nettets opbygning og funktionalitet vil disse spor, uden brugerens viden, kunne være placeret i flere lande. En lokal dansk lovgivning vil derfor være uden større effekt. En international lovgivning, der eventuelt ville forbyde anden brug end en af brugeren godkendt anvendelse, vil - om det ville være

muligt at gennemføre en sådan (hvilket det næppe er) ikke løse problemet, men i bedste fald kun reducere dette. Lovgivning forhindrer ikke fejl, sjusk og misbrug.

2. Af de informationer der afgives, er det brugeren der bestemmer, hvorvidt informationer af type 1 som ovenfor beskrevet skal afgives. Er der tale om køb, der forudsætter betaling og fremsendelse af en købt bestilt vare, kan en anonymitet ikke opretholdes ifølge sagens natur.

3. Er der tale om anden form for modtagelse af informationer (hvor der ikke er tale om betaling for ydelser) kan en anonymitet opretholdes i et vist omfang ved at optræde under "falsk" navn - evt. med et dertil oprettet e-mail-konto (hos eksempelvis www.hotmail.com til evt. modtagelse af password, bruger-id m.v. Samtidig bør der lukkes af for modtagelse af Cookies. Dette betyder ikke, at der ikke foretages registreringer som ovenfor anført, men disse registreringer kan ikke umiddelbart tilbageføres til brugeren og er derfor ikke informationer der kan misbruges til skade for afsenderen. Dog vil en politimæssig efterforskning (evt. med brug af dommerkendelser) i de fleste tilfælde kunne afsløre forbindelsen mellem afsender og modtager.

Undtagelsen herfra er såfremt brugeren har foretaget et download af et eksekverbart program (det være sig skjult i et andet program), der efterfølgende udføres fra brugerens maskine. I så fald kan alt ske uden at brugeren har kontrol hermed. Denne situation ligger imidlertid udenfor det rejste spørgsmåls rammer.

4. En bedre mulighed for at sikre sin anonymitet på nettet er gennem anvendelse af en proxy-server, således at de informationer, der videresendes til modtageren optræder i et og alt, som kommende fra denne proxy-server. Der er enkelte services af denne type på nettet - eksempelvis www.anonymizer.com. Dette betyder dog blot, at brugerinformationerne nu ligger på proxy-serveren (hvorfra de kan fremfindes af indehaveren og de lokale myndigheder) frem for hos modtageren.

Sammenfattende må det siges, at nogen fuldstændig sikring mod misbrug af informationer afgivet uden noget umiddelbart formål ikke er mulig at opnå om end risikoen kan herfor kan reduceres.

Ideelt set ville det være ønskeligt at der var et internationalt regelsæt, der satte regler for anvendelsen af sådanne informationer for at begrænse risikoen, men dette vil i givet flad tage lang tid. Dertil kommer, at man næppe kan forvente at en sådan lovgivning vil kunne accepteres af alle lande, og herved vil den i et vist omfang være illusorisk.

Endvidere ville det være ønskeligt, at der på browseren var en knap man kunne aktivere/deaktivere, og som sikrede fuldstændig anonymitet. Dette er dog ikke teknisk muligt på nuværende tidspunkt og det er næppe sandsynligt at det vil komme - ikke mindst

fordi dette er i modstrid med den p.t. værende kommercialisering af diverse web-sites med henblik på at give en bedre service gennem at kende kunderne bedre.

Indtil da kunne man måske overveje at lade Internet Service Providerne udvide deres service med en anonym proxy-server mulighed eller alternativt lade staten stille en sådan til rådighed. Adgang til informationerne heri ville kun være mulig for visse betroede medarbejdere hos ISP eller for politi med dommerkendelse. Omkostningerne hertil vil i sidste ende skulle betales af forbrugerne enten via direkte betaling eller via forbrugsskatter - afhængig af den valgte løsning.

Med venlig hilsen

Jan Carlsen

Henrik Waaben, Datatilsynet

Spørgsmål:
- Hvilke muligheder er der for at regulere og kontrollere registrering af elektronisk indsamlede oplysninger, opbevaring af dem, kommerciel udnyttelse og samkøring af disse?

Dette spørgsmål skal besvares ud fra reglerne i lov om behandling af personoplysninger (persondataloven). Loven gælder bl.a. for elektronisk behandling af oplysninger om personer.

Persondataloven stiller bl.a. følgende krav:

1. Indsamling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål (§ 5, stk. 2).

2. Indsamlingen og registreringen af oplysninger skal have hjemmel i persondataloven (§§ 6-8), f.eks. være nødvendig for at varetage en berettiget interesse.

3. Indsamlingen og registreringen må ikke være i strid med anden lovgivning, f.eks. lov om forbud mod tv-overvågning.

4. De personer, der registreres, skal som hovedregel have oplysning herom, herunder som et minimum have at vide, hvem der registrerer oplysningerne (virksomhedens navn og adresse) samt formålet med registreringen (§§ 28-29).

5. En registreret person har ret til indsigt i de oplysninger, der angår den pågældende (§ 31).

6. Der skal være den fornødne datasikkerhed omkring oplysningerne. Dvs. at de ikke må komme til uvedkommendes kendskab, blive misbrugt eller i øvrigt behandlet i strid med loven (§ 43).

7. De registrerede personer kan klage til Datatilsynet, hvis de er utilfredse med registreringen. Så vil Datatilsynet undersøge, om reglerne i persondataloven er overholdt (§ 58).

8. Oplysningerne skal slettes, når virksomheden ikke længere har et sagligt behov for dem (§ 5, stk. 5). Sletning vil typisk skulle ske inden for en forholdsvis kort frist, f.eks. 30 dage.

I praksis vil det være sådan, at personoplysninger, der er indsamlet som led i elektronisk overvågning, ikke må anvendes til kommercielle formål. Oplysningerne må som hovedregel heller ikke samkøres med andre registre.

Vicepolitimester Arne Gram, Det Kriminalpræventive Råd

Spørgsmål:
- Hvilket behov vil der være for at regulere lovgivningen, når selv "bagatelagtige" lovovertrædelser opdages?
- Hvis elektronisk overvågning skaber en forventning om forøget sikkerhed for de overvågede (fx på plejehjem), medfører det så nogle særlige ansvarsmæssige forhold for dén hvis den hvis job det er at overvåge?

Mit navn er Arne Gram. Jeg er vicepolitimester hos Rigspolitichefen og til daglig sekretariatschef i 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 kort 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 "Retssikkerhed vedrørende elektronisk overvågning" .
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 to underspørgsmål:

* Hvilket behov vil der være for at regulere lovgivningen, når selv bagatelagtige" lovovertrædelser opdages?

* Hvis elektronisk overvågning skaber en forventning om forøget sikkerhed for de overvågede, medfører det så nogle særlige ansvarsmæssige forhold for dén, 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

På grund af den meget smalle tidsfrist for mit indlæg 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 for tv-overvågning 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, "udspioneret" og kontrolleret.

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 dén, 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 borger-undersøgelse.

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.

Tema 5: Registrering og brug af oplysninger om personer

Henrik Waaben, Datatilsynet

Spørgsmål:
- Hvem har rettighederne til information og brugen af denne?
- Hvor meget ved private virksomheder og offentlige myndigheder og hvad bruger de det til - nu og i fremtiden?

Persondataloven tager ikke stilling til, hvem der *ejer* registrerede personoplysninger. Loven indeholder derimod regler for, under hvilke omstændigheder en virksomhed eller myndighed kan *disponere* over registrerede personoplysninger.

Hvis reglerne i persondataloven overholdes, kan en virksomhed eller myndighed bruge registrerede oplysninger til det saglige formål, som de er indsamlet til. Oplysningerne kan i et vist omfang også bruges til andre saglige formål, men en sådan efterfølgende brug må ikke være uforenelig med det formål, som oplysningerne oprindeligt blev indsamlet til. Dette følger af lovens § 5, stk. 2.

Loven indeholder i kapitel 10 en række regler, der giver registrerede personer ret til at gøre indsigelse mod, at en virksomhed eller myndighed behandler oplysninger om en. F.eks. kan en registreret person modsætte sig, at en virksomhed videregiver oplysninger om ens forbrug og indkøbsvaner til andre virksomheder med henblik på markedsføring. Kan en person ikke komme overens med en virksomhed eller myndighed om en behandling, er der mulighed for at klage til Datatilsynet.

I praksis kan det være svært at skaffe sig overblik over, hvilke oplysninger private virksomheder og offentlige myndigheder ligger inde med om en selv, og hvad de bliver brugt til. Men de nye regler i persondataloven om oplysningspligt vil bidrage til at skabe gennemskuelighed omkring registrering og brug af personoplysninger. Det er reglerne i §§ 28 og 29, som giver registrerede personer ret til at blive oplyst om, hvem der indsamler oplysninger om en selv, og hvad de skal bruges til. Endvidere kan de registrerede personer få indsigt i oplysningerne efter reglerne i § 31.

Steffen Stripp, PLS-Rambøll

Spørgsmål:
- Hvem bør have rettighederne til information og brugen af denne?
- Hvad sker der med registrerede personlige oplysninger når offentlige og halv-offentlige institutioner bliver privatiserede/udliciterede?

Hos mand og kvinde er det gode navn,
min herre, sjælens bedste smykke;
at stjæle guld er bras, er noget, intet
var mit, er hans, har været træl for tusind;
men den der ta'r fra mig mit gode navn
han stjæler, hvad der ikke gør ham rig;
men mig gør det i sandhed fattig.
(Shakespeare i Othello)

Hvem har og hvem bør have rettighederne til information og brugen heraf?

Et fundamental spørgsmål, som det er godt at holde sig for øje, er, hvis oplysninger er de personlige oplysninger. Tilhører de den som har registreret dem, offentligheden eller personen selv. Det er min opfattelse at en persons data er en del af personen. Personen er en enhed i tid og rum. Han kan identificeres gennem sin krop og sine handlinger og har både fysiske og psykiske egenskaber. Personen bliver synlig og ansvarlig gennem den skikkelse han præsenterer for andre. Personen værdighed består i at han kan distancere sig fra andre. Personens liv, hans biografi, er totaliteten af hans handlinger. Retten til livet stammer fra kroppen. Retten til personoplysninger stammer fra personen. Svaret på spørgsmålet må derfor være, at de personlige oplysninger tilhører personen. Vi ***er*** vores personoplysninger.

Persondatabeskyttelsen er derfor også, som en del af privat livets fred, en menneskeret.

Der er i juraen ikke et svar på hvis de personlige oplysninger er. Man kan ikke tale om at man "ejer" dem i juridisk forstand og man kan heller ikke anvende ophavsretten, som jo ellers taler om en eneret. Det er min erfaring, at det er en god vinkel at tænke sig et lån. Når man har givet andre sine personoplysninger har dem kun til låns. Det betyder, at de har en

vis brugsret til dem - men de kan selvsagt ikke bruge dem til hvad som helst. Man kan ikke bare overdrage noget man har lånt til andre. Man kan ikke lave bøffer af ridehesten. Osv.

Ofte omtales spørgsmålet om overvågning - specielt i den juridiske litteratur - som en afvejning eller balance mellem forskellige hensyn eller interesser. Denne indfaldsvinkel kan let føre til en uheldig nedtoning af udgangspunktet, at der er tale om beskyttelse af privatlivets fred. Det er vigtigt at fastholde dette udgangspunkt, som let lader sig udvande over for modstående hensyn om effektiv offentlig forvaltning (skattekroner), hindring af svindel og kriminalitet og lignende.

Glashus
I diskussioner om privatliv og overvågning oplever jeg ofte, at to mundheld står over for hinanden. På den ene side:

"Rent mel i posen"
og på den anden side:
"Ingen har lyst til at bo i et glashus".

Jeg vil mene at det er det sidste mundheld som er relevant her - og som ganske godt sammenfatter, hvorfor vi skal undgå overvågning. Selv den der har rent mel i posen vil ikke bo i et glashus. Når man siger, at den der har rent mel i posen ikke frygter en kontrol som billede for myndigheder og andres generelle og indirekte overvågning fungerer det simpelthen som en afledning af de grundlæggende principper for databeskyttelsen.

Omvendte bevisbyrde
Anvendelse af overvågning indfører en omvendt bevisbyrde - som i almindelighed regnes for uacceptabel i en demokratisk retsstat. Det sker principielt i det alle jo ses efter og dermed som udgangspunkt antages for (mulige) overtrædere af de regler der kontrolleres. I praksis kan den omvendte bevisbyrde være så enkel at løfte, at man kan sige det er acceptabelt - du står og venter på S-toget mens du læser avis og det vurderes som acceptabel adfærd. I andre situationer kan overvågningens indirekte bevisbyrde blive meget nærværende. Den indirekte kontrol af arbejdsløsheds dagpenge giver anledning til tvivl og du bliver bedt om at dokumentere at udbetalingen er sket korrekt. Eller et tænkt eksempel: du har skrevet ordene "død" og "statsminister" i en e-mail og bliver udspurgt om du er ved at planlægge et mord.

Hvordan sikres at lovgivningen og administrationen er på højde med udviklingen, således at det enkelte menneskes retssikkerhed tilgodeses?

Med den ny Persondataloven er der etableret et lovgrundlag som også omfatter overvågning, idet loven regulerer enhver behandling af personoplysninger. Men loven indeholder rammer:

§6 Behandling af oplysninger må kun finde sted, hvis
..
6) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller
7) behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse.

Loven er ret ny, den trådte i kraft den 1. juli i år (2000) og dens bestemmelser vil blive nærmere fastlagt gennem Datatilsynets praksis. Endvidere må man forvente, at persondatabeskyttelsen vil blive fastlagt i særregler herom i andre love, der behandler et særligt område - som det bl.a. kendes med betalingskortloven, lov om helbredsoplysning, tinglysningsloven. Med direkte relevans for overvågning findes "Lov om forbud mod TV-overvågning".

Persondata indsamles og registreres på utallige måder til utallige formål i den private og offentlige sektor. Med overvågning ser vi på en særlig form for behandling af persondata. Der findes - mig bekendt - ikke en egentlig definition på overvågning. Jeg kan umiddelbart se tre typer:

Generel overvågning	• Omfatter en gruppe af personer. Alle dem som dukker op i overvågningens "øje". • De overvågede har ikke gjort sig "fortjent" til at blive overvågede.	For eksempel: kamera overvågning af offentlige pladser.
Indirekte overvågning	• Elektroniske spor • Sammenkøring af registre	For eksempel: kontrol af uberettigede udbetalte offentlige ydelser.
Konkret overvågning	• Bestemte personer til særlige formål	For eksempel: elektronisk lænke til prøve løsladt (anvendes i Sverige)

Teknologi udvikling
Udviklingen af informations teknologierne medfører, at det vil blive mere "lige for" at foretage forskellige former for overvågning i fremtiden.

- Digitalisering af data og en række daglig dags gøremål åbner mulighed for overvågning bliver praktisk muligt. Når du sender e-mail kan de automatisk aflæses, færden på

Internettet kan følges. Samtidig er der en tendens til at identifikation bliver mere tydelig, simpelthen for at opnå sikkerhed i den digitale kommunikation - du må vide hvem der snakker, handler osv. For eksempel kan arbejdsgivere følge medarbejdernes færden på Internettet.

- Muligheder for teletransmission udvikles og det bliver muligt at følge den enkeltes færden meget nøje - fiskerbådes position overvåges allerede, mobiltelefoner kan findes. For eksempel overvejes at indføre vejafgifter ved satellittransmission.
- Endvidere er der en hurtig udvikling af de såkaldte biometriske metoder til identifikation af personer. Det kan være fingeraftryk, iris i øjet, øreform, håndfladen. For eksempel anvendes ansigtsgenkendelse i England i forbindelse med kameraovervågning.

Overvejelser om forskellig overvågning:

TV overvågning (generel overvågning som sikkerhed)
Kamera overvågning ser ud til stille og roligt at brede sig. Når jeg venter på S-toget, går gennem mit lokale indkøbscenter. I supermarkedet. Toiletterne på motorvejens rasteplads. Der er alle steder små skilte med et kamera - som så let kan overses og bliver en vane. Ønsker vi virkelig gå fra kameraovervågning til kameraovervågning når vi går rundt i offentlig rum?

I den seneste finanslov er vedtaget at foto fartfælder skal udbredes. Det kritiseres som en omfattende overvågning. Umiddelbart er der da også tale om at alle biler (personer) overvåges og fartsyndere registreres med et foto. Set sådan må man da også sige, at der vil være tale om en overvågning i strid med et ønske om at undgå overvågning. Men sagen peger nok i højere grad på at det er centralt at forholde sig til hvordan man tilvejebringer en kontrol - her af den i bogstavelig forstand dødelige handling at køre for stærkt. Så vidt jeg kan se vil der ***ikke*** blive foretaget en personovervågning - ingen kan konstatere hvilke biler (personer) som har kørt på vejen, idet der ikke generelt indsamles personoplysninger - først når en lovovertrædelse kan konstateres sker der en registrering (fotografering). Foto fartfælderne er således ikke en generel overvågning, men nærmest et eksempel på at kontrol kan opnås uden overvågning.

Søster Sød (overvågning som hjælp)
En særlig mekanisme som kan udbrede overvågning kan kaldes Søster Sød, som er Big Brothers tvillingesøster. For at hjælpe borgerne må det offentlige overvåge deres adfærd så man kan gribe ind og hjælpe borgerne før det går rigtig galt. Eksempler er den kommunale familieforvaltning som iværksætter en overvågning via daginstitutioner og skoler for at opdage familier med problemer. Senest har man inddraget pædagoger og naboer i kontrollen af om enlige forsørgere nu også er reelt enlige.

Børn (generel overvågning som service)
En daginstitution har efter amerikansk forbillede forsøgt sig med overvågning af børnene - angiveligt som en service for forældrene som er glade for kunne "kigge ind" på Internettet. Der vist ingen lovregler som bestemmer om børn må overvåges - men er det virkelig nødvendigt. Der er selvfølgelig den logik i sagerne, at hvis i fremtiden skal bevæge os i kameraovervågningens øjne så kan man lige så godt tilvænne børnene fra de er små?

Efterfølgende kontrol (indirekte overvågning som kontrol)
I begyndelsen af 1980'erne ville man lave et forsøg med samkøring af registre for kontrollere udbetaling af syge- og arbejdsløshedsdagpenge. Forslaget rejste betydelig debat og Statsrevisorerne udtrykte principiel betænkelighed ved fremgangsmåden. I 1990 vedtog Folketinget en lov som åbnede op for omfattende samkøring af edb-registre for at kontrollere udbetalinger af sociale ydelser. Væk var den principielle betænkelig. Fokus var på besparelser på mindst 200 mill. kr. Besparelserne har vist sig at være væsentlig mindre - til gengæld er samkøringerne vokset i omfang. Denne efterfølgende kontrol omfatter alle som har modtaget de pågældende ydelser, hvoraf kun et lille fåtal har gjort noget forkert. Det er min vurdering at denne mistænkeliggørelse af i forvejen svage samfundsgrupper og udskillelse af enkeltpersoner, hvis forhold underkastes en nærmere undersøgelse, overskrider grænsen for borgernes retssikkerhed.

Elektroniske spor (potentiel indirekte overvågning)
Med udbredelsen af IT systemer vil vi sætte elektroniske spor fra stadig flere dagligdags aktiviteter, f.eks. betalinger med Dankort, telefonsamtaler, bilkørsel ved bro (og måske vejafgifter). Disse elektroniske spor anvendes - så vidt jeg ved - ikke i dag til overvågning eller kontrol. Det er utrolig vigtigt, at det fastholdes at sådanne oplysninger kun kan anvendes meget snævert til deres oprindelige formål - og at der ikke åbnes op for at elektroniske spor anvendes til indirekte overvågning.

Sikkerhed og overvågning
Overvågning kan opstå som led i etablering af sikkerhed ved brugen af IT systemer. Det er f.eks. kendt ved overvågning af medarbejderes færden på Internettet og logning af medarbejdernes anvendelse edb-systemer, som det f.eks. kræves ved behandling af følsomme personoplysninger. Med IT systemerne store samfundsmæssige betydning vil sikkerheden utvivlsomt komme til at spille en central rolle. OECD har i en anbefaling om Informationssystemers sikkerhed fremlagt en række principper, hvor det blandt andet hedder:

Etik.
Informationssystemerne og deres sikkerhed bør tilvejebringes og bruges med respekt for andres rettigheder og legitime interesser.
Demokrati.
Informationssystemernes sikkerhed bør stemme overens med et demokratisk samfunds legitime brug og fordeling af data og informationer

Det er ikke IT systemernes muligheder og sikkerhedskrav, som skal fastlægge hvilken overvågning vi skal leve med - men omvendt IT systemerne som må indrettes efter vores opfattelse af etik, demokrati og databeskyttelse.

På højde med udviklingen

Det er vanskeligt at holde lovgivning og administration på højde med udviklingen. Jeg tror det vigtigste er at få en almen holdning til overvågning, som kan spille en rolle i behandlingen af enkelt sager i Folketing og hos Datatilsynet. Men desværre viser det sig i virkelighedens verden, at enkeltsagerne har deres eget liv. I stedet for en speciel lov om TV-overvågning kunne det måske være en ide med en generel lov om overvågning, som udbygning til persondataloven, der kunne sætte nogle generelle grænser for overvågning.

Information er vigtig når man har overvågning - men information er ikke nok; og der synes at være en tendens til information nedsætter tærsklen for hvad man tillader. Det er som tankegangen er at når man nu informere så kan det tillades. Det bør være omvendt, hvis man (undtagelsesvist) tillader overvågning af gode grunde - så skal den følges op af information. Og altså ikke, man kan godt tillade overvågning for nu bliver der give information.

Efter min vurdering er kameraovervågning gået alt for vidt netop fordi det kan gøres når man informerer og så er det ok.

Der har været talt om privatlivssikrende teknologier. For eksempel krypterings teknologi til at sikre brevhemmeligheden i e-post. Den findes men har meget begrænset udbredelse. Der findes systemer som kan sikret at betalinger på Internettet kan gennemføres uden elektroniske spor med person identifikation. De anvendes ikke i stedet fortsætter udbredelse af betalingskort. Vejafgifterne kan gennemføres ved forudbetaling, men man overvejer systemer som bygger på elektroniske spor. Det kan være en overvågnings forebyggende handling hvis der blev satset bevidst på disse såkaldte privatlivssikrende teknologier.

Janne Glæsel, Bech-Bruun & Trolle Advokatfirma

Spørgsmål:
- Hvad kan forsikringsselskaber få adgang til og registrere nu og i fremtiden?
- Hvor langt er det offentlige fremme med hensyn til digital signatur?

1. Lovgrundlag

Danske forsikringsselskaber er ud over lov om forsikringsvirksomhed og dertil knyttet branchespecifik lovgivning også underkastet persondataloven.

1.01 Persondatalovens generelle principper

Dette indebærer, at forsikringsselskaber skal iagttage de generelle regler om behandling af persondata, dvs. behandling af oplysninger om fysiske personer, f.eks. registrering, videregivelse og samkøring af persondata.

Disse regler har følgende hovedindhold:

- Princippet om god databehandlingsskik (behandlingen skal være rimelig og lovlig)
- Princippet om formålsbestemthed (indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål)
- Princippet om proportionalitet (oplysninger, der behandles, skal være relevante og tilstrækkelige og må ikke omfatte mere, end hvad der kræves til brug for opfyldelse af formålet med behandlingen)
- Krav til et samtykkes indhold
- Oplysningspligt over for de personer, som oplysningerne angår
- Indsigtsret for de personer, som oplysningerne angår
- Særlige krav i forbindelse med videregivelse til brug for markedsføring
- Ret til at gøre indsigelse mod, at oplysninger behandles
- Anmeldelse til Datatilsynet
- Klageret til Datatilsynet
- Ret til at kalde samtykke tilbage

1.02 Lov om forsikringsvirksomhed - tavshedspligt

Ud over disse regler skal forsikringsselskaber iagttage de særlige regler i lov om forsikringsvirksomhed om tavshedspligt og videregivelse af kundeoplysninger. Dette

indebærer en yderligere kundebeskyttelse oven på det beskyttelsesniveau, der er i persondataloven.

Reglerne om tavshedspligt fastsætter, at bl.a. bestyrelsesmedlemmer, revisorer, granskningsmænd, direktører og øvrige ansatte ikke uberettiget må videregive eller udnytte fortrolige oplysninger, som de under udøvelsen af deres erhverv er blevet bekendt med. Som følge af denne tavshedspligt er der fortrolighed omkring de oplysninger, som kunder afgiver til forsikringsselskaber.

1.03 Udtrykkeligt samtykke

Udgangspunktet er endvidere, at behandling af kundeoplysninger kræver samtykke. Samtykke kan gives både mundtligt og skriftligt. Et samtykke skal være **udtrykkeligt**, **frivilligt**, **specifikt og informeret** og kan på hvilket som helst tidspunkt **tilbagekaldes** af kunden med den virkning, at oplysningerne ikke må behandles, herunder videregives i fremtiden. At et samtykke skal være udtrykkeligt betyder, at der ikke kan opnås et stiltiende eller indirekte samtykke. Samtykket skal være konkretiseret, så det står klart og tydeligt, hvad der meddeles samtykke til, herunder hvilke typer af oplysninger, der må videregives, hvem der kan foretage videregivelsen samt til hvilke formål, videregivelsen kan ske. Den, der afgiver samtykke, skal være tilstrækkeligt informeret om, hvad det er, vedkommende giver samtykke til.

2. Besvarelse af spørgsmålet - Hvilke oplysninger har forsikringsselskaberne adgang til, og hvilke oplysninger registreres?

Behandling af oplysninger inden for forsikringsområdet er som altovervejende hovedregel baseret på skriftligt samtykke fra forsikringstagernes, dvs. kundernes, side. Samtykke indhentes som hovedregel forudgående i forbindelse med, at forsikringstageren udfylder en forsikringsbegæring (en blanket i skemaform). Tegning af forsikring kan dog også ske på grundlag af en telefonisk henvendelse med efterfølgende fremsendelse af forsikringsvilkår og giroopkrævning.

Ud over almindelige kundeoplysninger i form af navn, stilling, adresse og telefonnummer samt cpr-nummer, kan der behandles de oplysninger, som er nødvendige og relevante, for at den konkrete forsikringsaftale kan indgås. Disse oplysninger varierer, alt efter hvad det er for en type forsikring, kunden ønsker: En husforsikring, en hundeforsikring, en ansvarsforsikring, en livsforsikring osv. Fælles for alle forsikringstyper er, at der indhentes oplysninger, der sætter forsikringsselskaberne i stand til at foretage en risikovurdering.

For så vidt angår livsforsikringsområdet, hvor der er tale om helbredsoplysninger, anmoder forsikringsselskaberne på tegningstidspunktet om samtykke til at indhente oplysninger inden for sundhedssystemet, herunder hos forsikringstagerens egen læge og om samtykke til eventuelt at videregive oplysningerne til Foreningen til Bedømmelse af Pensionsrisiko (Bedømmelsesforeningen), som er et samarbejde mellem et større antal forsikringsselskaber.

Ved tegning af livsforsikring behandles generelt sagt sådanne helbredsoplysninger, som er nødvendige, for at forsikringsselskaberne kan foretage en vurdering af dødsfaldsrisikoen i et tidsmæssigt perspektiv. Helbredsoplysninger tilhører kategorien af følsomme personoplysninger, der efter persondataloven kun kan behandles under særlige betingelser, herunder hvis den pågældende person har givet sit udtrykkelige samtykke til behandlingen.

De oplysninger, som forsikringsselskaberne kan få ved at rette henvendelse til sundhedssystemet, er som udgangspunkt de samme oplysninger, som man som patient har ret til at få indsigt i.

Disse helbredsoplysninger videregives til Bedømmelsesforeningen, hvis der er en formodning om en forringet helbredstilstand. Herefter undergives helbredsoplysningerne en vurdering i Bedømmelsesforeningen. Formålet med foreningen er at sikre en ensartet bedømmelse af helbredsforhold og at undgå forsikringssnyd eller forsøg herpå, idet Bedømmelsesforeningen fører et såkaldt advarselsregister.

Der gives meddelelse til den, der har begæret forsikringen, såfremt videregivelse sker.

Oplysningerne opbevares i 5 år efter forsikringstagerens død, eller indtil forsikringen kan tegnes på normale vilkår.

Forsikringstageren har ret til at få foretaget en revurdering 2 år efter en given periode, f.eks. 2 år efter et operativt indgreb. Forsikringstageren har fuld aktindsigt.

Bedømmelsesforeningen fører et såkaldt advarselsregister over alle personer, der har anmodet om en livsforsikring, men som ikke kan tegne den på normale vilkår.

De oplysninger, der behandles af forsikringsselskaberne og eventuelt optages i Bedømmelsesforeningens advarselsregister, er forsikringstagerens personnummer, navn, stilling, bopæl, interne sagsnumre, de for forsikringsbegæringen nødvendige helbredsoplysninger, risikovurderingen, tilsagn og årsagsforklaring. Oplysningerne kan overføres til de forsikringsselskaber og pensionskasser, som er medlem af

Bedømmelsesforeningen. Overførsel sker ved en direkte edb-forbindelse, og der er adgangskontrol til såvel lokaler som edb-system, ligesom der foretages logning.

Bedømmelsesforeningens advarselsregister har tilladelse fra Datatilsynet og er anmeldt til Datatilsynet.

(Hvad sker der, hvis den registrerede tilbagekalder samtykket?)

3. Praksis på forsikringsområdet

Nedenfor gives nogle udvalgte eksempler på afgørelser fra det tidligere Registertilsyn inden for forsikringsområdet.

Det tidligere Registertilsyn har udtalt, at oprettelse af et fælles skadesregister for forsikringsselskaberne ikke ville være i overensstemmelse med lov om private registre (§ 3, stk. 1) som følge af, **at** et sådant register ville blive meget stort og indeholde data om en meget betydelig del af samtlige forsikrede i Danmark, hvor langt hovedparten af de registrerede ville være registreret, selv om de ikke på nogen måde havde gjort sig skyldige i et ulovligt eller mistænkeligt forhold, **at** registeret måtte antages kun for en meget lille del at ville kunne afsløre egentlig forsikringsmisbrug, samt **at** det efter Tilsynets opfattelse reelt ikke kunne sikres, at registeret ikke blev anvendt til at sortere ærlige, men uheldige, kunder fra (I Norge findes et sådant register, som det Norske Forsikringsforbund havde skønnet gav en besparelse i form af opdaget forsikringssvindel på NOK 100 mio.).

Registertilsynet har endvidere i en anden sag udtalt, at et forsikringsselskabs videregivelse af oplysninger om formodede strafbare forhold vedrørende en forsikringstager til et andet forsikringsselskab var i strid med den daværende registerlovs § 4, stk. 1, idet registreringen og videregivelsen ikke var sket med hjemmel i lovgivningen eller med den pågældendes samtykke. Registreringen ville kunne ske med henblik på politianmeldelse, hvis anmeldelsen sker i umiddelbar forlængelse af registreringen.

Registertilsynet har i en sag udtalt, at et forsikringsselskabs registrering af ægtefælles/samlevers og børns personnumre måtte antages at være i strid med den dagældende lov om private registre.

Registertilsynet har i en sag udtalt, at anvendelsen af personnummer som policenummer ikke i sig selv var i strid med den daværende lov om private registre.

4. Fremtiden

Der vil i den nære fremtid næppe ske de store ændringer i, hvilke oplysninger forsikringsselskaberne kan få adgang til og registrere, hvis den nuværende praksis med samtykke fortsættes.

I øjeblikket arbejder et såkaldt tværgående udvalg under Økonomiministeriet med temaet "Beskyttelse af kundeoplysninger i finansielle virksomheder, herunder tavshedspligtreglerne".

Der er netop afgivet en redegørelse herom, og heri peges bl.a. på, at der kan ske en forbedret beskyttelse af kundeoplysninger i finansielle virksomheder, herunder forsikringsselskaber, såfremt der indføres et skriftlighedskrav i relation til samtykke. Omvendt peges der også på, at et skriftlighedskrav kan betyde, at det ikke vil være muligt at indgå forsikringsaftaler ved at der efter en telefonsamtale fremsendes en police og en præmieopkrævning.

Oluf Jørgensen, Afdelingsforstander i informationsret ved Danmarks Journalisthøjskole

Spørgsmål:
- Hvad kan sundhedssektoren få adgang til at registrere nu og i fremtiden?

Patientdata hører til de mest følsomme. På det sundhedsfaglige område registreres ikke blot ydre adfærd. Det enkelte menneskes indre kortlægges også. Patientdata handler om både krop og psyke - i fortid, nutid og fremtid.

Kortlægning af gener kan fx give oplysninger om det enkelte menneskes risiko for at udvikle bestemte sygdomme. Hidtil har genetisk testning kun været brugbar i forhold til nogle få, sjældne sygdomme. Der satses meget store ressourcer på at udvikle en teknik, der hurtigt kan analysere et menneskes samlede genmasse. Det bliver formentlig muligt om få år at gennemføre genetisk testning af arvelig former for hyppige og almindelige sygdomme. Dermed udvides målgruppen til potentielt at omfatte alle mennesker.

Forskningen sigter på at udvikle genterapier, hvor behandling og forebyggelse tilpasses det enkelte menneskes særlige genetiske forudsætninger. Mange forskere, politikere og Det Etiske Råd giver udtryk for, at genterapi kun bør anvendes ved behandling af alvorlige sygdomme og ikke til forbedring af normalegenskaber. Det er et stort spørgsmål, om anvendelsen af genterapi vil blive begrænset til behandling af alvorlige sygdomme. Der er meget stærke interesser i at udvikle behandling af menneskers normalegenskaber, fx hukommelse, nervøsitet, indlæring, fysisk formåen og udsættelse af den naturlige aldring.

Genterapi må ikke anvendes til at ændre kønsceller i forbindelse med kunstig befrugtning (jf. lov om kunstig befrugtning mv.).

"Den grundlæggende registrering af patientdata sker i journaler ved private praksiser, sygehuse, plejehjem m.v.. Læger har ifølge lægeloven pligt til at føre journaler med oplysninger om patienternes sygdomme, undersøgelser, observationer, diagnoser og behandling. I forbindelse med udskrivning fra sygehuse skrives typisk et udskrivningsbrev med summariske oplysninger om sygdom og behandling, der sendes til patientens alment praktiserende læge. Læger sender desuden mange patientoplysninger til myndigheder, forsikringsselskaber m.v. Andre faggrupper inden for sundhedsvæsenet, fx sygeplejersker, jordemødre, fysioterapeuter og psykologer, registrerer også patientdata i journaler, kardex m.v.." (kilde: "Persondataret" af Oluf Jørgensen, Systime, november 2000).

Den grundlæggende registrering og anvendelse af patientdata er reguleret af loven om patienters retsstilling (lpr). Den sikrer, at behandling bygger på et informeret samtykke. loven sikrer også, at videregivelse til andre konkrete formål end den aktuelle behandling

som hovedregel kræver patientens samtykke, fx videregivelse til forsikringsselskaber. Loven om patienters retsstilling tillader derimod videregivelse uden patientens samtykke til forskning, planlægning og statistik.

"Mange patientdata indgår i administrative og videnskabelige databanker, de såkaldte biobanker.
Nogle biobanker er oprettet med henblik på administration og planlægning, fx Sundhedsstyrelsens landspatientregister. Andre biobanker er oprettet med henblik på forskning, fx Cancerregistret. Nogle biobanker indeholder skriftlige patientdata, mens andre indeholder væv, blodprøver, røntgenbilleder, nedfrosne celler, DNA-fragmenter m.v. Fx har patologiske afdelinger vævs- og celleprøver for cirka halvdelen af befolkningen. Statens Seruminstitut har siden 1982 indsamlet og opbevaret blodprøver for samtlige nyfødte børn.

Offentlige myndigheder, der vil oprette en biobank, skal forinden anmelde systemet og indhente en udtalelse fra Datatilsynet (pdl § 45). Private, der vil oprette en biobank til forskningsformål mv. skal både anmelde og have en tilladelse fra Datatilsynet (pdl § 50). De fleste forskningsregistre er private i persondatalovens forstand, fordi de oprettes af forskere til brug for deres individuelle projekter. Det gælder også forskningsregistre, der oprettes af læger på offentlige sygehuse. Datatilsynet kan fastsætte vilkår for tilladelsen.

Et forskningsprojekt skal desuden godkendes af en videnskabsetisk komité, hvis det indebærer forsøg på mennesker (levende som døde), væv, celler og arvebestanddele. Der kræves desuden informeret samtykke fra en person, før han må bruges i forsøg. Ved sådanne forsøg gælder kravet om samtykke også for indsamling og anvendelse af patientdata. Som konsekvens heraf må en patient, der trækker sig ud af forsøget, kunne kræve at få indsamlede data udleveret eller destrueret." (kilde "Persondataret" af Oluf Jørgensen, Systime, november 2000).

Forskningsministeriet har i starten af november 2000 udsendt en bekendtgørelse om information og samtykke ved biomedicinske forsøg og en grundig vejledning. Ifølge vejledningen skal der fremover føres kontrol med, at lægerne overholder de forsøgsprotokoller, de har fået godkendt. Det vil styrke retssikkerheden ved de forskningsprojekter, der omfattes af komitéloven. Komitéloven gælder formentlig kun ved projekter, der direkte involverer den enkelte patient. Forskning, der bygger på oplysninger fra registre, vil typisk kun være omfattet, hvis registret er opbygget med et konkret forskningsprojekt for øje. Ifølge vejledningen gælder komitéloven ved projekter, der anvender materiale fra biobanker med organisk materiale, fx vævsprøver.

"Forskning, der ikke direkte involverer den enkelte patient, kan foregå uden samtykke. Det gælder forskning, der bygger på udtræk, samkøring og analyse af patientdata fra biobanker. Forskeren må ikke henvende sig til den enkelte patient uden tilladelse fra de sundhedspersoner, der har behandlet den pågældende (lpr § 29 stk.3). Patientdata, der er

indsamles til forskning, statistik og planlægning, må ikke bruges til andre formål. De må kun offentliggøres i en form, hvor enkeltpersoner ikke kan identificeres (lpr § 31).

De nye regler om informationspligt i persondataloven (pdl) gælder også for indsamling af patientdata (pdl § 28 og § 29). Der er en undtagelse, når underretning "viser sig umulig eller er uforholdsmæssigt vanskelig" (pdl § 29 stk.3). Den betyder ifølge lovforslagets bemærkninger, at der "kun i særdeles begrænset omfang" er pligt til at informere personer, når identificerbare data om dem bruges i forskningsprojekter. Denne bemærkning er besynderlig, fordi det ofte ikke er vanskeligt at sende en skriftlig information til patienterne.

Borgernes ret til aktindsigt i egne data gælder ikke, når oplysninger alene behandles i videnskabeligt eller statistik øjemed (lpr § 19 stk.2 og pdl § 32 stk.4).

Biobankernes oplysninger om borgerne er meget omfattende og vedrører de mest private forhold, der tænkes kan. Ved forskning kan genereres nye oplysninger om den enkelte borger. Det er uforudsigeligt, hvilke projekter og formål biobankerne ønskes benyttet til i fremtiden.

Det er vigtigt at sikre offentlig kontrol med biobankernes anvendelse. Det er også vigtigt, at den enkelte patient, der ønsker det, kan få information om, hvad hans data bruges til. Patienten bør sikres mulighed for at sige fra, hvis han ikke ønsker at bidrage til den pågældende forskning. Disse rettigheder har patienter ikke i dag. " (kilde: "Persondataret" af Oluf Jørgensen, Systime, november 2000).
Ovennævnte forslag er på linje med anbefalinger i rapporten "Biobanker", der blev udgivet af Etisk Råd i 1996, men ikke er blevet sikret i lovgivningen. Rapporten er forfattet af Linda Nielsen (Etisk Råd), Gert Almind (Statens Sundhedsvidenskabelige Forskningsråd, Povl Riis (Den Centrale Videnskabsetiske Komité) og Nils Strandberg Pedersen (Statens Sundhedsvidenskabelige Forskningsråd). I rapporten anbefales bl.a.:

<-- Alle borgere bør have ret til at vide, i hvilke registre de indgår, og med hvilke oplysninger. En sådan ret kan opfyldes ved at borgeren konkret forespørger, om han eller hun befinder sig i et bestemt register. Den praktiske gennemførelse sikres ved, at Registertilsynet (nu Datatilsynet) årligt udgiver en komplet liste over registrerede biobanker med en kort beskrivelse af de enkelte bankers natur og formål.

<-- Den enkelte patient bør ved generel og skriftlig information oplyses om, at blodprøver, væv mv., der afgives til diagnostisk brug, eventuelt senere vil indgå i en biobank og blive brugt til forskning mv. Det bør fremgå udtrykkeligt af den skriftlige information, at patienten kan vælge at sige nej til, at materialet opbevares i en biologisk bank med henblik på sådanne formål, og at et eventuelt samtykke når som helst kan trækkes tilbage.

Kortlægning af gener og genterapi kan få meget store menneskelige og samfundsmæssige konsekvenser. Hvis gentest bliver almindelige, kan der udvikles en bekymringskultur? Er der tale om sikre prognoser for det enkelte menneske eller bygger oplysninger på statistiske sammenhænge? Kan der tilbydes forebyggelse og behandling til de mange risici, der opdages? Kan det sikres, at den enkelte borger frit kan tage stilling til, om han ønsker oplysninger? Kan mennesket sikres mod overvågning af sig selv via DNA-mikrochips?

Loven om brug af helbredsoplysninger på arbejdsmarkedet hindrer som hovedregel, at arbejdsgivere får oplysninger om sygdomsrisici, men loven hindrer ikke at konkurrencen på arbejdsmarkedet får mennesker til at søge kunstige hjælpemidler for at styrke deres evner til indlæring, koncentration og udholdenhed. Kan det sikres, at genterapi kun bruges til behandling af alvorlige sygdomme? Kan det undgås, at mennesker, der er raske eller kun har småskavanker, får lyst til eller bliver presset til at prøve genterapiens muligheder? Hvordan sikres børn mod ambitiøse forældre? Er det menneskeligt og samfundsmæssigt forsvarligt, at naturlig aldring forhales af mennesker, der har råd til genterapi? Kan jordens ressourcer og miljøet bære, at mennesker lever længere i den rige del af Verden?

Peter Blume, Prof. dr. jur., Københavns Universitet, Retsvidenskabelig afdeling

Spørgsmål:
- Hvor lidt registrering har samfundet brug for, for at kunne opretholdes?
- Hvor meget registrering kan samfundet bære og stadig være et demokrati?

Registreringens minimum og maksimum
Dette papir søger at besvare de to rejste spørgsmål om henholdsvis, hvor lidt registrering, der er nødvendig for at opretholde samfundet, og hvor stort registreringsomfanget kan være for at vi stadig skal leve i et demokrati. Der er i og for sig allerede udstedt et løfte, som ikke kan holdes i og med, at det ikke er muligt at give noget særligt præcist svar på disse spørgsmål. Der kan ikke gives nogen kvantitativ besvarelse, fordi vurderingen afhænger af hvilket formål, registreringer har og hvad de opbevarede oplysninger anvendes til. Svaret afhænger også af, hvem der foretager registreringen. Således som spørgsmålene er formulerede, forekommer det naturligt i det følgende at sætte fokus på de offentlige myndigheder, selvom det er en almindelig iagttagelse, at det informationelle privatliv også i betydeligt omfang trues af private virksomheders persondatabehandling. Det er dog fortsat det offentliges praksis, der har størst betydning.

Indledningsvis må det endvidere bemærkes, at det ikke alene er registrering, men en bred vifte af forskellige former for behandling af personoplysninger, som må påkalde sig interesse. Problemstillingen angår brug og spredning af personoplysninger på basis af

foretagne registreringer. Spørgsmålet er dermed, hvor megen behandling, der er brug for, og hvor går smertegrænsen under et demokratisk perspektiv.

Der startes med undergrænsen. Det må her lægges til grund, at den person-databehandling, der finder sted i den offentlige forvaltning, er en konsekvens af den gældende lovgivning. Registre og anvendelse af de registrerede oplysninger tager sigte på at få lovgivningen til at fungere efter dens hensigt. Dette kan i praksis ikke lade sig gøre fuldt ud, idet en sådan form for retsoptimisme er urealistisk, men desuagtet er ønsket om at sikre lovmedholdelig adfærd årsagen til de mange registre. Juridisk bør det fremhæves, at der skal være hjemmel til at oprette et register og denne hjemmel udgøres af lovgivningen. På denne baggrund kunne problemstillingen omformuleres til at angå, hvor få love eller hvor begrænset en retlig regulering, samfundet kan klare sig med. Det kan i denne forbindelse konstateres, at samfundets retliggørelse har medført, at antallet af love er stadigt stigende og at ikke mindst forandringsomfanget er særdeles stort. Et moderne velordnet samfund synes at forudsætte omfattende lovgivning med heraf følgende registre. Den danske variant har betydet, at vores samfund er et af de mest registrerede i verden.

Denne konstatering indebærer, at staten (inkl. kommuner og amter) har stor viden om borgerne, hvis frihedsgrader dermed er tilsvarende mindre. Der kan utvivlsomt udpeges enkelte registre og behandlinger, der ikke er samfundsmæssigt nødvendige, men i hovedsagen er de eksisterende registre udtryk for en bestræbelse med henblik på, at de rettigheder og pligter, der følger af lovgivningen, faktisk skal blive til virkelighed. Dansk lovgivning skal ikke være papirjura. Spørgsmålet er dermed, om der er overflødig lovgivning, som medfører, at der foretages persondatabehandling, der ikke er påkrævet for samfundets opretholdelse. Atter bliver svaret, at dette nok er tilfældet, men dog ikke i et sådant omfang, at det får principiel betydning.

Muligheden for at begrænse registreringsomfanget indenfor det nuværende samfunds rammer lader sig således ikke præcist fastlægge. Det vil dog være hensigtsmæssigt at øge den demokratiske kontrol ved at sikre, at der altid blev taget stilling til foreslået ny lovgivnings konsekvenser i relation til registrering og persondatabehandling i det hele taget. Det bør sikres, at denne problemstilling indgår i den politiske proces.

Ifølge personoplysningslovens ' 57 skal Datatilsynet høres inden nye retsforskrifter, der har databeskyttelsesmæssige implikationer, gennemføres. For så vidt angår lovforslag, forekommer det naturligt at udvide denne ordning, således at det altid i lovforslag skal være angivet, om forslaget har registermæssige konsekvenser. I dag skal det angives, om et forslag har økonomiske, miljømæssige eller EU-retlige konsekvenser. Det er ønskeligt at udvide denne oplysningspligt, idet dette øger muligheden for, at Folketinget forstår og kan tage stilling til konsekvenserne af den lovgivning, som tinget gennemfører.

En anden problemstilling angår, om der under en demokratisk synsvinkel er en overgrænse for antallet af registre. Ved vurderingen af dette spørgsmål kan det være nyttigt kort at overveje, hvorfor personoplysninger bør beskyttes eller med andre ord, hvad der er baggrunden for, at der er et værn omkring privatlivet i forhold til information. Det er et naturligt udgangspunkt, at denne retsbeskyttelse skyldes hensynet til det enkelte individ. Beskyttelsen af privatlivets fred i den europæiske menneskerettighedskonventions artikel 8 betragtes normalt på denne måde. Dette er da også en betydelig del af sandheden, men det er ikke hele sandheden. Privatlivsbeskyttelsen har også en kollektiv facet, der er relateret til demokratiet. Et levende demokrati forudsætter folkelig deltagelse og dermed, at der eksisterer en god og frugtbar dialog mellem de folkevalgte og folket. Det er en forudsætning, at det enkelte individ faktisk kan deltage i den dialog. Denne forudsætning kan kun opfyldes, såfremt det enkelte individ har mulighed for at være sig selv og ikke smelter helt sammen med det kollektive. Den enkelte må have et privat rum og dette er ikke til stede, såfremt staten ved alt om borgerne.

Dette udgangspunkt betyder, at der er en grænse for registreringsomfanget, såfremt samfundet skal være demokratisk. Det er ikke muligt præcist at angive, hvor denne grænse går, men konsekvensen er, at det altid er et almen politisk spørgsmål om nye former for registrering skal iværksættes. En sådan stillingtagen er vanskelig, fordi der er tale om en glidende og ukoordineret udvikling. Det er karakteristisk, at lovgivningen og de heraf affødte registreringer sjældent ses i sammenhæng og at mere generelle ændringer af samfundets karakter dermed sker umærkeligt. Det er derfor ønskeligt som angivet ovenfor, at der skabes en større politisk bevidsthed om betydningen af at bevare et informationelt privatliv og dermed begrænse den stadig stigende persondatabehandling og dermed det øgede antal registre. En sådan bevidsthed vil øge mulighederne for at bevare et reelt deltagende demokrati.

København
November 2000

Hagen Jørgensen, Forbrugerombudsmand

Spørgsmål:
- Hvilke konkrete muligheder er der nu og bør der være for at privatpersoner kan kontrollere deres personlige oplysninger?

Først og fremmest tak for invitationen. Jeg er altid glad for at få mulighed for at fortælle lidt om mit virke som forbrugerombudsmand – ikke mindst når der er tale om et så aktuelt emne som *"registrering og brug af oplysninger om personer"*.

Emnet er jo næsten grænseløst, men i denne forsamling synes jeg det er naturligt og nødvendigt, at jeg indleder med – trods alt - at afgrænse mit indlæg.

Forbrugerombudsmandens hovedopgave er at føre tilsyn med at markedsføringsloven overholdes af de erhvervsdrivende. *"Navnlig ud fra hensynet til forbrugerne"* som det hedder i lovteksten.

Jeg vil i mit indlæg derfor koncentrere mig om emnet i forhold til begreberne "forbrugere" og "erhvervsdrivende".

Ifølge lovgivningen har jeg mulighed for at forholde mig til problemstillingen både generelt og konkret.

På det generelle område er hjemmelen markedsføringslovens § 1, der er markedsføringslovens grundregel – "generalklausulen" som vi også kalder den. Det er reglen om, at *virksomheder ikke må foretage handlinger, der strider mod god markedsføringsskik*. Kort fortalt betyder det, at alle virksomheder ud over at overholde landets øvrige love, også skal leve op til "god skik".

På det mere konkrete plan er hjemmelen den nye regel i markedsføringslovens § 6a, der populært kaldes "spamming-reglen". Denne bestemmelse blev indsat i markedsføringsloven samtidig med Folketingets vedtagelse af persondataloven, som administreres af Datatilsynet. "spamming-reglen" vedrører både elektronisk spamming og "papir-spamming", det, vi i dag kender som "direct mail". Det vil jeg vende tilbage til.

I forbindelse med ikrafttrædelsen af den nye regel i markedsføringslovens § 6a udsendte jeg et "hyrdebrev" om forståelsen af den nye bestemmelse. De overordnede hensyn, som jeg mener, bør tages over for forbrugerne, er gengivet i brevet. Brevet kan læses i sin helhed på Forbrugerstyrelsens hjemmeside, www.fs.dk. Her kan også ses et righoldigt materiale om forbrugerlovgivningen, Forbrugerombudsmandens retningslinier, vejledninger m.v. og omtale af principielle sager, bl.a. om fortolkning af begrebet "god markedsføringsskik".

Jeg har forståelse for, at virksomhederne, også ud fra et forbrugersynspunkt, kan have gode grunde til at anvende visse former for registreringer af personoplysninger. Det drejer sig særligt om situationer, hvor registrering sker for at yde optimal service over for forbrugerne.

Desværre er det generelle indtryk af de sager, vi hidtil har set, at anvendelse af personoplysninger sker på en måde, der først og fremmest er til fordel for virksomhederne. Forbrugersigtet kan ofte være svær at få øje på.

"Handel og privatliv"
På det generelle plan udsendte Forbrugerombudsmanden i sensommeren et udkast – foreløbig i notatform – om erhvervsdrivendes anvendelse af de moderne edb-værktøjer "data warehousing" og "data mining". Udkastet, der har titlen *"Handel og privatliv"* kan læses på www.fs.dk. Høringsrunden er nu afsluttet, og vi er ved at gennemgå

høringssvarene. Det er endnu ikke besluttet i hvilken form, det endelige materiale udsendes – det vil jeg vurdere, når vi har fået fuldt overblik over høringssvarene.

Data warehousing og data mining er kort fortalt edb-værktøjer til at registrere og behandle diverse oplysninger – fx om kunders adfærd. Det kan være telefonselskabets registrering af eksempelvis antallet af opkald, opkaldenes varighed, hvor ringes der til, om der betales til tiden osv. Det er herudfra muligt at udlede en lang række sammenhænge, selvom oplysningerne enkeltvis fremtræder "ustrukturerede".

I det udsendte notat "Handel og privatliv" er der nævnt et konstrueret eksempel, som jeg godt vil gengive her:

Det understreges, at der med eksemplet er tale om, hvad der er teknisk muligt, ikke nødvendigvis hvad der er lovligt:

Foretager en forbruger eksempelvis sine indkøb i et varehus, der sortimentsmæssigt dækker alle daglige fornødenheder, vil det på baggrund af registreringer fra kasseboner være muligt at beregne familiens sammensætning: Købes der jævnligt børnetøj og bleer, er der formodentlig tale om en husstand med børn. Købes der også jævnligt nylonstrømper og make up, er der formodentlig også tale om en husstand med mindst én kvinde.

På tilsvarende måde kan man kortlægge, om de enkelte forbrugere køber flere økologiske varer end gennemsnittet, om pågældende fortrinsvis går efter slagtilbud, ligesom man kan kortlægge, om netop denne forbruger typisk køber luksusvarer eller discountvarer. Efter et stykke tid kan virksomheden endda med stor sandsynlighed beregne, hvornår pågældende forbruger igen kommer, og hvilke basisvarer, der vil blive købt af vedkommende. Disse oplysninger kan bruges i markedsføringen over for den enkelte forbruger, således at forbrugeren kun præsenteres for reklamemateriale om produkter/produkttyper, som virksomheden erfaringsmæssigt ved, netop denne forbruger jævnligt køber.

Så langt så godt. Men det er også teknisk muligt at anvende oplysningerne fra kassebonen på en lidt mindre tillidvækkende måde:

Med udgangspunkt i de ovenfor nævnte eksempler kan der også foretages følgende konklusion over indkøbene: Købes der jævnligt børnetøj, nylonstrømper og dameblade men aldrig artikler til mænd, er det nærliggende at antage, at der er tale om en "enlig mor".

"Enlig mor" er vel ikke en betegnelse, der i dagens Danmark er problematisk at få hæftet på sig. Men det er bestemt berettiget at diskutere, hvorvidt det er noget, der vedkommer det lokale supermarked eller dettes ansatte - eller vedkommer de andre erhvervsdrivende, der med tiden muligvis får adgang til oplysningerne.

Men hvor går grænsen?

Det er ud fra den trofaste forbrugers kasseboner også muligt at vurdere, hvorvidt kunden køber mere - måske endda meget mere - alkohol end gennemsnitsforbrugeren. Det er vist ikke nødvendigt at udpensle de konklusioner, der kan drages af netop disse registreringer.

De nævnte eksempler er på en række punkter omfattet af persondataloven og på en række punkter omfattet af markedsføringsloven.

Et af hovedtemaerne i den endelige udmelding fra Forbrugerombudsmanden bliver, at de erhvervsdrivende skal forholde sig kritisk til anvendelsen af data warehousing og data mining og gøre sig bevidst, at man faktisk kan bevæge sig meget langt ind i forbrugernes privatliv med de negative konsekvenser, det kan have. Det gælder ikke mindst, når den erhvervsdrivende vil skaffe sig samtykke til registrering og behandling af oplysninger. Forbrugerombudsmanden har tidligere anført, at det er problematisk, hvis erhvervsdrivende slører det faktum, at der afgives personlige oplysninger til registrering ved fx at lokke med deltagelse i præmiekonkurrencer. Det gør sig ikke mindst gældende, når det er markedsføring, der retter sig mod børn og unge.

Forbrugerombudsmanden mener, det er vigtigt, at de enkelte erhvervsdrivende formulerer en registreringspolitik – derved skaber virksomheden både intern fokus på en række af de problemer, der kan opstå i kølvandet på anvendelsen af disse edb-værktøjer, ligesom man kan oplyse forbrugerne om politikken og dermed om, hvordan forbrugerens private oplysninger bliver behandlet.

I oktober i år udgav Forbrugerombudsmanden en rapport om handel og markedsføring på Internettet. I rapporten gennemgås en række større danske virksomheders Internet-hjemmesider, hvor der kan handles. En af rapportens konklusioner er, at det gennemgående stod sløjt til omkring registrering af personoplysninger. Af de ca. 20 undersøgte virksomheder gav ca. halvdelen slet ingen oplysninger om deres registreringspolitik. Og ingen af de undersøgte virksomheder oplyste om, hvor længe de registrerede oplysninger blev gemt. Rapporten kan læses i sin helhed på www.fs.dk.

Også i denne rapport blev det konkluderet, at det i mange henseender er vigtigt, at virksomhederne formulerer en offentlig tilgængelig politik for registrering og anvendelse af personoplysninger.

Et konkret eksempel på en sag om personoplysninger, der for tiden er under behandling, er en sag, der drejer sig om et samarbejde mellem Den Danske Bank og et forsikringsselskab, hvor kunder gennem banken kunne tegne en bilforsikring. Sagen har visse lighedstræk med det nævnte konstruerede eksempel omkring kassebonen - denne sag er imidlertid virkelighed.

Banken videregav oplysninger baseret på bankens mellemværende med forsikringstegnerne – i form af en såkaldt forsikringsscore - "et point", som sammen med mere forsikringstekniske oplysninger var med til at bestemme, hvilken præmie kunden skulle betale. Spørgsmål om hvor længe kundeforholdet med banken havde varet, om der havde været overtræk på konti o.l., var altså med til at bestemme præmiens størrelse.

Kunden var ikke orienteret om denne beregning og videregivelsen af scoren til forsikringsselskabet på en tilstrækkelig tydelig måde. At oplysninger om kontomellemværendet indgik i de oplysninger, som lå til grund for en bilforsikringstegning må siges at være ganske overraskende.

Sagen viste også, at der blev benyttet ganske bredt formulerede samtykkeerklæringer, som ikke reelt satte nogen grænser for hvilke oplysninger, der kunne videregives, eller præcist angav de formål, som oplysningerne kunne bruges til.

Markedsføringslovens § 6a
"Spamming-reglen" i markedsføringslovens § 6a er ny.

Bestemmelsen drejer sig om *direkte markedsføring,* dvs. uanmodet henvendelse til bestemte aftagere. Med bestemte aftagere menes, at modtageren er defineret ved navn, og/eller adresse, telefonnummer eller lignende. Det betyder, at eksempelvis adresseløse forsendelser, tilbudsaviser, Tv-reklamer og lignende, der henvender sig til en ubestemt kreds af mulige aftagere ikke er omfattet af disse regler.

Kun hvis den pågældende *forudgående har anmodet om det* må en erhvervsdrivende sende reklamer via elektronisk post, telefax og automatiske opkaldssystemer.

Ved brug af almindelig post må erhvervsdrivende som udgangspunkt sende personlig adresseret reklamemateriale til alle. Der er dog et par vigtige undtagelser: der må ikke sendes til dem, der har frabedt sig det direkte over for virksomheden, og der må heller ikke sendes reklamer til dem, der har tilmeldt sig den særlige liste hos Det Centrale Personregister, CPR.

Listen, der populært kaldes Robinson-listen, - og dermed refererer til Robinson Crusoe, der var isoleret på en øde ø - er indsat i loven for at beskytte de personer, der ikke ønsker nogen form for uanmodede personlige reklamehenvendelser.

Jeg har allerede set flere sager i relation til "spamming-reglen", og for at undgå alt for megen tvivl om bestemmelsens rækkevidde har vi netop udsendt en orienteringsskrivelse til erhvervs- og forbrugerorganisationer m.v. Den ligger på www.fs.dk. Jeg vil her nævne et par af de sager, der også har haft pressens bevågenhed.

Den Danske Bank har efter fusionen med BG Bank ca. 3 millioner private kunder. Det siger sig selv, at alene den datamængde en sådan kundegruppe giver, stiller en række krav til virksomheden til håndteringen af disse data.

Banken udsendte i foråret information til alle sine private kunder, hvor man oplyste om de nye regler i både persondataloven og markedsføringslovens § 6 a.

Banken var ikke omhyggelig nok ved formulering af sin pjece, og vildledte på denne måde sine kunder om de nye regler. Kunderne forstod næppe, hvorledes de skulle forholde sig, og hvilke regler, der fremover gjaldt for bankens henvendelser til dem.

En anden sag, der for tiden er under behandling drejer som Interessebank Danmark, der er et samarbejde mellem Post Danmark og Tele Danmark Forlag. Konceptet går ud på, at forbrugere kan tilmelde sig en database over forskellige angivne interesser. Herefter vil Interessebank Danmark sælge oplysninger til erhvervsdrivende, der vil bruge oplysningerne i markedsføringsmæssig øjemed.

Men Interessebank Danmark mener, at man også må sende direkte markedsføringsmateriale til de personer, der har tilmeldt sig Robinson-listen, hvis personen samtidig har tilmeldt sig Interessebank Danmark.

Ifølge loven må der kun sendes direkte reklamemateriale til personer, der *forudgående har anmodet om henvendelse fra den erhvervsdrivende*. Det fortolker Forbrugerombudsmanden således, at kun de erhvervsdrivende, som personen selv – eventuelt via en fuldmægtig - har henvendt sig til må sende direkte reklamemateriale. Når man tilmelder sig Interessebank Danmark, ved man ikke, hvem der med tiden vil købe ens adresse og oplysninger, og derfor ved man heller ikke, hvilke virksomheder, der siden vil henvende sig. Det gør det eksempelvis umuligt på forhånd at vide, til hvem man skal framelde sig, da Interessebank Danmark ikke på deres erhvervsdrivendes kunders vegne kan modtage framelding. Samlet er lovkravet efter min opfattelse dermed ikke opfyldt.

Sagen er stadig under behandling, og Interessebank Danmark har netop meddelt, at man ikke vil indrette sig i overensstemmelse med mine anvisninger. Jeg overvejer nu, hvad der herefter skal ske i sagen.

Som det måtte fremgå at mit indlæg, er spørgsmålet om "registrering og brug af oplysninger om personer" i høj grad noget, der har min bevågenhed. Det skyldes den teknologiske udvikling, der nu muliggør noget, der for år tilbage var utænkeligt, men det skyldes naturligvis også lovpakken, som persondataloven og markedsføringslovens § 6a var en del af. Vigtigst af alt har det min bevågenhed, fordi registrering og behandling af personoplysninger i denne tid virkelig boomer indenfor erhvervslivets forhold til forbrugerne. Mange typer af problemer vil kunne løse sig selv, hvis de erhvervsdrivende

især på dette vigtige punkt holder en høj grad af selvjustits, således at registrering og brug af personoplysninger kan finde et naturligt leje, som både udnytter nogle driftsfordele for de erhvervsdrivende, samtidig med at hensynet til forbrugerne stadig er i højsædet.

Tema 6: Overvågning på arbejdspladsen

Peter Christensen, Prosa

Spørgsmål:
- Hvilke fordele og ulemper er der ved elektronisk overvågning af mennesker på en arbejdsplads?

Fysisk overvågning

1. I sommeren '98 vedtog Folketinget efter nogle opsigtsvækkende historier om videoovervågning af individuelle, omklædningsrum osv. en lov: lov om videoovervågning. Men kan i bakspejlet undre sig over, at ingen af interessenterne i lovens udformning tilsyneladende forsøgte at stille spørgsmålet: hvordan vurderer vi kvalitativt, hvornår overvågning af person på en arbejdsplads kan tillades, altså hvornår vi har lov til at anvende overvågningsteknologien – al interesse blev lagt i, hvilke forudsætninger der skulle være til stede før man skulle informere de ansatte om, at de blev overvåget.

2.Fysisk overvågning er nemlig kommet for at blive – ikke pga. nødvendigheden; men fordi prisen på overvågningsudstyr er raslet ned. Det er altså igen ikke en kvalitativ stillingtagen til teknologiens anvendelse; men blot at vores moral-kodeks om hvad der er ret eller vrang tilsyneladende er underlagt den økonomiske udvikling.

Elektronisk overvågning

I dag er den generelle regel ifølge arbejdsmarkedet Hovedaftale, at arbejdsgiveren har retten – og pligten – til at lede og fordele arbejdet. Når vi påpeger pligten er det naturligvis fordi, at manglende ledelse af arbejdet ikke kan klandres de ansatte. Hvis den ansatte således resultatmæssigt opnår de af ledelsen fastsatte mål, er det således arbejdsgiverens problem, hvis den ansatte kan bruge f.eks. større dele af sin arbejdstid på områder, der i øvrigt er uvedkommende for arbejdsprocessen.
I dette ligger dog også, at det er resultaterne, der skal kontrolleres og ikke hvad den ansatte bruger spildtiden til.

I dag registreres mange data alene for at sikre systemernes tilgængelighed, afværgning af indbrud fra eksterne net osv. Disse data er udformet med det formål at kunne kontrollere IT-systemernes funktionalitet – men kan helt eller delvist anvendes til en indirekte kontrol

af de ansattes anvendelse af IT-systemerne. Et meget godt eksempel er de logs, der registrerer mulige hacker-indbrud på en FireWall. De samme logs vil kunne anvendes til at skabe sig et billede af trafikken mellem den enkelte arbejdsplads og Internettets forskellige hjemmesider og funktioner – altså kunne anvendes til at kontrollere den enkeltes Internetforbrug – ligesom et telefonanlæg registrerer forbrug på den enkelte lokaltelefon på en arbejdsplads.

Corporate Privacy – eller på dansk den enkeltes integritet på sin arbejdsplads – omfatter således regler om den enkelte arbejdsgivers ret til at læse e-mail mellem en ansat og en ekstern/intern modtager, regler for overvågning af den enkelte ansattes anvendelse af generelle Internet-adgang samt de kendte omkring overvågning af telefonanvendelse osv. Men udover dette også de kontrol-værktøjer, der sikrer arbejdsgiveren, at der faktisk bliver produceret noget.
PROSA fik i slutningen af 70'erne lavet en lokal-aftale på det daværende Datacentralen om, at registreringen af taste-damers produktivitet via deres indtastningsprogram ikke måtte udnyttes – altså en stillingtagen til om de eksisterende teknologiske muligheder måtte udnyttes! Og der er såmænd ikke så meget nyt under solen med de nye overvågningsprogrammer – blot interesserer de sig ofte mere for, hvad man bruger spildtiden til end den egentlige arbejdstid.

Egentlige overvågningsprogrammer eksisterer i dag til videoselektering af videoovervågning, så man kan automatisk kan afgrænse registreringen f.eks. til de perioder, hvor der er aktivitet.
Tasteregistrering – dvs. registrering af hvert eneste tryk på en keyboard-tast - eksisterer som programmer, hvor taste-logs automatisk sendes til en central server. E-mail-scanning kan i dag sættes op til at behandle e-mails med fastlagte udtryk ved at registrere eller for den sags skyld stoppe dem.

Programmer kan sikre mod download fra Internettet.
Programmer kan anvendes til at registrere en anvendelsesprofil af surfing på Internettet.

Elektronisk registrering

Det store problem i dag er netop mangelen på synlighed. Den elektroniske overvågning foregår via administrativ personregistrering; men det nye er softwareagenter i vores arbejdsstationer: de kan hjælpe os hvis vi ikke kan huske funktioner i programmellet, minde os om, at programmellet burde opdateres; men også registrere anvendelsesprofilen fra brugeren. Anvendelsesprofilen skal her ses bredt, idet mange af oplysningerne er af rent teknisk art; men de kan anvendes til at f.eks. gemme særlige profiler på e-mail eller internet-forbrug. Vi ved i dag også, at visse programmer er forberedt for at amerikanske autoriteter via Internettet kan skabe sig adgang til funktionaliteter – i dag primært til de-kryptering af kodede meddelelser.

1. Registerloven hedder efter sommerens vedtagelse Lov om behandling af personoplysninger og nu er persondata blevet til en vare og skal derfor – udover at følsomme oplysninger stadig skal behandles separat – behandles med respekt for OECD's handelsaftaler dvs. de kan sælges internationalt. Det formildende er, at man kun må anvende data til det formål de er indsamlet. Dette betyder, at der vil være en stigende fokusering på, hvad der registreres og med hvilket formål.

2.Den eneste sag, som der har været behandlet tidsmæssigt før lovens ikrafttrædelse men med skæven til denne er problemstillingen på Tryg-Baltica. Ledelsen anvendte her logs opsamlet af hensyn til sikkerhed og driftsstabilitet med et andet formål: nemlig at dokumentere fyringsgrund på en medarbejder, der surfede for meget i sin arbejdstid.

3.Datatilsynet, som er nedsat til at administrere loven, vendte da også i deres behandling af sagen tommelfingeren nedad på dette punkt; men undgik helt at forholde sig til, at firmaet ikke havde ansøgt om at få lov, og stemplede det som acceptabelt, fordi medarbejderne var blevet informeret. Datatilsynet lægger altså op til, at ledelsen ligesom med Lov om videoovervågning blot sætter et klistermærke på PC'en: "Du bliver registreret" – og derefter er det uden diskussion af formål, berettigelse m.m. tilladt.

4. Netop analogien med telefon-anlægget er interessant, fordi den tidligere lov indeholdt en restriktiv bestemmelse, der sagde, at en arbejdsgiver ikke måtte registrere den ansattes telefonforbrug – alligevel har Datatilsynet givet lov til at registrere internetforbruget – også selv om virksomheden forbryder sig mod lovens princip om, at data indsamlet med et specifikt formål ikke må anvendes med et andet formål for øje

Så vidt vides anvendes det ikke i større omfang, - men....
For et par år siden begyndte PROSA at opleve enkeltstående sager, hvor et medlem blev sat til at kontrollere kolleger, overvåge funktioner eller lignende og derfor henvendte til deres fagforening. I løbet af i år er der kommet så mange henvendelse om dette – og også at være udsat for overvågning – at PROSA gennemførte en arbejdspladsundersøgelse, der antyder at dette problem er klart stigende – og meget mere interessant: skaber konflikter på arbejdspladser mellem arbejdsgiver og de ansatte.

Kim Munch Lendal, Juridisk direktør, Dansk Handel & Service

Spørgsmål:
- Hvad er formålet med elektronisk overvågning på arbejdspladsen ?

Muligheden for at foretage elektronisk overvågning på arbejdspladsen eksisterer. Derfor er det meget relevant at vide, hvorfor en arbejdsgiver i det hele vælger at tage dette skridt. Arbejdsgiverne føler ikke nogen glæde ved at etablere elektronisk overvågning af virksomheden, men man gør det alene for at sikre sig selv mod uregelmæssigheder og for at sikre medarbejderen.

I detailhandlen har man et betydeligt svind - anslået til minimum 3 mia. kr. pr. år. Der er tale om kundetyveri og medarbejdertyveri samt svind i øvrigt. Detailhandlen er derfor nødsaget til at iværksætte nogle kontrolforanstaltninger, herunder videoovervågning for at mindske svindet.

Iværksættelsen af disse elektroniske overvågninger er, hvad man arbejdsretligt kalder en kontrolforanstaltning. Arbejdsgiveren leder og fordeler arbejdet, og en del af denne ledelsesret er retten til at iværksætte kontrolforanstaltninger.

Det er ikke frit spil med hensyn til at lave overvågning. Arbejdsretlig praksis har opstillet et sæt af kriterier, der er relevante, når man ser på, om det er lovligt at overvåge. Der er tale om en afvejning af hensynet til både arbejdsgiveren og lønmodtageren. For det første skal overvågningen have et fornuftigt og sagligt formål, den må ikke gå længere end nødvendigt, og for det tredje må overvågningen ikke være krænkede for den enkelte medarbejder.

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. Medarbejderne skal være helt klar over formålet med denne type foranstaltninger.

Det er også vigtigt at fremhæve det sikkerhedsmæssige aspekt. Det giver medarbejdere 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 medarbejderen.

Elektronisk overvågning kan komme i flere varianter. Jeg vil fokusere på videoovervågning

Videoovervågning
Overvågning af arbejdspladserne ved hjælp af TV eller video anvendes primært i detailhandlen. Kameraerne opstilles for at forhindre det betydelige svind, der løbende konstateres og for at sikre medarbejderen mod risikoen for at blive udsat for vold.

Opsætningen har et forebyggende og opklarende mål. Detailhandlen bruger store summer på at sikre sig mod svind, der som ovenfor nævnt er i milliardklassen

Det er ikke nogen hemmelighed, at arbejdsgiverne hellere var det foruden, men man er på den anden side nødsaget til at sikre sig mod tyveri. Det er ikke nogen fornøjelse at overvåge kunder eller medarbejdere.

Er der svind i en forretning, er det også ubehageligt for medarbejderen. Uregelmæssighederne består langt overvejende i, at der sker kundetyverier. Disse tyverier er medarbejderne lige så interesserede i at få opklaret, som arbejdsgiveren er.

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, der ikke er almindelig adgang til. Det kan være lageret eller kantiner. Forsvinder der ting herfra, kan gerningsmanden kun findes blandt dem, der har adgang til området, og det har personalet. 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, der er for at overvåge uden skiltning, er, hvis det sker som led i en strafferetlig efterforskning.

Det hører til blandt sjældenhederne at overvåge 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 mistanke om tyveri.

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.

Jørgen Hoppe, HK - HANDEL

Spørgsmål:
- Hvad er fagforeningens holdning til overvågning af medarbejdere?
- Hvilke problemer ser arbejdsgiverne?

Overvågning er fra at være et begreb, som man forholdt sig særdeles negativt og kritisk til, gået over til at være et hverdagsbegreb med en overvægt af positive klangtoner. Eller i det mindste til at være et begreb, som ikke straks får nakkehårene til at rejse sig, fordi der som regel er knyttet nogle "positive" funktioner til begrebet.
Det har vi set eksempler på i hobetal i detailhandelsbranchen, siden de første overvågningskameraer blev opsat i begyndelsen af 80'erne. Og vi ser dagligt nye områder blive indlemmet i kredsen af objekter, som af den ene eller anden grund åbenbart bliver vigtige at overvåge elektronisk.

Lad det være sagt straks: Overvågning er ikke udelukkende positiv.
Der er i langt de fleste af de eksempler på overvågning, som jeg kender til, næsten altid knyttet en byge af negative konsekvenser til overvågningen. Men desværre bliver der som regel skøjtet let henover de negative sider.

Og det er der mange årsager til. De virksomheder, som sætter udstyret op tjener godt på at sælge, og nogle – ikke alle – forsømmer sig groft mod, hvad der er god moral og etik ved overvågning.

Den samme synd gør mange butikker sig skyldige i. De opsætter overvågningsudstyr uden at inddrage de ansatte, og uden at tage højde for, at det kan være groft krænkende at blive overvåget. Og begrundelsen er klar. Butikkerne mener at kunne begrænse svind og dermed spare penge ved at overvåge. Det har vi dog endnu ikke set dokumentation for. Tværtimod er det vores erfaring, at det ikke er et kamera men en styring af omgangen med varer i butik og på lager, der kan nedbringe svindet.

Derfor mener vi også, at overvågning af personalet ofte i sig selv kan volde større skade end den skade, butikkerne prøver at gardere sig imod.

Det er indlysende, at ansatte, der overvåges konstant, er under et voldsomt psykisk pres og får deres arbejdsmiljø forringet betydeligt. Butikkerne møder de ansatte med mistillid og kontrol, hvilket hverken er motiverende eller fremmende for samarbejdet. Man kan ikke forlange sit personales respekt, hvis man selv går bag ryggen af dem og spionerer i det skjulte.

Virksomhederne må, inden de opsætter overvågningsudstyr, også tage disse forhold med i betragtning. Det glemmer de imidlertid ofte. Faktisk er det vores oplevelse, at dem, der køber/anvender udstyret, fokuserer så lidt på de negative sider af overvågningen, at de som oftest opfatter eksempelvis HK/HANDEL's gode råd, som værende udtryk for en generel modstand imod anvendelse af overvågnings- og kontrolforanstaltninger mere end som det det faktisk er; en række gode råd om etisk anvendelse af udstyret.

I HK/HANDEL er vi imidlertid ikke afvisende over for TV-overvågning. Men vi kræver, at overvågning anvendes i overensstemmelse med god moral og etik.

Vi mener, at TV-overvågning er i orden, når udstyret er opsat og anvendes etisk korrekt i forbindelse med mistanke om kundetyverier og ved forebyggelse af røverier og vold på f.eks. tankstationer. Derimod mener vi ikke, at det er acceptabelt, hvis overvågningen udelukkende har til formål at overvåge personalets gøren og laden. Og det er slet ikke acceptabelt, hvis teknikken anvendes til skjult overvågning af de ansatte.

Desværre har vi set mange eksempler på, at overvågningen er etableret helt i strid med god moral.

HK/HANDEL har gentagne gange rejst dette problem over for arbejdsgiverne ved overenskomstforhandlingerne. Men det er med undtagelse af bageområdet aldrig lykkedes os at få en aftale. Arbejdsgiverne har ikke ønsket en dialog om etik og moral i forbindelse med overvågningen.

I 1997 tog vi konsekvensen heraf. Vi kontaktede Justitsminister Frank Jensen og gjorde opmærksom på, at der var store problemer omkring TV-overvågning.

Overvågningsudstyret var blevet rørende billigt, og vi oplevede, at flere og flere arbejdsgivere satte overvågningsudstyr op for i det skjulte at overvåge de ansatte i frokoststuen, på lageret og i butikkerne.

Som eksempel kan jeg nævne, at vi oplevede medlemmer, som blev skjult overvåget af et kamera på størrelse med en 5 krone fastsat i et ringbind. Vi har også oplevet ansatte, som er blevet aflyttet af mikrofoner placeret i urtepotteskjulere. Og det er ikke i orden. Faktisk er hemmelig aflytning direkte strafbart.

Justitsminister Frank Jensen inviterede os med i et udvalg, som skulle skabe forbedrede retningslinier. Det klare formål med udvalgsarbejdet var at skabe regler, der beskyttede de ansattes personlige integritet.

Arbejdet mundede ud i et lovforslag, der forpligtede arbejdsgiveren til at informere de ansatte om overvågning og opsætte skilte om tv-overvågning. De ansatte skal - som det fremgår af bemærkningerne til loven - sikres kendskab til, om de befinder sig på et område

på arbejdspladsen, hvor der var TV-overvågning. HK/HANDEL tog i lovforslaget forbehold for at rejse spørgsmålet om TV-overvågning på ny, hvis det viser sig, at de skærpede regler ikke er tilstrækkelige. Samtidig påpegede vi, at det er nødvendigt, at der også bliver taget hånd om de problemer med det psykiske arbejdsmiljø, som overvågningen skaber.

Loven trådte i kraft den 1. april 1999. Og vi kan nu allerede her 1½ år efter konstatere, at loven på ny trænger til en gennemgang.

Den teknologiske udvikling på området går forbløffende stærkt. I dag er kameraerne på størrelse med et knappenålshoved, og de er ikke længere fastmonteret, hvilket gør, at virksomhederne nu frit kan flytte rundt med kameraerne. Og hverken de ansatte eller kunderne har mulighed for at kontrollere, hvor kameraerne er placeret. Vi har set eksempler på, at kameraer har været sat op i omklædningsrum, hvilket hverken kunderne eller de ansatte kan være tjent med.

Og det finder vi meget betænkeligt. Desværre har vi måttet konstatere, at lovgivningen ikke giver de ansatte og kunderne mulighed for at konstatere, om virksomhederne lever op til god moral og etik. Folketingets Retsudvalg tilkendegav i starten af året, at det faktisk er i overensstemmelse med lovgivningen, at arbejdsgiverne ikke har pligt til at fortælle de ansatte, hvor mange kameraer der er, og hvor de er sat op. Retsudvalget udtalte samtidig, at arbejdsgiveren i større supermarkeder heller ikke er forpligtet til at sætte skilte op i hver eneste afdeling, hvor der TV-overvåges. I et større supermarked som Bilka, er man således ikke forpligtet til at sætte skilte op i hver enkel afdeling. Dermed fortolkes loven lempeligere, end vi mener, det var tilsigtet. Fortolkningen betyder, at de ansatte ikke længere er beskyttet mod skjult overvågning, og det var ellers meningen med vedtagelsen af lovændringen.

HK/HANDEL mener derfor, at der er behov for en opstramning af loven. Vi må skjult overvågning til livs. Det er ganske umoralsk at overvåge kunder og ansatte, uden at de er klar over det. Alle må have ret til at vide, hvor kameraerne sidder, ligesom skiltningskravet må strammes op.

Samtidig må vi ved en ændring af loven tage højde for, at der siden lovændringen trådte i kraft, er sket en væsentlig teknologisk udvikling. Overvågningsudstyret i dag er blevet trådløst og uhyre billigt. Da loven blev ændret, var de kameraer, som blev sat op, fastmonteret. I dag er udstyret trådløst og kan flyttes rundt i butikker og baglokaler fra dag til dag. Og så har vi en ny situation, som gør livet endnu nemmere for dem, der gør tingene i det skjulte. Derfor er det vigtigt, at der er nogen i den meget brogede overvågningsbranche, man kan sætte sin lid til, og som har ansvar for, at systemerne er lovlige. En autorisation knyttet op på nogle etiske regler er oplagt. Det vil give de ansatte og forbrugerne en tryghedsgaranti for, at overvågningsudstyret blev etableret i overensstemmelse med god etik og moral. Den sikkerhed mangler vi i dag.

Går man på internettet finder man mange udbydere af overvågningsudstyr. Som eksempel kan vi nævne, at reolfirmaet Tri-Lines på deres hjemmeside reklamerer for et trådløst overvågningskamera til 3.000 kr. – og det MED LYD!, som det står fremhævet i annoncen. Men når det gælder lige netop lyd, er lovgivningen klar: Overvågningskameraer må ikke optage lyd kun billede.

Sådan er reklame fra Tri-Line er dybt kritisabel. Den er direkte i strid med straffeloven. Et firma som dette bør under ingen omstændigheder reklamere for direkte ulovligheder. Men det er endnu et argument for, at folk, der sælger og monterer anlæg, burde igennem en godkendelsesproces.

Et andet problem, som HK/HANDEL har kæmpet for at gøre noget ved er de psykiske arbejdsmiljøproblemer, som TV-overvågning fører med sig. Det er vores erfaring, at kontinuerlig eller vedvarende overvågning fører til krænkelser af de ansatte, som kan resultere i psykiske belastninger f.eks. post traumatisk stress-syndrom.

For at hindre, at den omsiggribende TV-overvågning ikke fører til et forringet psykisk arbejdsklima for de ansatte, mener vi, at Arbejdstilsynet skal have mulighed for at gribe ind over for TV-overvågning. Det har Tilsynet ikke i dag.

Det er ingen hemmelighed, at de ansatte føler sig voldsomt presset af at være overvåget. Det er stressende konstant at have et kamera i nakken. Men endnu værre er det at blive udsat for skjult overvågning. Personer, som har været udsat for skjult overvågning, reagerer som voldsofre eller andre, der har været udsat for en voldsom psykisk belastning.

Det kan vi ikke byde de ansatte. Derfor må Arbejdstilsynets mulighed for at gribe ind i sager på arbejdspladsen også udvides til at omfatte overvågning.

Men overvågning er jo ikke blot TV-overvågning. Det er også IT-overvågning af de ansatte. Mange danske virksomheder registrerer og gemmer oplysninger om ansattes brug af e-mail og internet uden at oplyse om det. Det er i dag muligt at overvåge alt, hvad medarbejderne foretager sig på nettet, og hvilke e-mail-adresser den elektriske postmand leverer adresser til og fra. En stor del af virksomhederne gemmer automatisk en kopi af hele molevitten. Og så har de en base, hvor det er muligt at søge efter medarbejdere, som bruger for eksempel ordene ”jobansøgning” eller ”brystkræft” i deres elektroniske post, og dermed kan de kontrollere, om folk søger nyt job eller er blevet syge.

Det er i dag lovligt at gemme oplysningerne, men de ansatte skal underrettes. Det bliver mange ansatte ikke. Og det er naturligvis dybt kritisabelt.

Men i HK/HANDEL kan vi heller ikke acceptere, at virksomhederne gemmer alt. Der skal være et sagligt formål med at arkivere og kontrollere medarbejderne. Det er derfor også

nødvendigt med en modernisering og opstramning af de gældende regler, som slet ikke er gearede til at takle de nye problemstillinger, som den rivende teknologiske udvikling har skabt. Samtidig er der behov for, at medarbejderne og virksomhederne sætter sig sammen i samarbejdsudvalget og diskuterer etik og moral og aftaler de nærmere retningslinier for kontrollen.

Jeg vil godt dvæle lidt ved begreberne etik og moral.

Der opsættes i dag overvågningsudstyr i hobetal. Ikke blot i butikkerne men også alle mulige andre steder i samfundet.

Hjemmehjælperen skal i dag kode sig ind hos hver enkel beboer, hun besøger, og nøjagtigt indtaste, hvad hun laver. Postbudet skal i dag flere gange på ruten have aflæst en stregkode ved en kontrolpost, sådan at posthuset kan kontrollere, at der ikke holdes pauser.

Rækken af områder, der omfattes af overvågningssystemer vokser dag for dag.

Hovedrystende og undrende må jeg dagligt spørge mig selv, om man virkelig har tænkt sig nøje om, da man indførte dette eller hint overvågningssystem, eller om "man bare" greb til den nemme løsning uden sans for hvilke ulemper, der kunne tænkes at følge i kølvandet på pågældende overvågningssystem.

Når jeg eksempelvis ser, at man i en børneinstitution har opsat web-kameraer, der gør det muligt for de passede børns forældre at følge børnenes – og pædagogernes - gøren og laden dagen igennem, spørger jeg mig selv: Er det virkelig nødvendigt? Og til gavn for hvem og med hvilket reelt formål er disse kameraer opsat?

Når jeg i radioen hører, at der nu er produceret en chip, der kan indopereres i børn, så forældrene altid kan følge børnenes færden, undres jeg såre.

Når jeg ser på tv, at kriminalforsorgen vil forsøge at komme fangeflugter til livs, ved at udstyre de indsatte med en fodring, der er forsynet med en chip, der altid kan afsløre fangens opholdssted, ser jeg tidligere tiders tugthusfanger for mig, og spørger mig selv om omfanget af fangeflugter er så stort, at det berettiger slige overvågningssystemer.

Når jeg i dagligdagen - som bruger af taxa – ser, hvor meget hurtigere jeg – grundet bl.a. satellitovervågning - i dag får en vogn i forhold til tidligere, glædes jeg som kunde over udviklingen, alt imens jeg stiller spørgsmålstegn ved chaufførens frihed.

Vi har travlt med at holde øje med hinanden i en grad, der ville være ganske uhørt for få år siden.

Når jeg tænker tilbage på, hvordan man opfattede George Orwells roman "1984" som en uvirkelig skrækvision, med fed streg under skræk, og når jeg tænker tilbage på, hvilken frygt der var for Bigbrother-samfundet for bare 20 år siden, da et butikscenter i Holstebro indførte udendørs tv-overvågning, der skulle afsløre eventuelt hærværk, må jeg undres over, hvad der ligger til grund for det totale holdningsskifte, der er sket på de relativt få år.

Udover de overvågningssystemer, der er knyttet til de forskellige og mangeartede jobs og jobfunktioner, jeg tidligere har omtalt, må jeg undres over den tavshed – manglende debat - der knytter sig til den omsiggribende anvendelse af web-kameraer på offentlig gade og vej. At der i lande, hvor man ikke på samme måde som i Danmark værner om privatlivets fred, kan opsættes kameraer hvor som helst, er eet.

Men at konstatere, at der f.eks. på POLITIKENS HUS på Rådhuspladsen sidder et web-kamera, der skifter billede hvert minut, må føre til undren, da bevægelsesfrihed og ytringsfrihed efter min opfattelse, er to sider af samme sag. Et tilsvarende indgreb i ytringsfriheden, som det indgreb i bevægelsesfriheden opsætningen af web-kameraet indebærer for den intetanende borger, havde næppe undgået demokrativogternes skarpe penne og utvetydige meningstilkendegivelser. Vi må ud over denne ligegyldighed og tavshed. Derfor hilser jeg også denne konference velkommen. Der er brug for, at vi taler højt om problemerne. De kan ikke ties ihjel. Og der er brug for, at vi drøfter, hvor langt vi vil gå med overvågningssamfundet. Hvilke værdier vil vi basere vort samspil på? God gammeldags tillid eller den omsiggribende mistillid, som overvågning er et udtryk for.

_____
Det er det talte ord, der gælder

Anne Kathrine Schøn, DA

Spørgsmål:
- Hvad er arbejdsgiverens holdning til overvågning af medarbejdere?
- Hvilke problemer ser arbejdsgiveren?

Generelt om kontrolforanstaltninger
Den teknologiske udvikling går stærkt, og det er da forståeligt, at risikoen for et overvågningssamfund optager de fleste.
Tanken om et overvågningssamfund gør os urolige, og det uanset om overvågningen sker på arbejdspladsen eller andre steder.
Den uro skal vi undgå, og derfor er det så vigtigt, at der er klarhed over spillereglerne.
Den klarhed skal arbejdsgiverne tilvejebringe, når kontrollen vedrører arbejdspladsen.
Arbejdsgiverne skal opstille retningslinjer for, hvornår og hvordan medarbejderne kontrolleres. Og det skal sikres, at medarbejderne kender retningslinjerne.

Arbejdsgivernes ledelsesret
Arbejdsgiverne har retten til at lede og fordele arbejdet. Herunder hører også retten til udstikke retningslinjer for arbejdets udførelse og retten til at kontrollere, at retningslinjerne følges.
Der har gennem årerne – siden indgåelsen af Hovedaftalen mellem DA og LO i septemberforliget 1899 – udviklet sig et ganske klart regelsæt om arbejdsgivers kontrolforanstaltninger. Regelsættet beskæftiger sig først og fremmest med spørgsmålene om, hvorfor der indføres kontrolforanstaltninger, og hvornår der indføres kontrolforanstaltninger.
Hvorfor kontrol?
Al kontrol skal være driftsmæssigt begrundet. Det betyder, at hensynet til en fornuftig drift af virksomheden skal tilsige kontrollen. Det kan for eksempel være pga. krav til sikkerheden på arbejdspladsen – eller mere specifikt sikkerheden om bord på skibe – eller det kan være pga. ønsket om at sikre en fornuftig brug af virksomhedens IT.

Det betyder også, at arbejdsgiveren ikke må udøve kontrol med et usagligt formål, herunder at få kendskab til medarbejdernes private forhold.

Hvordan kontrol?
Alle kontrolforanstaltninger skal være driftsmæssigt begrundet. Det er den generelle hovedbetingelse.

Dernæst må kontrollen ikke være krænkende eller forvolde tab eller nævneværdig ulempe for medarbejderne, og kontrollen må ikke gå videre end påkrævet.

Det fagretlige system
Kontrolforanstaltninger skal drøftes i samarbejdsudvalget.

Finder medarbejderne, at en eller flere af de betingelser, der er nævnt, ikke er opfyldt, kan sagen prøves fagretligt.

Andre regelsæt om kontrol
De arbejdsretlige regler om arbejdsgivers indførelse af kontrolforanstaltninger suppleres på nogle områder af regler i lovgivningen af mere generel karakter. Det vil sige regler, der i højere eller mindre grad gælder også i andre retsforhold end retsforholdet mellem arbejdsgiver og medarbejder.

Disse regler i lovgivningen skal arbejdsgiverne naturligvis også følge, når der indføres kontrolforanstaltninger.

De i den forbindelse mest relevante lovgivning findes i persondataloven og i straffeloven, og vi taler her om kontrol, der vedrører medarbejdernes private brug af e-mail og Internet, samt telefonaflytning.

Uden at gå i detaljer, kan man kort sige, at lovgivningen først og fremmest understøtter kravet om saglighed med hensyn til formålet bag en given kontrolforanstaltning og måske skærper kravet til den orientering, arbejdsgiver skal give til medarbejderne i forbindelse med indførelsen og praktiseringen af kontrolforanstaltningen.

Særligt om e-mail og Internet
Den teknologiske udvikling på IT-området har haft kolossal betydning for virksomhederne. Og der er ingen grund til at tro, at denne betydning vil blive mindre eller forblive på det nuværende niveau. Tværtimod !

Virksomhedernes kommunikation med omverdenen og i virksomheden internt, virksomhedens informationssøgning og meget andet er næsten fuldstændig afhængig af informationsteknologien (IT'en). Og altså også afhængig af, at der ikke sker nedbrud.
IT-sikkerheden

Der bruges mange ressourcer – både i mandetid og gennem indkøb af materiel og programmer – på at sikre sig mod nedbrud. Men dette alene kan ikke forhindre nedbrud. Det så vi jo senest med den så berømte "I love you"- virus, der gjorde også mange danske virksomheder ukampdygtige i flere dage. Medarbejderne kunne ikke gøre andet end sidde og trille tommelfingre, og virksomhederne mistede mange, mange millioner.

IT-sikkerheden skal altså være i top, og det er først og fremmest derfor, der sker logning af e-mail og Internetbrugen. Gennem logningen kan virksomheden lokalisere "farlige" (dvs.

virusbefængte) mail og programmer, og er skaden sket, kan logning gøre det lettere at rette op på skaderne.

Tillader virksomheden, at medarbejderne også bruger systemerne til private mail og privat søgning på Internettet, vil denne private brug altså også blive logget.

Det er i sig selv helt fornuftigt, da risiko for virus m.m. i lige så høj grad gør sig gældende her.

Går systemet ned – eller er der risiko for nedbrud – kan det altså være nødvendigt at åbne private mail.

Men der kan også forekomme andre situationer, hvor det tjener et sagligt formål at åbne private mail.

Udarbejdelse af retningslinjer
Hvis en virksomhed logger og vil have mulighed for at åbne private mail, skal virksomheden sikre sig, at medarbejderne er bekendt hermed.

Virksomheden skal derfor udarbejde klare retningslinjer, der redegør for
hvordan systemerne må bruges
at der logges
at logningerne kan kontrolleres
at der kan forekomme situationer, hvor private mail åbnes
mulige konsekvenser af misbrug.

Medarbejderadfærd
Medarbejderne har så mulighed for at indrette deres adfærd herefter.

Det betyder, at medarbejderne kan undlade at besøge de Internet-sider, der vedrører emner, som interesserer medarbejderen, men hvor medarbejderen ikke ønsker, at arbejdsgiveren skal kende til denne interesse.

Det betyder også, at medarbejderen kan undlade at sende mail, der omhandler sådanne private forhold, som arbejdsgiveren ikke skal kende til.

Og så er vi tilbage ved udgangspunktet – nemlig at der ikke må herske uklarhed om, hvad der foregår på virksomheden. Uklarhed gør det nemlig ikke muligt for medarbejderne at indrette adfærden efter den kontrol, der foretages.

Trine Rode, magister i kommunikation fra Aalborg Universitet

Spørgsmål:
- Hvilke løsninger ser arbejdsgiveren og fagforeningen?

Jeg har fået til opgave at svare på underspørgsmålet, der går på, hvilke løsninger fagforeningen og arbejdsgiverne ser. Med den viden og erfaring jeg har, vil jeg fokusere på hvilke løsninger, der kan være som både de ansatte og arbejdsgiver kan være tjente med. Og det gør jeg ved at fremdrage udledninger og konklusioner fra min specialeafhandling " *Videoovervågning – tryghed eller krænkelse?*" udarbejdet fra kommunikationsuddannelsen på Aalborg Universitet

En af de måder, den elektroniske overvågning af mennesker sker på i samfundet i dag, er ved at opsætte videoovervågning diverse steder, for at sørge for at tingene sker, som de skal, skabe tryghed, forhindre røveri- og tyveriforsøg og mindske svindet. Det har i hvert fald været nogle af de begrundelser, der har været fra bl.a. arbejdsgiveres side for at tage videoovervågning i brug. Det, man så kan spørge om, er, om videoovervågning vitterligt skaber tryghed, forebygger røverier og tyverier og mindsker svindet, for effekten af videoovervågning er nemlig ikke undersøgt. Det har i flere år været almindeligt med videoovervågning i eksempelvis banker, på posthuse, i døgnbutikker, hvor ansatte står alene om aftenen osv. Her har formålet synes klart, nemlig at forhindre røveriforsøg og samtidig give de ansatte den sikkerhedsfølelse, der ligger i at vide, at der bliver holdt øje med, at der ikke sker dem noget. Det, der er sket i samfundet i løbet af de sidste år, og som synes at blive mere og mere almindeligt, er, at videoovervågning også rykker ind på andre områder af arbejdsmarkedet, hvor behovet og formålet ikke synes så indlysende. Hertil må spørgsmålet lyde om en videoovervågning, som de ansatte måske ikke umiddelbart kan se behovet og formålet med, kan opfattes som en kontrol af dem som ansatte, således at forstå, at de som ansatte føler, at det er dem, der er under opsyn. Det kan føles belastende for de ansatte hele tiden at "have øjne i nakken", hvilket kan føre til en meget stresset arbejdstilværelse, der på sigt kan påvirke arbejdsmiljøet i ugunstig retning. Det må siges, at samfundet trænger til en debat på området, så der kan blive diskuteret, hvor grænserne går for den videoovervågning, der bliver mere og mere udbredt.

Man kan i den forbindelse starte med at spørge om videoovervågning skaber tryghed på arbejdspladsen eller om det snarere må anses for en krænkelse af de ansatte? Mine undersøgelser i forbindelse med udarbejdelse af mit speciale fra kommunikationsuddannelsen fra Aalborg Universitet viser, at det ikke er enten-eller, men både-og. Spørgsmålet om videoovervågning på arbejdspladsen skaber tryghed for de ansatte eller føles som en krænkelse, og eventuelt betragtes som en form for social kontrol, afhænger af en række forhold, herunder især *hvilken* arbejdsplads, der er tale om, hvad *formålet* med overvågningen er, og hvem de ansatte *er* som personer. Det betyder igen, at

det er en række komponenter, der må inddrages, når der skal tages stilling til, om der på en given arbejdsplads skal eller ikke skal indføres videoovervågning.

Konklusionen må da være, at samtalen mellem arbejdsgiver og de ansatte er essentiel, når man fra arbejdsgivers side påtænker at indføre videoovervågning. Det skyldes, at videoovervågning må, også selv om det ikke er afklaret i praksis, betragtes som en så indgribende foranstaltning, at det er noget arbejdsgiver bør tale sig til rette med de ansatte om. Foranstaltningen skal således ske med informeret samtykke fra de ansatte, i hvert fald, hvis arbejdsgiveren vil handle så etisk forsvarligt som muligt over for sine ansatte. Dette skal forstås på den måde, at de ansatte er informeret omkring foranstaltninger, der har indflydelse på deres arbejde eller psykiske trivsel, og de skal være indforstået med dette. Det man via samtalen kommer frem til kan være, at videoovervågning ikke skal indføres, eller det kan være, at det skal. Det vigtige i denne sammenhæng er, at man får vendt behovet for sikring og finder ud af om videoovervågning vitterligt er den bedste løsning, eller om der er andre og måske bedre metoder. Viser det sig, at videoovervågning er den bedste sikring, bør der diskuteres retningslinjer for dets indførelse, således at de ansatte er grundigt informeret om, hvor og hvor der ikke er videoovervågning, således, at hvis de har brug for det, kan komme væk fra "kameraets linse". Overvågningsfrie arealer er vigtige, så de ansatte ikke føler sig under konstant overvågning. Er der ikke mulighed for dette, så er der stor sandsynlighed for, at det kan påvirke det psykiske arbejdsmiljø i ugunstig retning.

De retningslinjer man taler sig til rette om, arbejdsgiver og de ansatte imellem, kan nedskrives i en såkaldt lokalaftale, som så kommer til at gælde på linje med en overenskomst på den pågældende arbejdsplads. At få udformet en lokalaftale på en given arbejdsplads kan samtidig virke gunstigt ind på det psykiske arbejdsmiljø, og dermed den enkeltes trivsel på jobbet. Det skyldes, at indføring i, samt indflydelse på egen arbejdsfunktion og –forhold er faktorer, der virker positivt ind på det psykiske arbejdsmiljø. I forbindelse med videoovervågning virker det bl.a. positivt ind, fordi de ansatte får en indsigt i, *hvorfor* videoovervågningen er taget i brug, og hvordan det bruges. Samtidig kan arbejdsgiveren modvirke, at de ansatte føler det som mistillid til dem som arbejdskraft, eller føler det som en decideret kontrol af *dem,* hvilket ikke er befordrende for et godt psykisk arbejdsmiljø. Desuden betyder en lokalaftale også, at de ansatte bliver informeret om, hvad konsekvenserne er for dem, hvis de gribes i ulovligheder. At de ansatte har mulighed for på skrift, at få indsigt i deres arbejdsforhold, betyder ligeledes, at de kan komme med indsigelser, eller eventuelt finde andet arbejde, hvis de ikke kan arbejde under de gældende forhold. Kommer de ansatte på sin side ikke med indsigelser, kan man sige, at de er kommet med et stiltiende samtykke. Nedskrives retningslinjer for videoovervågning på sin side ikke, og informeres de ansatte ikke om disse, så har de ansatte heller ingen reel mulighed for at komme med indsigelser. Man kan sige, at respekten for deres autonomi, deres ret til at vælge og vælge fra, er taget fra dem, og det må i mange henseender betragtes som uetisk. Om en arbejdsgiver vælger at inddrage de ansatte i beslutningsprocessen omkring indførelse af videoovervågning, er til syvende og sidst et spørgsmål om

arbejdsgiverens tolkning og forvaltning af ledelsesretten, der igen har noget med hans etiske ståsted og menneskesyn at gøre.

I forhold til videoovervågning og psykisk arbejdsmiljø, så forholder det sig sådan, at det, ligesom også påpeget med videoovervågning på arbejdspladsen generelt, at det afhænger af en række forhold. Dette betyder, at det ikke er så entydigt enten at sige, om videoovervågning påvirker det psykiske arbejdsmiljøet i negativ eller positiv retning. Konklusionen må derfor være, at der kan være arbejdspladser, hvor videoovervågning er en fordel, og arbejdspladser, hvor det er en ulempe. Da det er individuelt, hvornår den enkelte person føler sig krænket, er dette et område, der er meget svært at opstille regler omkring. Om den enkelte arbejdsgiver kan og vil tage individuelle hensyn, afhænger af mange forhold bl.a. hans/hendes etiske overbevisning, herunder værdier og menneskesyn. Nogle vil eksempelvis ikke tage individuelle hensyn, men handler i stedet ud fra, hvad der er bedst for arbejdspladsen som helhed, og de ansatte som gruppe. Det betyder igen, at det godt kan være, at der er ansatte, der føler sig krænket ved videoovervågning, men hvis størstedelen af de ansatte ikke har noget imod det, så indføres det, hvis det er gunstigt for arbejdsgiveren eller arbejdspladsen som helhed. Andre arbejdsgivere derimod tager gerne individuelle hensyn altså hensyn til den *enkelte* ansatte. Dette betyder i praksis, at hvis én eller få ansat(te) er imod videoovervågning, indføres det ikke, selvom de ansatte som gruppe ikke har noget imod det. Det må dog konkluderes, at det, især på større arbejdspladser kan være svært at tage individuelle hensyn, netop fordi det vil betyde at så *skal* videoovervågning indføres og på samme tid skal det *ikke* indføres. Hermed opstår der uundgåeligt etiske dilemmaer. Dette betyder, at arbejdsgiveren bliver sat over for at skulle træffe et (etisk) valg, og selve valget kan give anledning til etiske problemer, fordi hvordan prioriterer man mellem forskellige, måske lige vigtige hensyn. Konklusionen må være, at her kommer skønnet ind i billedet, og et sådant skøn er i bund og grund subjektivt, idet det helt afhænger af vedkommende, der træffer valget, og de tanker og overvejelser, der fører til valget.

Det kan i den forbindelse være nødvendigt at tale om et målsætnings- og anvendelsesniveau. En arbejdsplads/en arbejdsgiver kan eksempelvis have som målsætning, at der ikke videoovervåges det pågældende sted, og hvis der videoovervåges, så skal det ske med informeret samtykke fra de ansatte. Dog kan den konkrete situationen eventuelt fordre, at det kan være nødvendigt i visse tilfælde, at fravige de etiske principper, på målsætningsniveauet, og tage videoovervågning i brug, eller situationen kan kræve, at arbejdsgiveren skal handle her og nu og således ikke har mulighed for at inddrage og informere de ansatte. Om der skal fraviges etiske principper, hviler til syvende og sidst på et skøn fra arbejdsgivers side, og hvad (hvilke hensyn) han vælger at prioritere højest, afhænger helt af hans etiske ståsted, og dermed også hans livs- og menneskesyn.

I et lidt bredere perspektiv, på samfundsplan, kan man sige, at eftersom videoovervågning er et meget holdningsladet område, med mange forskellige og til tider modsatrettede holdninger og hensyn, må det siges, at være et svært område for politikerne at lovgive om.

Det, der er sket i forhold til lovgivningen på området, er, at der nyligt er sket en regulering af lov om forbud mod privates tv-overvågning. Reguleringen er sket som en konsekvens af den teknologiske udvikling og det faktum, at de ansatte på danske arbejdspladser fra 1982 til 1997 ikke har været juridisk beskyttet mht. arbejdsgiverens skjulte videoovervågning af dem på arbejdet. Reguleringen er sket efter et skøn, hvor forskellige hensyn er blevet sat op over for hinanden, og det har i dette tilfælde været hensynet til arbejdsgiver og hans berettigelse til at indføre kontrolforanstaltninger og sikre sin virksomhed på bedste vis, og så hensynet til det enkelte menneskes integritet. Fra politisk side har man skønnet, at disse hensyn bedst tilgodeses ved en udvidelse af skiltnings-pligten til også at gælde arbejdspladser, således at ansatte, på lige fod med eksempelvis kunder og publikum, skal beskyttes mod skjult videoovervågning. Det betyder i praksis, at de ansatte skal vide om de er på et område af arbejdspladsen, som er under videoovervågning. Tv-overvågningsloven af i dag omfatter både private og offentligt ansatte, med de undtagelser, der skal tages i forhold til offentlige myndigheder, der i modsætning til private, kan have behov for at foretage skjult videoovervågning. Her kan bl.a. nævnes politiets videoovervågning som led i en straffe-retslig efterforskning, videoovervågning af kriminalforsorgens institutioner som led i almindelig sikring mod undvigelse mv. eller med henblik på at beskytte militære anlæg.

Da en lov gerne skulle tilgodese så mange som muligt, vil en afvejning af interesser og hensyn fra politikernes side ofte ske ud fra et skøn, der naturligt nok vil tage udgangspunkt i, hvad der generelt set er bedst og ikke på enkelt tilfælde. Dermed bliver det vigtigt, at den enkelte arbejdsgiver, ikke bare gør noget, fordi det eventuelt er tilladt, men at han som sagt inddrager sine ansatte og derud fra finder retningslinjer for, hvad der på det pågældende sted er i orden og ikke i orden at gøre. For der behøver ikke nødvendigvis være overensstemmelse mellem etik (bør) og lov (må), forstået på den måde, at fordi noget er tilladt, behøver det ikke være etisk forsvarligt. Det er bl.a., hvad det har vist sig med tv-overvågnings loven, således at det i praksis har vist sig, at det stadig er muligt at foretage "skjult" videoovervågning af de ansatte, og også en decideret skjult overvågning af enkelte ansatte, uden at bryde loven. Dette skal forståes på den måde, at de ansatte godt nok er informeret om, at der på et givent sted er videoovervågning, men ikke præcis hvor kameraerne peger hen, hvormed arbejdsgiveren kan installere kameraer direkte på enkelte personer, f.eks. ved kasseområdet i butikker. Arbejdsgivere inden for detailhandelen kan f.eks. vælge at installere systemer såsom "kasseterminalovervågning" (Cashscan), for at sikre sig, at de ansatte ikke laver noget ulovligt. Dette system går ud på, at der opsættes et lille kamera over kasseapparatet, og så køres der data ind på lydsporet på videobåndet. Herved kan man ved at afspille et videobånd sammenholde billedet af varerne med de informationer, der er blevet indtastet på kasseapparatet. Systemet er meget brugt at installere, - også uden at fortælle medarbejderne om det! Dermed kan der således stilles spørgsmålstegn ved, om loven yder nok beskyttelse til ansatte på danske arbejdspladser.

I tv-overvågnings loven, er der ikke noget med omkring de data, der efterfølgende er på videobånd eller disk fra overvågningskameraerne, og reglerne omkring disse er meget

uklare. Regler herfor skal findes i den nye persondatalov, der trådte i kraft den 1. juli 2000. Det har vist sig i praksis, at netop dette forhold har skabt en del usikkerhed blandt den danske befolkning. Det synes derfor som et vigtigt punkt i fremtiden at se nærmere på, således at der enten defineres klare regler i selve tv-overvågnings- loven (som man har gjort i Norge), eller at man får lavet en central rammeaftale omkring dette, der eventuelt kan udfyldes lokalt. Det ville således betyde, at man fra centralt hold fik defineret nogle overordnede retningslinjer for *hvor længe* videobånd fra overvågningskameraer må opbevares, *hvor* de må opbevares, *hvem* der må få adgang til dem, *hvad* der sker med videobåndene efterfølgende osv. Disse overordnede retningslinjer kan man så mere specifikt uddybe på den enkelte virksomhed, alt efter forholdene, og nedskrive i den føromtalte *Lokalaftale*, der også indeholder retningslinjer for selve brugen af videoovervågning.

En måde at sikre, at optagelserne ikke kan ses af hvem som helst, og for at sikre mod misbrug kan man i dag gøre det, at der indlægges en elektronisk lås i systemet. Det bevirker, at når videooptagelser skal ses igennem, er det kun personer med kendskab til koden, der kan gennemse dataene. Det kan f.eks. aftales, at ledelsen kun må se de registrerede data, hvis der er en tillidsmand tilstede. Det, der så gøres, er, at parterne hver især får halvdelen af den kode, der skal til for at kunne "låse" låsen op, og se dataene. Man kan også vælge, at det kun må gennemses af tredjepart, det kan f.eks. være installatøren, politiet, eller hvem man nu har haft med at gøre. Derforuden kan man også gøre det, at man kan sende de data, der ligger fra overvågningskameraerne til kontrolcentralen. Dette betyder således, at dataene bliver gemt et andet sted end i virksomheden.

En anden faktor, der kan skabe mere tryghed blandt de ansatte på danske arbejdspladser og befolkningen mere generelt, er hvis der iværksættes en autorisationsordning for firmaer, der vil nedsætte sig som sælgere og opsættere af overvågningsudstyr. Personer eller firmaer, der i dag ønsker at nedsætte sig som sælgere og opsættere af overvågningsudstyr kan "bare" gøre det, der er ingen regler eller krav, der skal indfries. Så alle kan i realiteten starte et overvågningsfirma.

Det der er kendetegnet for overvågningsbranchen i øjeblikket er, at der bliver flere og flere udbydere, men hvor mange flere, og hvor mange udbydere der på nuværende tidspunkt er i Danmark vides ikke, og det skyldes bl.a., at der ikke er noget krav om autorisation. Det betyder videre at der stort set ikke nogen, der tjekker, at overvågnings-branchen holder sig inden for lovens rammer, andre end dem, der har kommerciel interesse heri, som f.eks. forsikringsselskaberne. Herved synes det netop vigtigt, at man får etableret en autorisationsordning inden for denne branche, idet det ville være en måde, at holde lidt tjek på branchen. Det kan også skabe tryghed blandt befolkningen at vide, at det ikke er hvem som helst, der må nedsætte sig som overvågningsfirma, men at der er nogle retningslinjer, der skal være opfyldt.

Man kan som juraprofessor Claus Haagen Jensen fra Aalborg Universitet gør, spørge sig selv, hvorfor ikke netop overvågningsfirmaer *skal* have en bevilling for at kunne nedsætte sig, når nu mange andre brancher skal, såsom eksempelvis sundhedspersonale af enhver slags, revisorer, advokater osv. Især set i lyset af at netop denne branche har så stor mulighed for at gå ind i folks privatsfære og krænke enkelt personer. Man kan så spørge sig selv om, hvorfor der ikke allerede er iværksat eller taget afsæt til at få iværksat en sådan autorisationsordning. HK/Handel fortæller, at de har lagt op til, at man skulle lave en autorisationsordning, i stil med den el-installatører skal have, ligesom de gerne så, at der blev defineret etiske regler for sælgere, eksempelvis lavet af branchen selv. Disse regler skulle bevirke, at hvis man overtrådte dem, mistede man sin autorisation og altså sin ret til at sælge og opsætte overvågningsudstyr. Dette var man ifølge HK/Handel ikke indstillet på fra branchens side, og som medlem af EU, er det et åbent marked, hvor der skal være lige vilkår for alle. Det skal i den forbindelse påpeges, at rent juridisk så er der ingen problemer i at få iværksat en sådan. Det har jeg erfaret efter en lang samtale med juraprofessor Claus Haagen Jensen fra Aalborg Universitet, og han siger i den forbindelse og jeg citerer ”*..det der med, at vores medlemskab af EU skulle hindre, at vi iværksætter en autorisationsordning for overvågningsfirmaer, det er ren snak”*. Det eneste det kræver er, at det fremlægges i Folketinget, og at man her kan få opbakning fra et flertal (altså mindst 90 mandater). Det synes derfor underligt, at der ikke allerede er iværksat eller taget afsæt til at lave en sådan, især set i lyset af, at der er tale om en branche i kolossal vækst, og en branche, hvori der er så mange ” brodne kar”. Dvs. personer, der ikke viger tilbage for at tjene penge, og eventuelt opsætter videoovervågning steder eller på måder, der er ulovlige eller etisk uforsvarlige. Det, man så kan spørge om, er, hvorfor HK/Handel ikke har undersøgt muligheden for at få iværksat en sådan ordning nærmere, når nu de i så høj grad påpeger vigtigheden af en sådan. Og i et videre perspektiv hvorfor, der i det hele taget ikke er nogen, der har undersøgt eller påpeget dette forhold.

Slutteligt er det vigtigt at påpege, at vi alle (som samfund) har et ansvar for, at tingene er og udvikler sig, som de gør. Det er således vigtigt, at man som befolkning, såvel som hver især, tager stilling til, hvad man vil være med til og ikke være med til, altså hvor grænsen går for ikke bare videoovervågning men elektronisk overvågning generelt i samfundet.

Udgivelser fra Teknologirådet

Mange af Teknologirådets udgivelser kan ses - og hentes gratis fra - Rådets hjemmeside www.tekno.dk.

Arbejdsliv
Nær eller fjern. Slutdokument og ekspertoplæg fra konsensuskonferencen om telearbejde 2. - 5. maj 1997. 1997. 95 kr. Best.nr. 182.

Som tiden går - hverdag og værdier. Et debatoplæg om fremtidens liv og arbejde. Video. 1993. 33 min. 100 kr. Med debathæfte. Best.nr. 447

Bioteknologi
Gensplejsede fødevarer. Slutdokument og ekspertoplæg fra konsensuskonferencen 12. - 15. marts 1999. 1999/2.

Kloning af dyr. Resumé og udskrift af høring i Folketinget den 9. april 1997. 150 sider. 95 kr. Best. nr. 181

Gensplejsede planter - regulering og anvendelse. Rapport fra ekspertseminar marts 1995. 1996. 90 sider. 80 kr. Best.nr. 171

Debatten om genteknologi. En dansk bibliografi for 1971 -1990. Ole Borre, Annie G. Frandsen og Peter Ørberg. 1992. 134 sider. 80 kr. Best. nr. 148

Bioteknologi og etik i den offentlige debat - i USA, Tyskland og England. Svend Andersen, Jørgen Husted og Viggo Mortensen. 1992. 90 sider. 80 kr. Best. nr. 147

Xenotransplantation. Resumé og redigeret udskrift af intern høring i Folketinget den 23. februar 2000. 35 kr. Best. nr. 205.

Gensplejsede fødevarer - Problemer og Perspektiver. Udskrift af oplægholdernes manuskripter ved konferencen på Christiansborg den 4. april 2000. 123 sider. 95 kr. Best nr. 206.

Grundvand/drikkevand
Drikkevand - rent vand, men hvordan? redigeret af Anne Funch Rohmann. 1997. 60 sider/ill. 40 kr. Rabat ved køb over 10 eks. Best.nr. 455

Danmarks grundvandsressource - et oplæg til handlingsplan. 1992. 92 sider/ill. 60 kr. Best. nr. 144

Fødevarer
Borgernes madpolitik - en undersøgelse af forbrugernes bud på fremtidens fødevarepolitik. Af Ida-Elisabeth Andersen og Trine Iversen. 1998. 150 sider.

Bioteknologi i levnedsmiddelsektoren. Konsekvenser for ansatte og forbrugere. Erling Jelsøe m.fl. 1990. 196 sider. 80 kr. Best.nr.134

Konsensuskonference om bestråling af madvarer. Slutdokument fra konsensuskonferencen 22.-24. maj 1989. 26 sider. 50 kr. Best. nr. 126

Informationsteknologi
Fremtidens tv og radio. Resumé og redigeret udskrift af høring i Folketinget den 1. februar 2000. 185 sider 35 kr. Best.nr. 204.

Info-samfundet - direkte demokrati og overvågning. Steffen Stripp (red.). 1998. 58 sider.

Informationsteknologi og folkeskolen - en udfordring! Bente Schwartz. 1997. 35 sider. 30 kr. Best.nr. 456

Fremtidens bibliotek - scenarieværkstedspakke. Teknologirådet tilbyder en scenarieværkstedspakke til alle folkebiblioteker. Pakken gør det muligt at holde værksted i den enkelte kommune om handlingsplaner for bibliotekets udvikling. Teknologirådet bidrager med blandt andet værkstedsledelse og en del af materialet til deltagerne. Hør nærmere om værkstedspakken og pris i Teknologirådets sekretariat.

Ballerup og Cyberspace. Konferenceoplæg med visioner og handlingsforslag til fremtidens bibliotek 2005 fra konferencen 3. juni 1996. 23 sider.
Bibliotek 2005 - 4 scenarier. Scenarier for fremtidens bibliotek og anvendelse af informationsteknologi. 23 sider.
Bibliotek 2005 - Introduktion til scenarieværksted. 16 sider.

Fremtidens bibliotek - Ballerup og Cyberspace. Rapport fra projektet Fremtidens bibliotek, med scenarier, Delfi-undersøgelse, visioner og handlingsforslag, slutdokument fra et elektronisk forsamlingshus. 1996. 87 sider. 85 kr. Best.nr. 176

Universel adgang - et spørgsmål om demokrati. Rapport fra Teknologirådets elektroniske forsamlingshus 11. sept. - 2. okt. 1995. Lars Qvortrup. 53 sider. 80 kr. Best. nr. 169

Magt og modeller. Om den stigende anvendelse af edb-modeller i de politiske beslutninger. 1995. 101 sider. 95 kr inkl. oplæg til konferencen 14/9-95. Best.nr. 164

Plastkort som borgerkort. Anvendelse af ic-kort teknologien til borgerkort. Steffen Stripp. 160 sider. 85 kr. Best.nr. 156

Dansk sprogteknologi - status, perspektiver og handlemuligheder. 1994. 141 sider. 70 kr. Best.nr. 154

Sprogteknologi. Udarbejdet på baggrund af rapporten Dansk sprogteknologi. 1994. 16 sider/ill. Best.nr. 154

Virtual Reality. Et ungdomspanels status over vr's muligheder og konsekvenser. 1994. 66 sider/ill. 139 kr. Købes i boghandlen.

Det er kort, men er det godt? Skal vi danskere have et privatkort? Claus Engelund. 1994. 20 sider/ill. Oplæg til konferencen 12. - 14. april 1994.

Landbrug/fiskeri

Visionen om økologisk landbrug - komparativ økonomiske analyse af fuld omlægning af dansk landbrug til økologisk drift. 1998.

Salmonella. Resumé og udskrift af høring i Folketinget den 11. november 1998.

Udledning af næringsstoffer til vandmiljøet. Resumé og udskrift af høring i Folketinget den 29. oktober 1997. 1997. 35 kr. Best. nr. 184.

Fremtidens fiskeri. Slutdokumenter og ekspertindlæg fra konsensuskonferencen 22.-25. november 1996. 1997. 167 sider. 95 kr. Best.nr. 177

Det lysegrønne landbrug. Slutdokument og ekspertoplæg fra konsensuskonferencen 23.-25. november 1994. 142 sider. 80 kr. Best.nr. 159

Miljø, industri og energi

Kemikaliestrategien, resumé og udskrift af høring i Folketinget den 12. maj 1999.

Miljøstyret affaldspolitik. Resumé og udskrift af høring i Folketinget den 29. september 1998.

Genanvendelse - oplæg til sporskifte i indsatsen på affaldsområdet. Rapport og anbefalinger fra en tværfaglig arbejdsgruppe. 1998.

Energisektoren under forandring - trusler og muligheder. Resumé og redigeret udskrift fra høring i Folketinget den 2. juni 1998. 1998. 150 sider.

Fremtidens forbrug og miljø. Slutdokument og ekspertindlæg fra konsensuskonferencen 1.-4. november 1996. 1997. 98 sider. 95 kr. Best.nr. 178

Hvilket forbrug vil vi ha'? - tre scenarier for fremtidens forbrug og miljø. Ida-Elisabeth Andersen, Thomas Breck og Peter Hesseldahl. Forbrugerrådet og Teknologirådet. 1996. 32 sider. 20 kr. Best.nr. 437

Debatpakke: Fremtidens forbrug og miljø - Teknologirådet støtter debatten. Med lister over oplægsholdere, litteratur m.m. samt ansøgningsskema.

The non-assessed chemicals in EU. Presentations from the conference 30. october 1996. 1997. pris ca. 95 kr.

The non-assessed chemicals in EU. Report and recommendations from an interdisciplinary group of Danish experts. 1996. 120 sider. 95 kr. Best.nr. 173

Uvurderede kemiske stoffer. Rapport og anbefalinger fra en tværfaglig arbejdsgruppe. 1996. 113 sider. 95 kr. Best.nr. 172

Ecological tax reform. Contributions and debate from the conference june 22, 1995. 1996. 114 sider. 95 kr. Best.nr. 174

Ecological tax-reform. 16-siders introduktion, udgivet som oplæg til konference om grønne skatter, juni 1995.

Hvor går grænsen. Kemiske stoffer i mad og miljø. Slutdokument og ekspertoplæg fra konsensuskonferencen 9.-12. juni 1995. 140 sider. 85 kr. Best.nr. 163

Fremtidens vedvarende energisystem - et lysegrønt og et mørkegrønt scenarie. 1994. 68 sider. 70 kr. Best.nr. 158

Biomasse til energiformål - et strategisk oplæg. 1994. 115 sider. 70 kr. Best.nr. 157

Registre og datasikkerhed

En dansk krypto-politik. Hvordan skal digitale informationer hemmeligholdes? Steffen Stripp (red.). 1995. 76 sider. 95 kr. Best.nr. 165

Elektroniske spor. Rapport fra et forprojekt. 1995. 32 sider. 70 kr. Best.nr. 162

Kommunen på nettet. Rapport fra projektet om elektronisk selvbetjening i det offentlige. Oktober 1999 - april 2000. 66 sider. 95 kroner. Best. nr. 208

Sundhedsvæsen
Prioritering af nye lægemidler. Resumé og redigeret udskrift af høring i Folketinget den 22. september 1999. Teknologirådets rapporter 1999/4

Telemedicin - En vej til et bedre sundhedsvæsen. Udarbejdet af en tværfaglig arbejdsgruppe. 1997. 56 sider. 85 kr. Best. nr. 183.

Genterapi. Hvad kan man, hvad vil vi? Slutdokument og ekspertoplæg fra konsensuskonferencen 21.-25. september 1995. 144 sider. 90 kr. Best.nr 167

Barnløshed. Slutdokument og ekspertoplæg fra konsensuskonferencen 29. oktober - 1. november 1993 på Christiansborg, arrangeret af Teknologinævnet i samarbejde med Folketingets Forskningsudvalg og Det Etiske Råd. 1994. 153 sider. 75 kr. Best. nr. 153

Handlingsplan for forebyggelse af overfølsomhed og allergiske sygdomme i Danmark 2001-2005. Udarbejdet af en tværfaglig arbejdsgruppe under Teknologirådet. November 2000. 42 sider.

Teknologivurdering og samfund
Farlig Teknologi - Miljøregulering ved samhandel med udviklingslande. Rapport og anbefalinger fra en uafhængig arbejdsgruppe under Teknologirådet. Teknologirådets rapporter 1999/5.

Teknologisk fremsyn i Danmark. Rapport og anbefalinger fra en uafhængig arbejdsgruppe. 1999.

Tid og Teknologi - indlæg i debatten om tid, teknologi og velfærd. En tidshjemmeside med debatindlæg, fra den elektroniske konference om tid og teknologi. Teknologirådet, 1999.

Viden og værdier i risikokommunikation - Oplæg fra arbejdsgruppen til workshop den 23. marts 1999. Teknologirådet, 1999.

Før teknologien løber løbsk - om lægfolks opfattelse af risiko - Diskursanalyse af 15 slutdokumenter fra teknologirådets konsensuskonferencer 1988 til 1997. Ursula Plesner, 1999

Samfund for alle - også for handicappede. Indlæg og debat fra Teknologirådets konference 5.-6. september 1995. 1996. 51 sider. 85 kr. Best.nr. 175

Femern og fremtiden. Oplæg og diskussion fra konferencen 23. maj 1995 om inddragelse af offentlighed og borgere i beslutningsprocessen. 1995. 69 sider. 85 kr. Best. nr. 168

Sport og teknologi. Cykling, sejlads, windsurfing, tennis, atletik. 1994. Teknologinævnet og Forlaget Thorup. 126 sider/ill. 198 kr. Købes i boghandlen

Støj. Slutdokument og ekspertindlæg fra konsensuskonference 12.-15. maj 2000. 170 sider. 95 kroner. Best. nr. 207

Trafik
Københavns Metro. Resumé og udskrift fra høring i Folketinget den 10. juni 1998. 1998.

På vej mod intelligent trafik. Slutdokument og ekspertoplæg fra Teknologinævnets konsensuskonference 28. - 31. oktober 1994.121 sider. 75 kr. Best. nr. 161

Bilismens fremtid. Slutdokument og scenarier fra konsensuskonferencen 11. - 14. juni 1993 på Christiansborg. 1993. 89 sider. 70 kr. Best.nr. 152

Andet
Teknologirådet 1998. En årsberetning. 1999. 57 sider.

Teknologirådet 1997. En årsberetning. 1998. 36 sider.

Oplægsguide. En guide over oplægsholdere inden for aktuelle emner.

Teknologirådet 1996. En årsberetning. 1997. 32 sider.

Ti år med Teknologinævnet. Samlet oversigt over Teknologinævnets virksomhed 1986-1995. Anne Funch Rohmann. 1996. 95 sider.

TeknologiDebat. TeknologiDebat er Teknologirådets blad. Det kommer seks gange om året, med nyhedshistorier, baggrund, reportage og debat, særlig i forbindelse med Rådets projekter. Pris 85 kr. pr. år.

Teknonyt. Teknonyt er Teknologirådets elektroniske nyhedsbrev. Nyhedsbrevet udkommer hver 14. dag og oplyser dig om Teknologirådets aktiviteter. Du kan abonnere på det gratis ved at sende en mail til Mette Bom (mbekno.dk).

December 2000