

Baggrundsmateriale til novellen ”Den chipløse mand”

Det følgende er udarbejdet til brug sammen med novellesamlingen ”Den chipløse mand og andre noveller om sex, magt og informationsteknologi” af Georg Strøm

Georg Strøm

12. december 2008

Jeg har haft svært ved at skrive baggrundsmateriale til denne novelle. Der er hele tiden kommet nyt om registrering og spredning af personlige oplysninger.

I foråret 2008 annoncerede Bispebjerg Hospital at man ville starte en fjernovervågning af hjertepatienter. Ganske vist over mobiltelefoner, men ellers som i baggrunden for novellen. Det var endda en af de mere usandsynlige forudsigelser.

Samtidig er brugen af chips til fjernaflæsning vokset kraftigt. Der er kommet flere mulige anvendelser som ligner dem jeg beskriver i novellen.

Der er i øvrigt også kommet biler med automatisk parkering som forudset i novellen.

Det eneste punkt, hvor novellen delvist går forkert, er at den ikke omtaler den mængde af oplysninger om forskellige personer som allerede er offentligt tilgængelige. På den anden side foregår novellen ude på landet og langt væk fra de store informationsstrømme. Så er det naturligt at den kun beskriver de sidste udløbere af de mængder af informationer som ligger tilgængelige om det enkelte menneske.

Overvågningskameraer

Georg Orwells roman 1984 er blevet et billede på overvågningssamfundet, og hvordan det tvinger det enkelte menneske til at undertrykke sine egne tanker. I den roman er overvågningskameraer den vigtigste form for teknologi. Årsagen er nok, at da romanen blev skrevet i 1948, var kameraer den mest avancerede form for elektronisk overvågning man kunne forestille sig.

I virkeligheden er kameraer en meget ineffektiv form for overvågning. Det er svært at behandle optagelserne elektronisk, og det tager tid for mennesker at se dem igennem.

Det kan være svært at identificere de personer som er på optagelserne, og det bliver ikke bedre af at det er vanskeligt at sætte kameraer op og indstille dem, så de giver tydelige billeder. Endelig kan kameraerne normalt ikke give et indtryk af hvad folk tænker på. Selv Orwell lægger ikke skjul på at det er vanskeligt.

Det kan føles ubehageligt, at blive optaget på video, eller at der måske sidder en vagtmand et andet sted og ser hvad man foretager sig, men den følelse ser ud til at aftage, efterhånden som vi vænner os til at der er kameraer flere offentlige steder. Til gengæld lader det ikke til at kameraer forhindrer forbrydelser. De kan højst hjælpe til at finde dem der har lavet forbrydelser og til at levere beviser mod dem.

Registerloven og samkøring

I halvfjerdserne da mange firmaer indførte EDB – Elektronisk Data Behandling som det hed dengang – var der en del diskussion af om private firmaer ville samle og misbruge personlige oplysninger. Derfor fik man Registerloven.

Der var ingen begrænsninger på registreringen af oplysninger som allerede var offentligt tilgængelige, som for eksempel indlæg i aviser. Desuden kunne et firma få lov til at registrere folks helbred, sociale problemer og andre følsomme oplysninger, hvis folk havde givet deres tilladelse, og hvis firmaet behøvede oplysningerne.

Undtagelserne i loven er et problem. Det kan for eksempel være umuligt at få en forsikring, hvis man ikke vil skrive under på at forsikringsselskabet må hente oplysninger om ens helbred.

I dag er det imidlertid et større problem, at det teknisk er blevet let at lave noget som går ud over rammerne i registerloven, så myndighederne langt fra kan stoppe alle

som gør det. For eksempel kræver det en tilladelse før man må lave et register som advarer mod bestemte firmaer. Det nytter dog ikke så meget, når det er nærmest umuligt at stoppe indlæg på diskussionsfora hvor kunder advarer mod firmaer de har været oppe at toppes med.

I halvfjerdsere var der også en udbredt frygt for samkøring. Altså for at forskellige offentlige myndigheder kombinerede deres oplysninger. Årsagen var nok en generel nervøsitet for at forholdet mellem myndigheder og borgere blev for ulige, hvis den enkelte sagsbehandler – eller endda klasselærer – kunne sidde med alle oplysninger om en familie eller en person.

Imidlertid kan myndigheder i følge Persondataloven få tilladelse til at lave samkøring, hvis oplysningerne er nødvendige for at træffe en afgørelse, eller hvis myndighederne mener “den sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.” Samkøring kan altså tillades, når en myndighed kan argumentere for at den har brug for det.

Et eksempel var en samkøring af registre for skat og dagpenge, så man kunne finde frem til personer som fik understøttelse selv om de faktisk havde arbejde. Et senere eksempel var en såkaldt portal så den daværende udlændingestyrelse hurtigt kunne få at vide fra en kommune, hvis en udenlandsk kvinde var flyttet fra sin mand og derfor i følge reglerne skulle udvises.

De fleste er nok enige om, at det er en god ide at samkøre registre, hvis det kan afsløre svindel. Det forudsætter bare at registrene giver de rigtige oplysninger, eller at myndighederne ikke bare stoler på samkøringerne, men tager sig tid til at undersøge hver enkelt sag. Det kan være at en person er kommet i arbejde midt i en måned, så samkøringen derfor viser at han eller hun både har arbejdet og fået dagpenge i samme måned. Jeg har desværre set et eksempel på at registre ikke kunne håndtere sådanne ændringer midt i en måned.

Nogle gange kan det også være en fordel hvis systemerne ikke hænger alt for tæt sammen. Et eksempel er

Udlændingestyrelsens portal. En udenlandsk kvinde kan i følge reglerne faktisk have lov til at blive i Danmark, men alligevel blive udvist før hun finder ud af sine rettigheder og får søgt om at blive.

I dag er reglerne om samkøring også ved at være uaktuelle. For tredive år siden lå oplysningerne i adskilte registre, som det var svært at kombinere. I dag ligger oplysningerne i databaser, hvor det kan være svært at forhindre at de bliver kombineret. Samtidig kan en myndighed have svært ved at nægte en anden myndighed adgang til dens oplysninger. Derfor må vi i dag gå ud fra at de forskellige myndigheder kan kombinere alle oplysninger på kryds og tværs, når de kan se en grund til det.

Internettet og offentligt tilgængelige oplysninger

De forskellige offentlige myndigheder gemmer flere oplysninger end nogen sinde før, og vi er i Danmark nok det mest gennemregistrerede land i verden. Alligevel er denne organiserede offentlige registrering måske det mindste problem. Der er nogle begrænsninger på hvem der må se de forskellige oplysninger, der er en vis kontrol med de oplysninger som bliver registreret, og der er krav om at nogle oplysninger skal slettes efter et vist antal år.

Det gælder ikke for oplysninger på internettet. Infomedia er en database som indeholder de fleste artikler og læserbreve som er skrevet i danske aviser. Jeg ved at den indeholder en artikel som jeg selv skrev for fjorten år siden. Den er en fantastisk hjælp når man skal finde oplysninger om nutidige begivenheder. Det har været omtalt at firmaer bruger den til at checke hvad en journalist tidligere har skrevet, før de siger ja eller nej til at deres direktør stiller op til et interview. Kritiske journalister kan altså blive udelukket på forhånd. Det har også været fremme at Dansk Folkeparti har brugt Infomedia til at undersøge om dem der søger om medlemskab har skrevet læserbreve som strider mod partiets politik.

Google giver tilsvarende muligheder. Jeg kender selv til studerende som søger oplysninger på censor før en eksamen, så de ved hvad han eller hun er specielt

interesseret i og kan læse op på det. Det er også mit indtryk at studerende som bruger oplysningerne uden at skilte med dem, godt kan have fordel af det.

Virksomheder kan opleve at konkurrenter og journalister finder nogle af deres hemmeligheder gennem Google. Jeg har selv set flere eksempler på præsentationer som var mærket "confidential" eller "Internal use only" som dukkede op da jeg søgte på Google. Selv om virksomhederne mente at de havde gemt deres fortrolige oplysninger hvor ingen kunne finde dem, kunne de alligevel findes gennem Google.

Aviserne omtalte et mere ekstremt eksempel i efteråret 2008. Læger havde nogle gange indsat oplysninger om patienter direkte fra regneark i deres præsentationer. Det viste sig så, at ikke bare oplysninger om sygdomme og behandling kom med, men også oplysninger om patienternes navne og cpr-numre. De oplysninger kunne ikke ses når præsentationen blev vist, men de kunne findes i de elektroniske kopier af præsentationen som var lagt ud på nettet.

Med internet 2.0 er udviklingen gået et skridt videre. Udtrykket dækker over at brugere selv lægger materiale op på internettet, for eksempel på YouTube eller på Facebook. Med Google og Infomedia har den enkelte person trods alt nogen kontrol over hvad han eller hun selv har skrevet og andre kan læse. Med internet 2.0 kan andre skrive om personer de kender eller tage billeder eller videoklip og lægge dem op. Samtidig er det i dag muligt at lave optagelser med en mobiltelefon uden at andre lægger mærke til det.

Et af de omtalte tilfælde var en arrangement på Silkeborg Gymnasium som løb af sporet i 2007. Ved et arrangement var der en gruppe piger som smed det meste af tøjet og dansede rundt i trusser og brystholder. Det ville tidligere have ført til en samtale på rektors kontor. Nu blev det optaget af en elev som bagefter lagde et klip ud på Youtube. Pludselig var der en uddannelsespolitisk ordfører som reagerede, og optagelsen blev endda diskuteret i udlandet. Det var svært at undgå når klippet lå på YouTube.

Optagelsen blev fjernet fra YouTube, men der var allerede lavet kopier som stadig

ligger andre steder på internettet. Hvis noget er tilstrækkeligt opsigtsvækkende, er det nærmest umuligt at fjerne når det først er lagt ud på internettet, og det kan som regel findes gennem Google.

I dag må vi regne med at vores egne dumheder ved private arrangementer kan komme ud på internettet, hvor de kan ses af venner, kæresten eller der hvor vi søger arbejde om fem eller ti år.

De kan endda holde langt længere. Det har for nylig været fremme at Det Kongelige Bibliotek regelmæssigt høster danske web-sider, også profiler på kontaktsider som er beskyttet med password. Indholdet på disse sider vil blive offentligt tilgængelige halvfjerds år efter at forfatteren er død. Dem der har brugt dating-sider kan altså tænke på at det de har skrevet i en sen natstid kan være det billede af dem selv som går over i historien.

Det positive er at videooptagelser kan forhindre eller opklare forbrydelser. Der har været forbløffende mange tilfælde hvor folk som har overtrådt loven selv har filmet hvad de har lavet. Et eksempel var en ung mand som lagde en optagelse ud som viste at han groft havde overtrådt hastighedsgrænsen med sin motorcykel.

Der har været flere eksempler hvor overgreb fra politi og andre er blevet dokumenteret og lagt ud på internettet. Et aktuelt eksempel er en ung mand som for få dage siden blev mishandlet af en vagt i Hundige storcenter. Tidligere ville det være vanskeligt at få dømt vagten, når det var hans ord med den unge mands. Nu gør optagelsen det vanskeligt at undgå en retssag.

Automatisk opsamling af oplysninger

De forskellige systemer som vi benytter os af, lagrer automatisk store mængder information om os. Nogle gange som en bivirkning af deres funktion, og sådan at de ansvarlige nogle gange helst vil være fri for informationen.

Der var et eksempel med en pengeautomat i England helt tilbage i firserne. Den var installeret i den bydel hvor prostituerede hang på gadehjørnerne, og banken blev opmærksom på at der havde været en hel del mænd som havde hævet det samme

runde beløb sent om aftenen. Banken fandt med andre ord ud af, at den havde fået en liste over mænd som sandsynligvis havde besøgt prostituerede.

Da man lavede Dankort-systemet var et af kravene at det skulle være umuligt at kombinere oplysningerne så man kunne se hvad den enkelte person brugte sine penge på. Da Dankort-systemet kom frem i firserne, var det også svært at lave et system hvor man kunne kombinere oplysningerne. Til gengæld er det i dag ved handel på internettet nødvendigt at have oplysninger om hvad den enkelte person har købt. Ellers er det umuligt at håndtere klager og byttere. Når man så har oplysningerne, er det indlysende at bruge dem til at finde varer som den samme kunde måske er interesseret i. Nogle gange kan det være gode forslag, andre gange kan det føles som manipulation, og nogle gange kan det føre til ubehagelige afsløringer, når andre ser de anbefalinger som en internet butik sender.

Systemet til mobiltelefoner gemmer automatisk information om de sendemaster som en telefon har været i kontakt med. Inde i byerne er det derfor muligt at bestemme hvor en mobiltelefon har været henne på et bestemt tidspunkt med under 100 meters nøjagtighed. Det er ikke engang tilstrækkeligt at der har været talt i telefonen eller ringet fra den. Når en mobiltelefon bevæger sig fra et område til et andet, skal systemet have nye oplysninger om dens position, og de bliver også registreret.

Blandt andet i PFA sagen var et af de afgørende beviser oplysninger som viste hvor de anklagede havde brugt deres mobiltelefoner henne og hvornår.

Oplysninger fra mobiltelefoner kan også bruges til at finde vidner til en forbrydelse. Der kan være folk som er bange for at vidne, og der kan gymnasieelever som ikke har lyst til at deres forældre skal få at vide hvor de har været henne. Her kan politiet nu få oplysninger om samtlige telefoner der har været i kontakt med en bestemt sendemast, og bruge dem til at finde ud af hvem der har været i nærheden, da der blev begået en forbrydelse.

Det sidste nye indenfor indsamling af oplysninger hedder RFID. Det står for Radio

Frequency Identification. Attså identifikation på afstand ved hjælp af radiobølger.

En anvendelse er i identitetskort. Fordelen er at man ikke skal køre kortet gennem en scanner men blot holde det hen i nærheden, eller endda bare gå forbi. Hvis kortet kan aflæses på længere afstand, vil der endda være mulighed for at fjernaflæse det, så man kan følge hvem der går op på perronen på en togstation, eller ind på gågaden. Man kan endda forestille sig at politiet får scannere og ret til at stoppe folk som ikke har deres ID-kort på sig.

RFID chips falder kraftigt i pris. Det betyder at de kan blive brugt til mærkning af dyre varer, ligesom en tyverisikring. Når de kan aflæses på afstand, bliver det samtidig muligt for forretningen at følge den enkelte kunde rundt, og registrere hvor han eller hun stopper op. Blot ved at følge chipsene på de varer som ligger i kurven.

RFID chips kan laves stadig mindre. Det er muligt at indlægge chip på en millimeter på hver led i en pengeseddel med dens nummer, så det bliver nærmest umuligt at forfalske sedlen. Det betyder også at det bliver muligt at følge den enkelte pengeseddel, når forretninger og banker læser chippen for at kontrollere om sedlen er ægte.

Grænsen for hvad vi accepterer

Der er to yderpunkter når det gælder beskyttelsen af private oplysninger. Tilhængerne af det ene yderpunkt kan ikke se noget problem, så længe man ikke har gjort noget forkert. Tilhængerne af det andet yderpunkt kan ikke acceptere at dybt personlige oplysninger om dem selv ligger spredt et utal af forskellige steder hvor de ikke selv har kontrol over hvordan de anvendes.

Vi er nødt til at se begge holdninger i sammenhæng.

Den amerikanske forsker Lawrence Lessig beskriver hvordan noget bliver mere moralsk acceptabelt, når teknikken gør det lettere at gøre det. Et eksempel er ansatte på et kontors ret til privatliv. Traditionelt har ledelsen ikke haft lov til at registrere hvem de ringede til fra telefonen på deres skrivebord. I et gammeldags telefonsystem

var det også vanskeligt at gøre. I dag vil computersystemet automatisk registrere hvis en ansat har sendt en privat e-mail og hvilke hjemmesider han eller hun har besøgt i arbejdstiden. Samtidig har ledelsen fået ret til at se på oplysningerne. De skal blot have klare regler om hvornår de gør det.

Når noget bliver teknisk enklere, så flytter den moralske grænse sig altså, så vi synes det er mere acceptabelt.

Samtidig afhænger den enkeltes modvilje mod at få spredt sine private oplysninger af de konsekvenser som han eller hun forventer.

Det er praktisk at Amazon kan gøre opmærksom på bøger som er interessante for en selv, men som man ellers aldrig ville høre om. Også selv om de gemmer personlige oplysninger om ens interesser. Andre gange er det besværligt at forhindre lagring og brug af private oplysninger. Man skal undgå en række forretninger og services, og selv begrænse ens egen frihed til at gøre bestemte ting, hvis man vil undgå at det bliver registeret oplysninger om en selv.

Hvis man ikke ved hvilke oplysninger der ligger hvor henne, så er det selvfølgelig naturligt at ville være på den sikre side og begrænse spredning af private oplysninger mindst muligt.

På den anden side, vil dem der lægger oplysninger om dem selv og deres privatliv ud på internettet godt have at andre ser oplysningerne. Det er hele ideen med at lægge oplysningerne ud.

Da George Orwell skrev romanen 1984 mens Stalin regerede i Sovjetunionen, og i efterdønningerne af den kontrol som der havde været af det engelske samfund under den Anden Verdenskrig. Det var

baggrunden for hans Big Brother som holdt øje med den enkelte.

I dag er der nogen som bruger udtrykket Big Mother om den registrering der foregår. Vi er på mange måder vant til at det offentlige passer på os. De fleste har tillid til myndighederne, og vil derfor gå fra at myndighederne overvåger og registrerer for at passe på os.

Der gælder noget andet for oplysninger som bliver spredt til den store offentlighed. Vi vil ikke have indskrænket vores ytringsfrihed og måske især ikke vores muligheder for at få noget at vide om andre. Det vejer tungt i forhold til beskyttelsen af den enkelte persons privatliv.

Samtidig rammer problemerne kun enkelte personer, lidt ligesom det er de færreste som bliver ofre for trafikuheld.

Endelig er der i dag så mange oplysninger, at vi måske ikke længere skal nøjes med at diskutere retten til at beskytte vores privatliv. Måske skal vi også - lige som i novellen - kræve at vi kan slippe for at få noget at vide som kan være for ubehageligt, eller for ødelæggende for vores forhold til et andet menneske.

Litteratur

Lawrence Lessig: Code and other laws of cyberspace. Basic Books 1999