Kan siteres som:
Hannemyr, G. (2002) *Foucault i kyberrommet,* I: Digital Makt, (Red., Tore Slaatta) Gyldendal Akademisk, Oslo, pp. 41-63.

Kapittel 2

Gisle Hannemyr

FOUCAULT I KYBERROMMET

Forbrukerrettigheter og teknologiskesperrer i vår digitale hverdag

For tiden skjer det en endring i maktforholdene mellom forbrukere, næringsliv og myndigheter. Årsaken til endringen er de muligheter, begrensninger, egenskaper og føringer som, enten gjennom design eller som en bivirkning, er bakt inn i det utall av nye reproduksjonsteknikker, distribusjonsformer og transaksjonsprosesser som preger medie- og forretningslandskapet i det tidlige 21. århundre. Effekten av disse endringene forsterkes av den omstendighet at mange av oss opplever at en stadig større deler av vår hverdag og vår livsverden veves inn den komplekse veven av digitale teknologier som det ofte refereres til med besvergelsen «konvergens».

Midt i dette endringslandskapet finner vi den konflikten som utspiller seg mellom de såkalte hackere, på den ene siden, og innholdsindustrien og myndighetene på den andre. Vi skal se nærmere på denne konflikten og om hvilke implikasjoner utfallet av den vil ha.

Konfrontasjoner

I januar år 2000 slår norske Økokrim til mot Jon Lech Johansen, en 16 år gammel dataentusiast og skoleelev i fra Lardal i Vestfold. Bakgrunnen for politiets aksjon er en anmeldelse fra flere amerikanske og japanske filmdistributører, der unggutten blir anklaget for å ha utviklet, og deretter spredt via Internett, et datamaskinprogram, *DeCSS,* som gjør det mulig å hente fram krypterte data lagret på DVD (Digital Video Disc) slik at innholdet på disse platene (vanligvis spillefilmer) lot seg vise på annet utstyr enn det som på forhånd var godkjent av organisasjonen DVD-CCA (Content Control Association). For dette er han tiltalt for datainnbrudd etter straffelovens §145 (2. ledd), med en strafferamme på inntil to års fengsel.

I mars 2000 klarer svenske Eddy Jansson og kanadieren Matthew Skala å knekke kodene som beskytter de såkalte sperrelistene som er «motoren» i programmet Cyber-Patrol. CyberPatrol er et program som skal hindre barn som surfer på Internett i å komme i kontakt med pornografi. Dette skjer ved at alle nettsider som sperrelistene peker ut blir sperret for visning. Men studerer man disse listene, blir det raskt åpenbart at programmet er konstruert for å sperre for mye mer enn pornografi. Materiale om fagbevegelsen, venstreorienterte politiske sider og sider som inneholder kritikk av bruk av slike programmer som CyberPatrol blir også luket ut. Begge får raskt besøk av

industriens advokater. Etter å ha møtt foran en dommer og gjort gjenstand for en midlertidig forføyning og deretter truet med en større erstatningssak, velger begge å inngå et forlik. Ifølge forliket skal de to slippe ytterligere rettslig forfølgelse i bytte mot å overdra alle rettigheter til programmet som knekker kodene, *CPHack*, til leketøysprodusenten Mattel, som eier CyberPatrol. Dette juridiske grepet gjør det mulig for Mattel å forfølge enhver distributør av *CPHack* for opphavsrettsbrudd.

I april 2001 får Edward W. Felten, professor ved Princeton University og ekspert på datasikkerhet og kryptografi, brev fra den amerikanske musikkindustriens advokater. Brevet advarer ham mot å publisere et notat der han blant annet drøfter et kryptografisk system som musikkindustrien har utviklet. Brevet gir Felten beskjed om at han dersom på noe vis offentliggjør resultatene fra sin forskning omkring dette systemet, risikerer han å bli forfulgt rettslig med hjemmel i den såkalte *Digital Millenium Copyright Act* (DMCA). DMCA trådte i kraft i USA på tampen av år 2000, og er en lov som blant annet gjør det til en forbrytelse i USA å drøfte offentlig virkemåten til teknologi konstruert for å beskytte intellektuell eiendom. Professor Felten tar trusselen fra musikkindustrien alvorlig, og trekker sitt notat tilbake fra den vitenskapelige konferansen han er invitert til.

Dmitri Sklyarov, en 27 år gammel russisk programmerer, er mindre forsiktig. I midten av juli 2001 takker han ja til å delta å en konferanse i Las Vegas for å presentere det han har funnet ut om dataformatet som det amerikanske programvarehuset Adobe benytter for å beskytte elektroniske bøker mot uautorisert bruk. Like etter blir Sklyarov pågrepet av det amerikanske føderale politiet FBI for å ha forbrutt seg mot DMCA. Paradoksalt nok ønsker ikke den angivelig fornærmede part i saken, Adobe, å straffe Sklyarov. I en kort kommentar sier Adobe at det «ikke kan se at de involverte parter eller programvareindustrien er tjent med en rettslig forfølgelse av hr. Sklyarov». Sklyarov blir likevel fengslet. I desember 2001 blir likevel tiltalen mot ham frafalt, på det vilkår at han vitner i en amerikansk rettsak mot sin arbeidsgiver, det Moskva-baserte programvareselskapet ElcomSoft. ElcomSoft er fortsatt tiltalt i USA for brudd på DMCA.

Alle disse historiene handler om *makt*. På overflaten ser vi at tradisjonelle maktoperatører som politiet og rettsapparatet settes i sving for å disiplinere adferden til de involverte personer. Men den *kunnskapen* disse personene har innebærer også makt til å ødelegge bestemte anvendelser av teknologi. Til sist: Også de proprietære dataformatene[1] er en form for maktutøvelse. Gjennom slike formater kan nemlig selskapene bak dem kartlegge sine kunders adferd, kontrollere i detalj hvordan produktene benyttes av kundene, sperre konkurrenter ute fra sentrale distribusjonskanaler, erobre eierskap over markeder og endog sensurere ytringer. Bruken av proprietære dataformater føyer seg derfor pent inn den lange rekken av maktutøvelser som står til rådighet for selskaper og regjeringer gjennom deres kontroll over ting og teknologier.

Mikromakt

Ingen har skildret dette spillet mellom makt og kunnskap (fransk: *pouvoir et savoir*) bedre enn Michel Foucault.

[1] Dvs. måter og kode og lagre data på som eies og kontrolleres av et privat selskap.

Tradisjonell sosial teori betrakter gjerne makt som en egenskap som er institusjonalisert i form av et asymmetrisk makt/avmakts-forhold (hersker/slave, overordnet/underordnet, lærer/elev). Den ene part *besitter* makt, den andre gjør det ikke.

Foucault er kritisk til denne forståelsen av makt. Forestillingen om at en person (eller institusjon) tar makten i besittelse og at makt deretter hefter ved vedkommende som en egenskap er både for begrenset og for statisk. Den institusjonaliserte makt eksisterer riktignok i form av de maktrelasjoner som for eksempel er fasttømret i lovverket og i en del samfunnsinstitusjoner, men for Foucault er det langt mer interessant å analysere det han kaller for *disiplinerende makt*, slik den «utøves av politiske teknologier gjennom samfunnslegemet» (Foucault 1982).

Disiplinerende makt karakteriseres blant annet ved at den *utøves* snarere enn besittes, er *implisitt* snarere enn eksplisitt, er gjenstand for *endring* snarere enn uforanderlig, og er *distribuert* i et nett av aktører snarere enn befestet i en bestemt relasjon. Foucault poengterer videre at maktutøvelse ikke utelukkende fungerer hemmende og begrensende. Mange av modernitetens manifestasjoner (det vil si fenomener som skoler, sykehus, fengsler, fabrikker og storbyer) er ifølge Foucault *skapt* ved en prosess der makt gjennom sosiotekniske konfrontasjoner oversettes og omdannes til fysiske gjenstander og måter å organisere rommet på (Foucault 1977, Foucault 1980).

For å forstå denne formen for makt må vi rette vår analyse mot maktens materielle operatorer, dvs. de maskiner og mekanismer, de strategier og taktikker som benyttes til å dominere. Foucault bruker betegnelsen «mikromakt» på disse individuelle utøvelsene av dominans. Snarere enn en kamp langs fast opptrukne fronter, sier han, er utøvelsene av mikromakt fragmentert og definerer derfor «utallige konfrontasjonspunkter». Og i motsetning til de store slag blir slike episoder ikke skrevet inn i historiebøkene. I stedet gjør de seg gjeldende gjennom de effekter de induserer i de nett av aktører som de er en del av. Til sist bør det bemerkes at slike episoder sjelden er innbyrdes koordinerte, og at de heller ikke nødvendigvis er uttrykk for, eller formuleringer av, bevisste strategier for makt eller motmakt (Foucault 1977. s. 26f).

Hackere

Edward Felten, Dmitri Sklyarov, Jan Lech Johansen, Eddy Jansson og Matthew Skala tilhører alle en løst sammensatt internasjonal bevegelse som i media blir identifisert under etiketter som *tilhengere av fri programvare, bevegelsen for åpen kildekode* eller rett og slett *hackere*. Nedenfor brukes betegnelsen *hacker*, både fordi det er den opprinnelige, og fordi begrepet brukes ute av kontekst såpass ofte at det kan være på tide å presentere det i den rette historiske og politiske sammenheng.

Opprinnelig er *hacker* rett og slett en betegnelse som særdeles gode programmerere brukte om hverandre – en spøkefull hederstittel datafolk imellom (ordet *hacker* på engelsk betydde opprinnelig «en som lager møbler med øks»). I tråd med den økende politiseringen av ungdomskullene som finner sted på 1970-tallet øker også det politiske engasjementet blant hackerne. Det kommer blant annet til uttrykk gjennom prosjekter som *Community Memory* og *People's Computer Company*, der hackere gir skoleelever og andre ikke-fagfolk tilgang til, og opplæring i, bruk av datamaskiner gjennom terminaler utplassert på biblioteker og bydelshus. Verbalt kommer hackerbevegelsen til orde gjennom en bok som gis ut av en av de toneangivende personlighetene i miljøet, Theodore Holm Nelson, i 1974.

Nelsons bok er i samme format som hippiebevegelsen «bibel», *The Whole Earth Catalogue*[2]: 27x34 cm. Typografisk minner den også om sitt forbilde. Sidene flommer over av tekst og illustrasjoner, delt opp i smale spalter med håndtegnede overskrifter og med et innhold som spenner fra filosofi og politiske manifester til håndfaste fakta-artikler og praktiske veivisere i bruk av datateknologi og programmering. Ved nærmere ettersyn viser det seg dessuten at det dreier seg om to bøker. Den ene «forsiden» bærer tittelen *Computer Lib* og viser en tegning av en gigantisk knyttneve foran en datamaskin. Snur man boken viser det seg at «baksiden» er en ny «forside». Denne bærer tittelen *Dream Machines*.

At *Dream Machines* ledsager *Computer Lib* er ikke tilfeldig. Mens *Computer Lib* beskriver Nelsons framtidsvisjon av hvordan datamaskiner kan brukes som medium for kreativt uttrykk i et samfunn der all informasjon er åpent tilgjengelig og kan deles mellom likemenn, forsøker han i *Dream Machines* å gi en detaljert og i all hovedsak teknisk beskrivelse av hvordan han ser for seg denne utopien realisert.

I forordet til *Computer Lib* erklærer Nelson sin politiske visjon slik:

> I have an axe to grind: I want to see computers useful to individuals, and the sooner the better, without necessary complication or human servility being required. […]
>
> THIS BOOK IS FOR PERSONAL FREEDOM
> AND AGAINST RESTRICTION AND COERCION
> A chant you can take to the streets:
> COMPUTER POWER TO THE PEOPLE
>
> (Nelson 1974)

Kjernen i *Dream Machines* er at man må konstruere datamaskinene slik at enhver datamaskin kan knyttes sammen med enhver annen datamaskin, og denne sammen-knytningen må være noe *mer* enn en fysisk eller elektrisk forbindelse som muliggjør transport av data. Nelson foreslår at *informasjonen* på de ulike maskinene skal være lenket sammen på en slik måte at brukerne til enhver tid kan lese den informasjonen som befinner seg på andre brukeres maskiner bare ved å følge «lenker» som han ser for seg skal knytte informasjonselementene sammen. Systemet er dessuten konstruert slik at informasjon lar seg kopiere mellom de ulike systemene, og disse kopiene skal kunne modifiseres og tilpasses lokale formål. Allerede ti år tidligere har Ted Nelson lansert begrepet «hypertekst» som betegnelse for denne måten å lenke sammen informasjon på (Nelson 1965).

Nelson har så langt ikke lykkes med å realisere et fungerende hypertekst-system. Det har imidlertid engelskmannen Tim Berners-Lee, som inspirert av blant annet *Dream Machines* på begynnelsen av 1990-tallet skaper det som vi dag kjenner som World Wide Web. I tråd med hackertradisjonen er teknologien som ligger bak World Wide Web ikke patentert eller beskyttet på annet vis. Det er heller ikke lagt andre restriksjoner på bruk av World Wide Web. Og de dataformat som gjennom World Wide Web muliggjør datautveksling mellom millioner av mennesker verden over: HTTP (Hyper Text Transfer Protocol), HTML (Hyper Text Markup Language) og XML (eXtensible Markup Language), er fullstendig åpne og fritt tilgjengelige for alle som måtte ønske å ta dem i bruk.

[2] Utgitt av tusenkunstneren Stuart Brand, som også i november 1984 organiserte den første hacker-konferansen.

Ti år etter publiseringen av *Computer Lib/Dream Machines* dukker ett nytt skriftstykke opp i hackermiljøet. Forfatter er Richard M. Stallman, en ung programmerer som akkurat hadde sagt opp stillingen sin på laboratoriet for kunstig intelligens ved Massachusetts Instititute of Technology (MIT) i protest mot at han var blitt bedt om å skrive under på et såkalt «nondisclosure agreement» – en avtale der han forpliktet seg til ikke å dele sin kunnskap om virkemåten til bestemte dataprogrammer med andre.

I en artikkel med den kryptiske overskriften *The GNU Manifesto* begrunner han sin avskjed med det presisjefylte laboratoriet slik:

> I consider that the golden rule requires that if I like a program I must share it with other people who like it. Software sellers want to divide the users and conquer them, making each user agree not to share with others. I refuse to break solidarity with other users in this way. I cannot in good conscience sign a nondisclosure agreement or a software license agreement. For years I worked within the Artificial Intelligence Lab to resist such tendencies and other inhospitalities, but eventually they had gone too far: I could not remain in an institution where such things are done for me against my will. (Stallman 1985)

Videre lanserer Stallman det prosjektet som har gitt manifestet navn: «GNU» er et akronym dannet fra forbokstavene i setningen «Gnu's Not Unix». Det er navnet på et fullstendig åpent datasystem som Stallman akter å utvikle.

> So that I can continue to use computers without dishonor, I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free. I have resigned from the AI Lab to deny MIT any legal excuse to prevent me from giving GNU away. (ibid.)

GNU er et avansert datasystem av samme type som Unix, men i stedet for at et tradisjonelt programvareselskap står bak utviklingen blir systemet implementert og vedlikeholdt av frivillige over hele verden. Dermed kan GNU distribueres fritt til alle som ønsker å ta det i bruk. Men like viktig som at produktet er gratis, er prinsippet om at systemet skulle være åpent. Ingen hemmelige eller proprietære dataformater brukes i GNU-systemet. Dermed er det også umulig å legge restriksjoner på hvordan de ideer som var nedfelt i systemet benyttes, enten disse finnes i form av programkoder eller i form av dataformater.

Ved første øyekast framtrer GNU som en slags oppvisning i hippieinspirert selvforsyningsøkonomi, men Stallman sikter langt høyere. Som programmerer i det kreative miljøet ved MIT AI Lab på 1970 og -80-tallet oppdaget Stallman at å skape ideer (og dataprogrammer er ikke noe annet enn ideer kodet i matematisk form) er en kollektiv prosess som har mange arbeidsmåter og praksiser til felles med fri forskning. Men en slik arbeidsform som den kommersielle delen av dataindustrien lite tilfreds med, fordi den gir industrien liten kontroll over programmerene qua arbeidere – og enda mindre kontroll over den merverdi som arbeidet deres skaper. Industrien forsøker derfor å bryte opp denne måten å arbeide på, og erstatte den med arbeidsformer som innebærer større grad av kontroll. Et av virkemidlene er bruksbegrensninger, proprietære formater og non-disclosure-avtaler som gjør det vanskelig for programmere å samarbeide på tvers av selskapsgrenser og ulovlig for dem å dele enkelte ideer med andre.

Det Stallman i realiteten forsøker å få til gjennom GNU, er å sabotere denne utviklingen innen programvarebransjen. Hans egentlige prosjekt er åpenbart å skape en nisje for

utvikling av datasystemer der kontrollen ligger hos programmerene og dem som bruker programvare, og ikke hos aksjonærene i de store programvareselskapene.

Stallmans fremste virkemiddel i dette prosjektet er en konstruksjon som går under navnet *GNU Public License* (GPL). Denne spesielle lisensavtalen går ut på at programvare som er underlagt GPL kan brukes, endres, kopieres og formidles videre til tredjepart, men at den som gjør dette ikke kan knytte bestemmelser, betingelser eller dataformater til produktet som begrenser mottakerens rettigheter i forhold til den opprinnelige lisensen.

I tillegg til å verne om brukerens rettigheter er det i GPL innbakt konstruksjoner som tar sikte på å verne prosjektets integritet. For eksempel er det tatt med en egen klausul som slår fast at GPL automatisk også omfatter avledede konstruksjoner. Dette er en elegant forsikring mot at GNUs integritet ødelegges ved at basisproduktet tilføres proprietære *tillegg*. Å ødelegge og erobre kontrollen over åpne standarder og formater gjennom proprietære utvidelser er en så vanlig strategi i programvarebransjen at den har fått et eget navn: *omfavn og utvid* (engelsk: *embrace and extend*). GPL har så langt vist seg motstandsdyktig mot denne type angrep, noe som later til å ha irritert Microsoft i oppsiktsvekkende grad. Lederen for Microsofts operativsystemavdeling, Jim Allchin, har gått såpass langt som å karakterisere GPL som u-amerikansk, en trussel mot programvareindustrien og en fare for næringslivet. Han uttaler videre at det snart er på tide at amerikanske lovgivere forstår hva denne trusselen innebærer (Cnet 2001, Pahati 2001).

På samme måte som Ted Nelsons visjon om informasjonsutveksling i dag finnes realisert i form av World Wide Web, er Stallmans visjon om et helt åpent datasystem realisert i form av det systemet de fleste kjenner under navnet *Linux*. Linux består av en Unix-lignende operativsystemkjerne utviklet av den unge finske programmereren Linus Torvalds, og tilhørende utviklingsverktøy, systemomgivelser og en lang rekke nytte-programmer utviklet av Stallman selv og entusiaster over hele verden.

En kuriøs, men like fullt interessant parallell til hackerbevegelsens motstand mot proprietære dataformater er de britiske ludditenes opprør mot maskinteknologi i begynnelsen av det 19. århundre.

Ludditene observerte hvordan den begynnende industrialisering førte til at menn, kvinner, og i enkelte tilfelle også barn, ble stuet sammen i mørke fabrikkbygninger der de måtte underkaste seg en organisering av arbeidet som i all hovedsak fant sted på maskinenes premisser. Ludditene reagerte med å ødelegge maskinene. I dag har ordet «luddit» i all hovedsak en negativ valør, akkurat som «hacker» har det. Aktive ludditer ble fordømt som vandaler i pressen, og det britiske parlamentet gikk så langt at det ble innført dødsstraff for den som med vilje ødela en maskin – men ludditenes protester rettet like fullt søkelyset mot barnearbeid og andre usosiale konsekvenser av industrisamfunnet, og bidro til å presse fram en rekke høyst tiltrengte reformer.

I dag betraktes hackerens forsøk på å sabotere proprietære dataformater med den samme motvilje av maktens representanter. Særlig statsmakten har de seneste årene klart valgt å ta parti for industrien i denne konflikten. I USA har dette i første rekke gitt seg utslag i den tidligere omtalte *Digital Millennium Copyright Act*, hvis effekt er å begrense ytringsfriheten i verdens førende demokrati på måter det knapt er noen som ennå overskuer. En annen juridisk konstruksjon, Haag-konvensjonen, som også Norge vil tiltre dersom det ikke skjer et mirakel, vil i realiteten gjøre DMCA gjeldende innen norsk jurisdiksjon.

I Norge har justis- og politidepartementet laget et eget notat, «Strategi for forebygging av IKT-kriminalitet blant barn og unge», der endog det at ungdommer tar i bruk Linux i stedet for produkter fra Microsoft nevnes som en kilde til bekymring (Justis- og politidepartementet 2000, Johansen 2000). Daværende justis- og politiminister, Hanne Harlem, er enda klarere i sin fordømmelse når hun på følgende måte velger side i konflikten mellom Jon Lech Johansen og filmindustrien: «Det er mange som syntes at DVD-Jon var tøff da han knakk koden, men det er ødeleggende for næringslivet hvis man aksepterer den typen ødeleggelser» (Werenskiold 2000, Stormark 2000).

Sett i dette perspektivet finnes det altså en direkte linje fra det 19. århundres maskinstormere, til våre dagers kryptostormere. Begge grupper forsøker å ødelegge anvendelser av en teknologi som de mener forrykker maktforholdene i retning av det uakseptable og det usosiale.

Regulerbarhet

Vårt moderne samfunn reguleres gjennom en kompleks vev som i tillegg til vedtatte lover og regler består av (blant annet) normer, fysiske gjenstander, markedsmekanismer samt tingenes naturgitte egenskaper (Lessig 1999).

Når for eksempel en større bro ikke blir stjålet, skyldes det ikke bare at tyveri er ulovlig, men like mye den omstendighet at en bro er så stor og tung at det rett og slett er fysisk umulig å stjele den. I tillegg er markedets interesse for brukte broer relativt liten. For sykler forholder det seg motsatt. Disse er høyst transportable og lar seg kjapt omsette. Dersom jeg parkerer min kostbare sykkel på gata i Oslo, er det meget sannsynlig at den blir stjålet med mindre den er sikret med en solid lås. Blomster er både kostbare og lette å ta med seg. Likevel får blomsterkransene som pryder graven etter en begravelse som regel ligge i fred, rett og slett fordi det finnes normer som beskytter disse mot å bli stjålet.

Grovt sett er opphavsrett den rett til å råde over et åndsverk som samfunnet gir verkets opphavsmann. Før oppfinnelsen av trykkpressen var slike rettigheter lite utviklet, rett og slett fordi det å framstille kopier av verket var en så kostbar og møysommelig prosess at verkets natur ga det tilstrekkelig beskyttelse. Først når trykkpressen dukket opp ble det for alvor aktuelt å gi opphavsmannen økt beskyttelse gjennom lover som regulerer opphavsrett. I vårt århundre har nye teknologier som kopimaskiner, båndopptagere, videoopptakere og de siste årene: digital reproduksjon og distribusjon over datanett bidratt til å ytterligere aktualisere problemstillingen.

Vi vet at en lov mot (sykkel)tyveri alene ikke er nok til å forhindre våre sykler i å bli stjålet: både sykkelens natur (lett og transportabel) og markedet (stjålne sykler er lette å omsette) er imot oss. Derfor tar de fleste av oss den forholdsregel å utstyre sykkelen med en solid lås.

Innholdsindustriens dilemma er at nye teknologier for digital reproduksjon og distribusjon gjør det enklere å kopiere åndsverk, og letter formidlingen av både legale og illegale kopier. At denne industrien nå ønsker å beskytte sine produkter – musikk, filmer og dataprogrammer i digital form – med elektroniske låser i form av koder og proprietære formater er derfor i utgangspunktet ikke noe mer oppsiktsvekkende enn at en sykkeleier beskytter sin doning med en solid lås før han setter den fra seg. I begge tilfeller er det snakk om å regulere adgangen til gjenstanden gjennom bruk av teknologi.

Industrien har imidlertid oppdaget at ved å regulere gjennom teknologi kan de tilta seg makt som verken vedtatte lover, normer eller markedet har vært villig til å innrømme dem. I stedet for å selge en bok som kan leses gang på gang, lånes ut, noteres i, osv. kan for eksempel et forlag ved å kapsle boken inn i passende teknologi selge rettighetene til en enkelt gjennomlesning. Ønsker bokens eier å lese dem på nytt, notere i margen, eller låne verket til en venn – så må det betales på nytt.

Hva slags type rettigheter teknologileverandørene ser for seg røpes i dette avsnittet fra sluttbrukeravtalen til *FrontPage 2002* (et forfatterverktøy for websider):

> You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services, infringe any intellectual property or other rights of these parties, violate any state, federal or international law, or promote racism, hatred or pornography. (Microsoft Corp. 2001)

Industrien har imidlertid et problem. De teknologier den så langt har tatt i bruk for å disiplinere brukerne har vist seg å være langt fra så effektive som de skulle ønske. Denne typen maktutøvelse fra industriens side er blitt møtt av motstand ved at såkalte «hackere» har angrepet utøvelser av makt-gjennom-teknologi med en tilsvarende mot-makt. Det vil for eksempel si at de har eksponert industriens skjulte koder og hemmelige formater og dermed gitt forbrukerne *tilbake* noen av de rettighetene i forhold til slike produkter som forbrukerne tradisjonelt har hatt.

Derfor har industrien forstått at den ikke kan stole på makt-gjennom-teknologi alene. For å regulere bruken av teknologi tas det i bruk holdningsskapende arbeid med sikte på å etablere normer som barrierer mot ulovlig kopiering, det tas i bruk teknologier som har som siktemål å disiplinere forbrukere og borgere, og ikke minst: Samfunnets makt-apparat (dvs. lovverket, politiet og rettsvesenet) mobiliseres mot hackere og andre som forsøker å utfordre industrien på disse områdene.

Digitale portvakter

DVD (Digital Video Disc) er et system for lagring av data på plastplater med en diameter på 12 cm. Det er mulig å lagre mer enn 4,7 Gigabyte med data på en slik plate, tilstrekkelig til at en helaftens spillefilm får plass. Data på DVD-plater er som regel kryptert. I tillegg kan dataene gjennom en tallkode (sone) knyttes til en bestemt geografisk region.

Krypteringen skal forhindre at platen avspilles på andre spillere enn dem som er har lisens fra en sammenslutning av verdens største filmselskaper som går under navnet DVD-CCA (Content Control Association), og sonekoden har til hensikt å gjøre platen ubrukelig utenfor dens primære geografiske salgsområde.

I Norge foregår det som sagt politietterforskning mot Jon Lech Johansen fordi han har vært med på å bryte denne sperren.

Men hvorfor er det nødvendigvis slik at det å *bryte* en avspillingssperre er en forbrytelse, men det å *opprette* en lignende sperre skal være tillatt? Kunne man ikke like gjerne tenke seg at det bryter mot lovfestede forbrukerrettigheter (og altså er forbudt) å på dette vis koble forbrukerens kjøp av ett produkt (en DVD-plate) til et annet (en bestemt type avspillingssystem for platen)?

En slik avveiing mellom forbrukerrettigheter og næringslivsrettigheter er sannsynligvis lagt til grunn av det amerikanske justisdepartementet i dommen der det slås fast at Microsofts teknologiske sperre mot å la andre programvareprodusenter «plassere» sitt produkt på Windows-skrivebordet var et konkurransehinder og derfor i strid med amerikansk lovgivning. Men på den annen side: De samme myndigheter har *ikke* bestemt at Office-fil-formatene (Word, Excel, Powerpoint og Outlook), som de facto er utvekslingsformat for tilnærmet 100 % av verdens kontorstøttesystemer, skal åpnes og offentliggjøres. Dermed risikerer enhver som gyver løs på disse formatene for å avsløre deres hemmeligheter å bli straffeforfulgt på samme måten som Jon Lech Johansen med venner blir det.

Det neste store slaget kommer sannsynligvis til å stå om settop-bokser til digitalt fjern-syn. Settop-bokser er slike bokser som man setter oppe på toppen av TV-apparatet (derav navnet). Disse er tiltenkt en lang rekke oppgaver, men primært brukes de til å administrere abonnements- og betalingsregimer, dekode krypterte kanaler og til å tilby brukeren en såkalt elektronisk programguide. Settop-boksens elektroniske program-guide er et stykke programvare som på mange måter arter seg som den nettleseren som de fleste av oss etter hvert er blitt kjent med gjennom bruk av Internett. Som nettleseren er det også i utgangspunktet meningen at den elektroniske programguiden skal hjelpe oss med å navigere i strømmen av programmer, kanaler og assosierte tjenester (eksempelvis shopping, spill og banktjenester) som vil bli en del av tilbudet på digitalfjernsyn.

Det burde derfor ikke komme som en overraskelse at det for øyeblikket foregår en kamp mellom ulike telecom-selskaper om retten til å definere denne underliggende tekniske standarden. For øyeblikket kniver et stort antall aktører om å få aksept for hver sin «standard».

Den som vinner denne kampen (dersom den lar seg vinne), vil komme i en unik posisjon i forhold til å kontrollere hvordan den elektroniske programguiden skal presentere seg selv for brukeren, og derigjennom også bestemme hvilke programtilbud brukeren får, hvilke shoppingstilbud som eksponeres kraftigst og hvilke tilleggstilbud som får plass der de faktisk synes. På mange måter vil tjenesten minne om de ulike portalenes startsider på World Wide Web. Men World Wide Web er tuftet på åpne standarder, og brukerne kan (i prinsippet) selv velge både nettleser og startside. Da Tim Berners-Lee skapte den teknologien som muliggjør dagens nettlesere, skjedde det underlagt ideologiske føringer med røtter i hacker-kulturen der åpenhet var det førende prinsipp (Berners-Lee 1999, s. 80). Slik er det ikke med de planlagte settop-boksene for digitalt fjernsyn. Akkurat som DVD-spillere er disse settop-boksene *konstruert* for å være lukkede enheter som det i utgangspunktet ikke vil være mulig å endre uten en forutgående avtale med den som «eier» spesifikasjonen av den underliggende tekniske standarden.

Den som har gitt deg boksen kommer dermed til å ha en betydelig påvirkningskraft på en del av livet ditt. For eksempel: hvilke programmer og mediekanaler du primært vil oppsøke og hvilke butikker som vil være dine «nærbutikker» i kyberrommet.

I Europa har enkelte telecom-selskaper gått enda lenger. De nekter rett og slett å distribuere de programmene innholdsprodusentene gjerne vil tilby lytterne/seerne/leser-ne/surferne med mindre innholdsprodusenten betaler dem for å utføre transporten. Mange ser på dette som en helt naturlig konsekvens av markedsøkonomien. Nemlig at transport av digitale medier er en tjeneste som det er opplagt at det skal betales for.

Dessverre er det ikke så enkelt. En konsekvens av konvergensprosessen er at de fleste av oss vil være nødt til å forholde seg til *en enkelt* leverandør av infrastruktur for transport av digitalt innhold. Det burde være uproblematisk så lenge infrastrukturen er åpen, slik dagens telefonnett er det, våre veier (stort sett) er det, og Internett (i Vesten) er det. Men det blir langt mer problematisk dersom en privat (eller offentlig) infrastrukturleverandør ønsker å utøve innflytelse på *hva slags* og hvilket innhold vi får adgang til.

Og det er akkurat dette som nå er i ferd med å skje. Ved siden av den eksplisitte tekniske kontroll som kan oppnås gjennom å kontrollere tekniske standarder er vi også vitne til økende bruk av pris-, markeds- og politiske mekanismer for å ta kontroll over informasjonsstrømmen.

I den utstrekning infrastrukturleverandøren har eierinteresser i innholdsselskaper (og det har de som regel, jf. Storsul 1999, Storsul 2001) kan de for eksempel sørge for å bruke prismekanismen for å prise ute innhold som stammer fra konkurrerende innholds-produsenter.

De fleste produsentene av de tidligere omtalte nettfiltre har lenge benyttet seg av sin portvakt-posisjon til å sperre adgangen til enhver webside som ytrer seg kritisk om slike filtre. Fra USA meldes det om at AOL Time-Warner-fusjonen allerede har hatt den effekt at innhold fra andre innholdsleverandører enn nettopp Time-Warner er blitt vanskeligere tilgjengelig for AOL-abonnentene.

Bruk av digitale portvakter er maktutøvelse. Dessuten innebærer ofte slike portvakter en privatisering av makt, dvs. at maktutøvelsen flyttes i fra staten og over i den private sfære. I verste fall kan digitale portvakter benyttes til å utøve en makt som aktøren eksplisitt er nektet av gjeldende lov.

Panoptikon

Overvåkningens pedagogiske funksjon har en særlig plass i Foucaults maktanalyse. Gjennom en rekke eksempler viser han hvordan arkitekturen i institusjoner som fengsler, militærakademier, hospitaler og fabrikker endres fra omkring midten av det 18. århundre. Mens denne typen institusjoner tidligere hadde vært konstruert for å utøve fysisk makt i from av «tykke vegger og en tung port som hindrer en i å komme å gå» (Foucault 1977), blir maktutøvelsen nå langt mer sofistikert. Bygningens arkitektur endres fra å være hemmende til å bli en læremaskin, og slik konstrueres så moderniteten og det moderne mennesket – en mennesketype som er langt mer sosial og føyelig og derfor langt bedre egnet til å være fabrikkarbeider, student og soldat enn middelalderens røffe individualister.

Klarest, sier Foucault, kommer disse pedagogiske ideene til uttrykk i det briten Jeremy Bentham (1748-1832) kalte *panoptikon* (fra de greske ordene *pan* «overalt» og *optikos* «synlig»). På midten av 1700-tallet er fengslets funksjon å straffe forbryteren og å avskrekke andre fra å begå forbrytelser. Bentham mener at dette bare vil gjøre forbryteren enda mer asosial og ytterligere forherdet. Hans plan er derfor å konstruere et fengsel som forbedrer fangens moralske karakter – «en kvern som maler banditter om til ærlige menn» (Semple 1993). For å oppnå dette, sier Bentham, må fangene settes i arbeid og arbeidet må utføres under konstant overvåkning slik at fangen ikke sluntrer unna og hengir seg til asosial aktivitet. Fra Benthams tegninger og beskrivelse framgår

det at dette rent praktisk skal realiseres i form av en sirkulær bygning med et sentralt observasjonstårn, mens fangene plasseres i konstant opplyste celler langs periferien. En særlig finesse er at observasjonstårnet er mørkt, og utstyrt med vinduer slik at det er umulig for fangene å vite *når* de faktisk blir observert, og når vokterne er opptatt med andre ting.

Kyberrommet[3] er det ikke-fysiske «rommet» som dannes når datamaskiner over hele kloden kobles sammen i et gigantisk nettverk. På samme måten som det fysiske rommet formes gjennom arkitektur, bestemmes kyberrommets egenskaper av nettets arkitektur, det vil si de tekniske standardene for datakommunikasjon som sørger for samvirke mellom ulike datasystemer.

I dag kjenner vi kyberrommet som Internett, som både er et verdensomspennende fysisk nett og et sett med tekniske standarder. De mest sentrale av disse standardene betegnes med initialene TCP/IP, som står for henholdsvis *Transmission Control Protocol* og *Internet Protocol*. Sammen sørger disse to protokollene[4] for at data på Internett transporteres effektivt og feilfritt mellom ulike destinasjoner.

Slik TCP og IP er konstruert gir disse protokollene i utgangspunktet ingen direkte hjelp til overvåkning av individers aktivitet på nettet. Kun gjennom et møysommelig analysearbeid der man blant annet kobler data om bruk av TCP/IP (såkalte logger) sammen med andre registre, er det mulig å knytte forbindelse mellom en bestemt dataoverføring på nettet og et bestemt individ. Og ved hjelp av relativt enkle håndgrep, som for eksempel å sende data via en såkalt *anonymiserende stedfortreder* (engelsk: *anonymizing proxy*) kan denne forbindelsen brytes.

I flere land i verden har dette ført til at myndighetene har gjort inngrep i kyberrommets arkitektur. I USA har for eksempel det føderale politiet FBI plassert ut et system i nettet som eksisterer side om side med TCP/IP. Systemet er kjent under kodenavnet *Carnivore*, og gir i prinsippet FBI mulighet til å overvåke all nettrafikk (Smith et al. 2000). Innføringen av et slikt system kan likestilles med konstruksjonen av et virtuelt *panoptikon* i kyberrommet.

Konturene av et slikt virtuelt panoptikon kan også skimtes i en artikkel der første statsadvokat Inger Marie Sunde tar orde for følgende endringer i vår tele- og personvernlovgiving (Sunde 2000):

- Det må ikke være adgang til å tilby anonyme kommunikasjonstjenester slik at brukeren er uidentifiserbar for politiet.
- Det må foreligge registreringer som sporer bruken tilbake til abonnent.
- Registreringene og abonnementsdataene må oppbevares i minst ett år etter at bruken skjedde.
- Opplysningene må utleveres direkte til politiet i forbindelse med etterforsking.

Det er verd å merke seg at Sunde ikke ser noen grunn til å skille mellom ordinære borgere og personer som politiet har skjellig grunn til å mistenke for kriminalitet. *All* vår aktivitet på nettet skal registreres, knyttes til vår identitet, lagres i minst ett år, og

[3] Begrepet *cyberspace* (kyberrommet) ble introdusert av forfatteren William Gibson i romanen *Neuromancer*. I boken forflytter personene seg helst mellom ulike datamaskiner i et verdensomspennende datanett (kyberrommet), i stedet for å reise omkring i det fysiske rommet.
[4] En *protokoll* er i denne konteksten et sett regler for utveksling av data. En formell beskrivelse av en slik protokoll kalles en *standard*.

stilles til disposisjon for politiet uten at politiets rett til å få utlevert slike opplysninger først skal prøves for retten.

Tilsvarende ønsker om overvåking finner man igjen hos politimyndigheter i hele EØS-området. I Storbritannia forligger allerede et utkast til lovendring (*Regulation of Investigatory Powers Bill*) som blant annet påbyr alle operatører av kommunikasjonsnettverk, private så vel som offentlige å installere «svarte bokser» som muliggjør registrering og avlytting av trafikken. Den samme loven foreslår at personer som krypterer data kan straffes med fengsel i inntil to år dersom de nekter eller er ute av stand til å gi kode-nøkkelen til myndighetene (Hansard 2000). Det britiske politiet foreslår videre at logger og abonnementsdata må oppbevares i minst syv år (McCarthy 2000, Ahmed 2000). Og etter et fire dager langt møte arrangert av det svenske riksåklagarämbetet for kolleger fra EU-området utformet forsamlingen et sluttdokument der det blant annet ble slått fast at muligheten for å opptre anonymt på nettet «må innskrenkes» og videre at all nettrafikk må registreres, lagres og bli stilt til disposisjon for politiet (Expressen 2001, Metro 2001). David Calvert-Smith, riksadvokat i Storbritannia, uttalte etter møtet at de enorme informasjonsmengdene som en slik registrering ville generere ikke var noe problem. Politiet har allerede tilgang til spesialprogramvare og superdatamaskiner som uten problemer kan søke gjennom enorme mengder med slikt materiale (ibid.)

Selv registre over relativt lite sensitive data, som for eksempel nettadresser (såkalte URIer) kan brukes til etterforsking. En URI til en søkemotor vil for eksempel avsløre hvilke konkrete søk som er utført. I en norsk giftmordsak ble det faktum at mistenkte hadde søkt etter opplysninger om en bestemt gift på Internett brukt som bevis mot ham i retten.

Det er ingen grunn til å tvile på at denne typen overvåkningssystemer vil lette politiets arbeide vis-à-vis kriminalitet i og utenfor kyberrommet. Men som Foucault har påvist: *Panoptisk* overvåkning fungerer også disiplinerende. En slik overvåkningsteknologi er ikke derfor bare kriminalitetsbekjempende og -forebyggende, den er også en «terapeutisk operator», «en pedagogisk maskin», «et apparat for observasjon, informasjonsinnsamling og opplæring» (Foucault 1977). Det faktum at alle bevegelser og besøk blir registrert og kan bli gjort tilgjengelig for politiet kan for eksempel føre til at en del mennesker avstår fra å oppsøke *lovlig* pornografisk materiale på Internett som de ellers ville ha benyttet seg av. Likeledes vil noen sannsynligvis la være å hente informasjon fra steder i kyberrommet som for eksempel kan knyttes til spesielle seksuelle legninger, sykdommer, alternative livssyn og radikale politiske bevegelser.

Et tankekors er at mange av de teknologiene som er utviklet for elektronisk handel åpner opp for overvåkning i privat regi i et omfang som tidligere ikke har vært mulig. Mens FBI etter amerikansk lov ikke har rett til å få vite hvilke bøker en borger sjekker ut på biblioteket eller hvilke fra hvilke TV-kanaler vedkommende henter sine nyheter, er det ingenting som hindrer en nettbutikk som Amazon.com i å føre detaljerte registre over sine kunders lesevaner.

Jeg må innrømme at jeg har hatt et ambivalent forhold til de «anbefalinger» som jeg har mottatt fra Internett-bokhandlen Amazon.com. Anbefalingene bygger på de data som selskapet har registrert om meg. På den ene siden har jeg satt pris på å bli fortalt om nye, interessante publikasjoner. På den annen side er jeg blitt skremt av presisjonen i anbefalingene: Det var åpenbart at Amazon.com vet mye om hva jeg leser, og dermed også om hva jeg tenker og mener.

Min holdning til dette fikk imidlertid en langt mer negativ valør da selskapet i september 2000 sendte meg et brev der jeg ble fortalt at den «mappe» de hadde samlet om meg var å betrakte som en «overførbar eiendel» (engelsk: «*transferable asset*»). I klartekst betydde det at Amazon.com aktet å behandle de detaljerte kundeprofilene som selskapet har om meg og andre som en vare. Mine persondata kunne bli solgt – som et hvilket som helst annet produkt. (Se også Oberg 2000)

Amazon.com forteller meg imidlertid hva de registrerer og tar bryet med å skrive brev til meg og fortelle hva de akter å gjøre med disse dataene. Andre aktører opererer i det skjulte. Leketøysprodusenten Mattel, for eksempel, leverer såkalte «lek og lær»-programmer gjennom datterselskapet Broderbund. Et av produktene, «Arthur's Reading Race», har femåringer som målgruppe. Med dette programmet fulgte det opprinnelig med en skjult komponent kalt *DSSAgent*. Med jevne mellomrom ville DSSAgent koble seg opp på nettet, «ringe hjem» og utveksle krypterte data med Broderbunds sentrale datamaskiner. Siden datene var kryptert, vet ingen hva slags data som ble utvekslet, men i prinsippet kan en slik agent brukes til å spionere på brukeren. Da DSSAgent ble avslørt, var Mattel raskt ute med å forsikre kundene om at programmet er harmløst. Uansett: DSSAgent er nå fjernet fra «Arthur's Reading Race» (Garfinkel 2000).

I januar 2001 offentliggjorde det anerkjente fagtidsskriftet *Communications of the ACM* utdrag av en rapport fra Privacy Foundation knyttet til University of Denver (Martin Jr. et al. 2001). Forskerne ved institusjonen hadde analysert 16 gratis tilleggsprogrammer («plug-ins») til den populære nettleseren Microsoft Internet Explorer. De oppdaget at samtlige programmer «ringte hjem». I noen tilfeller var brukerne informert om at programmet ville gjøre dette gjennom en såkalt klikk-lisens[5]. Men selv når informasjon ble gitt, var den ofte formulert så uklart eller i så tekniske termer at de fleste brukere neppe var i stand til å fatte hva slags overvåkning de «samtykket» i ved å installere programmet. Programmene registrerte som regel nettadresser (URIer) som ble besøkt, og hvordan brukeren forholdt seg til tilbud og produkter fra konkurrenter. Ett av programmene fanget til og med opp transaksjonsdata som brukeren trodde kun ble kommunisert til en tredjepart.

Det er imidlertid ikke nødvendig å installere tilleggsprogrammer for å bli gjenstand for overvåkning. Samtlige nettlesere som er i vanlig bruk i dag støtter utplassering av såkalte informasjonskapsler («cookies») på brukerens harddisk. Disse ble opprinnelig utviklet for å bøte på den begrensning (i alle fall fra et e-handel-perspektiv) at World Wide Web er tilstandsløst. Det finnes mange situasjoner der det er helt legitimt å gjøre bruk av informasjonskapsler, og hvor informasjonskapselen ikke utgjør en trussel mot personvernet. Dessverre er det også mulig å misbruke informasjonskapsler til overvåkning. Særlig gjelder dette tredjeparts-informasjonskapsler, som muliggjør kobling av registre fra flere kilder og dermed åpner opp for utstrakt kartlegging på tvers av selskapsgrenser og kundeforhold.

Registrering og lagring av personinformasjon uten hensyntaken til informasjonens forretningsmessige eller politimessige relevans reiser også et annet problem. Når

[5] En klikk-lisens er noe som vises før en bruker for første gang tar i bruk et program eller en online-tjeneste. Den består som regel av en plakat som viser vilkårene for bruk, inklusive de vilkår som regulerer innsamling, bruk av og distribusjon av brukerdata. Brukeren skal indikere at han har lest vilkårene, og aksepterer dem ved å «klikke» på en knapp med teksten «Jeg aksepterer».

informasjonen først er lagret, er den søkbar, tilgjengelig for datautgraving (engelsk: *data mining*) og kan lett kobles til annen informasjon.

En lærdom man kan trekke av de norske jødenes skjebne under siste krig er at slike registre kan, gitt forandringer i det politiske klima, bli brukt til helt andre formål enn de var tiltenkt. Fordi okkupasjonsmakten fikk adgang til bostedsstatistikken fra Statistisk sentralbyrå, kunne den med skremmende effektivitet lokalisere jøder som så ble sendt til Tyskland for utslettelse. På samme måte bruker den israelske hæren i våre dager data fra de palestinske selvstyremyndighetenes statistikkontor, som de skaffet seg adgang til gjennom et militært raid mot det sentrale dataanlegget i Al Bireh utenfor Ramallah 5. desember 2001, til å lokalisere boligene til palestinske aktivister og medlemmer av Hamas. Disse husene rives så ned med bulldosere eller sprenges i luften. Under den kalde krigen ble det registrert informasjon om aktiviteter som i og for seg ikke var kriminelle, men som røpet utøverens politiske sympatier. Disse ble benyttet til å stenge personer med antatt venstreradikal holdning ute fra arbeidsmarkedet.

Digital livsstil

Digital teknologi, i form av datamaskiner og digital kommunikasjonsutrustning, har forlengst spredt seg fra laboratoriene og datasentralene og befinner seg som en integrert del av mange arbeidsplasser og hjem. På tampen av år 2000 har over halvparten av norske husstander hjemmedatamaskin med tilgang til Internett, og omlag tretti prosent av den norske befolkning over 13 år benytter Internett daglig (Norsk Gallup Institutt 2000).

Dette betyr blant annet at mange av oss allerede har utviklet en livsstil der digital teknologi benyttes i utøvelse av en rekke dagligdagse aktiviteter, som for eksempel sosialisering, informasjonssøking, betaling og innkjøp. Nye digitale tjenester, som fjern-undervisning, telemedisin, nettaviser, nettbank og åpen online offentlig informasjon er i ferd med å bli en del av vår hverdag. På beddingen ligger nå en er rekke gjenstander og teknologier (for eksempel personlige digitale assistenter, dataklær, e-bøker, digital-fjernsyn, Internett-telefoni, mobilt Internett, intelligente agenter og digitale program-guider) som hver for seg kan bidra ytterligere til digitalisering av hverdagen. Noen ser for seg en framtid der både de gjenstander som omgir oss, og vi selv, har en eller flere digitale innretninger innebygget som er koblet opp mot nettet[6].

Men det er selvsagt ikke gitt at framtiden blir slik. Teknologi er ikke autonom. I prinsippet kan vi velge hva slags teknologi vi vil ta i bruk, og hva slags egenskaper den skal ha.

Men dette innebærer likevel ikke at den enkelte av oss vil kunne beslutte dette for oss selv, heller ikke at slike beslutninger er uavhengig av andre beslutninger. Og dersom du

[6] En gruppe forskere ved Göteborg Universitet har laget et system for datastøttet samarbeid der det forutsettes at man bærer med seg en «personlig digital assistent» som både rapporterer hvor man selv befinner seg, og posisjonen til de personer man er interessert i å følge bevegelsene til (Dahlberg et al. 2001). En slik «assistent», sier de, vil være nyttig dersom man har behov for å vite om kollegaer og venner befinner seg i nærheten. Professor Kevin Warwick ved Reading University har gått et skritt lenger. Han har operert inn i kroppen en digital sonde. Dermed kan datamaskiner som sonden kommuniserer med åpne dører og spille av en personlig hilsen når Warwick nærmer seg (Warwick 2000).

forventer at det norske samfunnets adopsjon og implementasjon av digital livsstil en eller annen gang vil bli plassert på en stemmeseddel slik at hver især skal kunne ta stilling til spørsmålet gjennom et eksplisitt valg, vil du sannsynligvis bli skuffet.

Som blant andre Wiebe E. Bijker har påvist: Utviklingen av teknologi, og parallelt med dette, samfunnets adopsjon av teknologi, er gjenstand for innfløkte prosesser som blant annet karakteriseres ved at inntil teknologien er «stabilisert» finnes det en såkalt tolkningsfleksibilitet, (dvs. ulike alternativer for utforming, forståelse og bruk av teknologien) som i sin natur er en sosial prosess og gjenstand for blant annet verdivalg, interessemotsetninger, samt praktiske og økonomiske vurderinger – kort sagt: politikk (Bijker 1995, s. 84ff). Som Foucault poengterer Bijker at aktørene i denne prosessen like gjerne kan være maskiner som mennesker, og at den makt og mot-makt som utøves skjer i en matrise der det ikke eksisterer klare fronter, men snarere en mengde konfrontasjonspunkter fordelt over kantene i et nettverk. Bijker kaller slike nett «sosio-tekniske ensembler» (ibid., s. 274).

La oss nå betrakte et konkret konfrontasjonspunkt i spørsmålet om «digital livsstil». Punktet manifesterer seg i form av en notis med overskriften «Ingen forsikring uten nett» i Nettavisen 10. november 2000. Bakgrunnen er at et forsikringsselskap, Aktiv Forsikring, har besluttet at det utelukkende vil tilby salg og vedlikehold av forsikrings-produkter via Internett (Lilleås 2000). Kunder som av ulike årsaker ikke ønsker å la seg betjene via Internett, vil altså ikke ha tilgang til selskapets tjenester.

Et annet konfrontasjonspunkt er Statens *elektroniske reiseregning*. Kun én elektronisk utgave eksisterer, og den introduseres for potensielle brukere på følgende måte:

> Vi gjør oppmerksom på at utgaven bare kan benyttes for Windows 95/98/2000 samt forskjellige utgaver av NT. (Statens Forvaltningstjeneste 2001)

Det ligger i denne tjenestens natur at man må ha tilgang til et datasystem for å kunne benytte den, men teksten røper at det også foreligger et tilleggskrav, nemlig at man må ha tilgang til en datasystem fra én bestemt produsent. Produktnavnene det refereres til skrives fullt ut: *Microsoft Windows* og *Microsoft NT*, og viser altså til en serie proprietære datasystemer som alle selges av selskapet Microsoft Corp. Ved å knytte bruken av Statens elektroniske reiseregning *direkte* til denne produsentens datasystemer utøver Staten mikromakt der de etater og institusjoner i Staten som eventuelt har valgt et annet datasystem (Apple, Linux, Sun, etc.) blir «fortalt» at de bør skifte ut sin nåværende plattform med datasystemer fra Microsoft Corp. Den utbredte bruken av proprietære utvekslingsformater for dokumenter (les: *Microsoft Word* og *Microsoft Excel*) er et annet eksempel på utøvelse av mikromakt som virker i samme retning.

I den senere tid er det kommet signaler fra Microsoft og andre ledende produsenter av programvare om at selskapene akter å gå bort fra å selge programmer. I stedet vil selskapene lisensiere til kundene retten til å bruke programmet i en begrenset tids-periode. Med andre ord: I det øyeblikket kunden slutter å betale lisensen, slutter programmet å virke. Gjennom bruk av proprietære lagringsformater har selskapene allerede sikret seg at ingen *andre* programmer kan lese de data som er lagret med programmet. Dermed må kundene pent finne seg i å betale programvareselskapene på nytt og på nytt for å beholde muligheten til å bruke *sine egne* data.

Forsikringsselskapets, Statens og programvareselskapenes artikulasjon av sin posisjon vis-à-vis kunder/ansatte og teknologi er både synlig og usynlig. Den er *synlig* i den forstand at vilkårene for å kunne benytte tjenestene og produktene uttrykkes eksplisitt.

Den er *usynlig* i den forstand at selve maktutøvelsen er delegert til det sosiotekniske ensemblet der PC-en, Internett/Windows, programvaren, dataene, samt brukerne/ansatte og forsikringsselskapet/Staten er aktører.

Minst like interessant som å observere den delegering av maktutøvelse som her foregår, er den observasjon at delegeringen bidrar til å gjøre maktutøvelsen *varig* og *distribuert*, nettopp fordi den skjer gjennom fysiske gjenstander og teknologier som i seg selv er varige og distribuerte (Latour 1991).

Kunder som av ulike grunner ikke ønsker om å gi etter for Forsikringsselskapets krav om bruke Internett kan selvsagt avvise kravet ved å flytte sitt kundeforholdet til et annet forsikringsselskap, og ansatte i staten som ikke ønsker å velge Microsoft som sin systemleverandør kan selvsagt levere en tradisjonell reiseregning på papir. Men dette er bare muligheter så lenge slike alternativer eksisterer[7]. Dersom *samtlige* finansinstitusjoner følger Aktiv Forsikrings eksempel og stenger døren for kunder uten Internett-tilknytning blir det vanskeligere for en forsikringskunde å holde fast ved en slik strategi. Og dersom sentrale institusjoner i samfunns- og arbeidsliv følger etter, og for eksempel gjør det umulig (eller svært tungvint, eller svært kostbart) å få seg en utdannelse, samarbeide, benytte offentlige helsetjenester, stemme ved valgene, eller levere en reiseregning uten at man bruker bestemte typer teknologi, da er det neppe lenger mulig å yte motstand mot å ta i bruk teknologien og *samtidig* fungere som borger av samfunnet.

Implikasjoner

Vi er i disse dager vitne til et massivt skifte i maktforholdene mellom næringsliv og forbrukere, og mellom staten og borgerne. Skiftet er først og fremst forårsaket av de økte muligheter for utøvelse av mikromakt som ligger latent i kraftfulle nye informasjons- og kommunikasjonsteknologier, konvergensutviklingen og den økte betydningen disse teknologiene får i vår felles hverdag.

Denne utviklingen har hittil vært preget av at industrien (så langt) har vært langt flinkere enn borgerne og forbrukerne til å mobilisere mediemessig og politisk støtte for sitt prosjekt. Derfor har motstanden hittil vært minimal mot den uthuling av forebrukerrettigheter, ytringsfrihet og personvern som disse teknologiene representerer. Folk flest finner seg tilsynelatende i å miste kontrollen over egne data gjennom bruk av proprietære lagringsformater, og godtar både misbruk av informasjonskapsler og andre former for privat spionasje. Lover som DMCA og Haag-konvensjonen, som utfordrer forbrukerrettigheter, ytringsfrihet, personvern og demokrati, lobbyes gjennom uten noen forutgående offentlig debatt, og knapt nok uten at det heves et øyenbryn utenfor hackermiljøet.

Jeg er likevel ikke pessimist. De utskjelte ludditene vant til slutt fram med sine krav om regulert arbeidstid, forbud mot barnearbeid og krav til arbeidsmiljø og -kvalitet.

I dag utøves motmakten i kyberrommet av en marginal og utskjelt gruppe: hackerne. Men jeg er overbevist om at etter hvert som vår forståelsen knyttet til maktutøvelse i kyberrommet modner, vil vi se en økt og folkelig motstand mot at de proprietære

[7] For øyeblikket ser det imidlertid ut til at det er motkreftene som vinner konfrontasjonen med Aktiv Forsikring. Selskapet har siden november 2000 tapt en betydelig andel av sine kunder (Kvalheim 2001).

formatene, kodene, digitale portvaktene og usosiale lovene som i dag disiplinerer vår digitale hverdag og enn så lenge gjør det mulig for de store markedsaktørene å forme forbrukerne, kontrollere kundene og kue konkurrentene.

Referanser

Ahmed, K. (2000) Secret plan to spy on all British phone calls, *Observer*, London, Sunday, December 3.

Berners-Lee, T. (1999) *Weaving the Web. The original design and ultimate destiny of the World Wide Web, by its inventor.*, Orion Business, London.

Bijker, W. E. (1995) *Of Bicycles, Bakelites and Bulbs. Towards a Theory of Sociotechnical Change*, MIT Press, Cambridge, Massachusetts.

Cnet (2001) *Microsoft Executive Says Linux Threatens Innovation*, [2001-08-22], oppdatert: February 14, Cnet, (web newspaper) <http://news.cnet.com/investor/news/newsitem/0-9900-1028-4825719-RHAT.html?tag=ltnc>.

Dahlberg, P., Ljungberg, F. and Sanneblad, J. (2001) Proxy Lady: Mobile Support for Opportunistic Communication, *Scandinavian Journal of Information Systems*, vol. 13, no. 1.

Expressen (2001) Domare och polis vill registrera all e-post inom EU, *Expressen*, Stockholm, Feb. 15, s. 1.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison.*, Allen Lane, London.

Foucault, M. (1980) *Power/knowledge: Selected interviews and other writings by Michel Foucault 1972-1977*, Pantheon, New York.

Foucault, M. (1982) The subject and power. I: *Michel Foucault: Beyond structuralism and hermeneutics*, (Red. H. L. Dreyfus and P. Rabinow), University of Chicago Press, Chicago, ss. 208-226.

Garfinkel, S. (2000) *Software that can spy on you*, [2000-06-16], oppdatert: June 15, Salon.com, (web magazine) <http://www.salon.com/tech/col/garf/2000/06/15-/brodcast/index.html>.

Hansard (2000) *Regulation of Investigatory Powers Bill*, May 25, House of Lords, London, pp. col. 880-913.

Johansen, P. A. (2000) Justisminister Hanne Harlem:Kamp mot yngres datakrim, *Aftenposten*, Oslo, 17. august, s. 22.

Justis- og politidepartementet (2000) *Strategi for forebygging av IKT-kriminalitet blant barn og unge*, udatert, Justis- og Politidepartementet, Oslo.

Kvalheim, E. (2001) Internett-satsing halverer kundemassen, *Finansavisen*, Oslo, 19. februar, s. 17.

Latour, B. (1991) Technology is society made durable. I: *A Sociology of Monsters. Essays on Power, Technology and Domination.*, (Red. J. Law), Routledge, London, ss. 103-131.

Lessig, L. (1999) *Code and other laws of cyberspace*, Basic Books, New York.

Lilleås, H. S. (2000) Ingen forsikring uten nett, *Nettavisen*, 10. november.

Martin Jr., D. M., et al. (2001) The Privacy Practices of Web Browser Extensions, *Communications of the ACM*, vol. 44, no. 2, ss. 45-50.

McCarthy, K. (2000) *Police request right to spy on every UK phone call and email*, [2001-01-02], oppdatert: Dec. 4 2000, The Register, (web page) <http://www.-theregister.co.uk/content/6/15203.html>.

Metro (2001) Åklagare vill registrera all trafik på Internet, *Metro Stockholm*, Feb. 16, s. 1.

Microsoft Corp. (2001) Frontpage 2002 End-User License Agreement For Microsoft Software.

Nelson, T. (1965) The Hypertext, I: *World Documentation Federation*, ACM.

Nelson, T. (1974) *Computer Lib / Dream Machines*, Theodor H. Nelson, Sausalito.

Norsk Gallup Institutt (2000) *Intertrack*, November, Oslo.

Oberg, A. (2000) Why does Amazon think it owns my privacy? *USA Today*, September 12, s. 29A.

Pahati, O. J. (2001) *Microsoft Goes McCarthy in War Against Linux*, [2001-08-22], oppdatert: August 14, Alternet.org, (web page) <http://www.alternet.org/story.-html?StoryID=11321>.

Semple, J. (1993) *Bentham's Prison: A Study of the Panopticon Penitentiary*, Oxford University Press, Oxford.

Smith, S. P., et al. (2000) *Independent Review of the Carnivore System*, November 17, IIT Research Institute, Lanham, MD, p. 121.

Stallman, R. M. (1985) *The GNU Manifesto*, Free Software Foundation, (web page) <http://www.fsf.org/gnu/manifesto.html>.

Statens Forvaltningstjeneste (2001) *Reiseregningen*, [2001-02-16], oppdatert: 2001-01-02, Statens Forvaltningstjeneste, (web page) <http://www.ft.dep.no/publiser.nsf-/lookup/9E513BCF0DB17D95C12566CF00432612?OpenDocument>.

Stormark, K. (2000) DVD-Jon får ris, *VG*, Oslo, 30. mai.

Storsul, T. (1999) Konvergering og konsentrasjon - om eierskap og mangfold i det nye mediebildet. I: *Nettsamfunn*, (Red. K. Braa, P. Hetland and G. Liestøl), Tano Aschehoug, Oslo, ss. 141-156.

Storsul, T. (2001) På begge sider av kamera, *Dagens Næringsliv*, Oslo, 5. jan, s. 39.

Sunde, I.-M. (2000) IKT-kriminalitet: Etterforskningsmetoder og personvern, *Nordisk Tidsskrift for Kriminalvidenskab*, no. september.

Warwick, K. (2000) I want to be a cyborg, *Guardian*, January 26.

Werenskiold, T. (2000) *Hacker-jegere møtes i Oslo*, [2000-05-29], oppdatert: 2000-05-29, digi.no, (webpage) <http://www.digi.no/digi98.nsf/pub/dd20000529144800-TKW7066758221>.