telematik 2004

KFB & teldok.

Privatliv & Internet – som olja och vatten?

Anders R Olsson

telematik

Denna rapport i programmet Telematik 2004 är på samma gång KFB-rapport 2000:16 (ISBN 91-88371-71-9) och TELDOK Rapport 134 (ISSN 0281-8574).

2004

TITEL/TITLE
Privatliv & Internet
– som olja och vatten?

ISSN
KFB: 1104-2621
ISSN TELDOK: 0281-8574

FÖRFATTARE/AUTHOR
Anders R Olsson

PUBLICERINGSDATUM/DATE PUBLISHED
April 2000

SERIE/SERIES
Telematik 2004
KFB-Rapport 2000:16
TELDOK Rapport 134

UTGIVARE/PUBLISHER
TELDOK och KFB – Kommunikations-forskningsberedningen, Stockholm

KFBs DNR
99-330

ISBN KFB:
91-88371-71-9

TELDOK-rapporter kan beställas från Lindegården, telefon 020-23 00 11.

TELDOK-reports can be ordered from Lindgården by calling +46-20-23 00 11.

I Kommunikationsforskningsberedningens – KFB – publikationsserier redovisar forskare sina projekt. Publiceringen innebär inte att KFB tar ställning till framförda åsikter, slutsatser och resultat.

KFB-rapporter försäljs genom Fritzes Offentliga Publikationer, 106 47 Stockholm, tel 08-690 90 90.

Övriga KFB-publikationer beställs och erhålls direkt från KFB**.** Man kan dessutom abonnera på tidningen KFB-Kommuniké.

KFB Reports are sold through Fritzes', S-106 47 Stockholm.
Other KFB publications are ordered directly from KFB.

Privatliv & Internet
– som olja och vatten?

Anders R Olsson

Företal

De tekniska framstegen – kan ingen sätta stopp för all denna utveckling? – och framstegen beträffande informationsbearbetning i det moderna samhället har ibland, inte bara av dysterkvistar och fantasyförfattare, setts gå hand i hand med att möjligheterna till personlig integritet och privatliv blir hotade. ”Storebror ser dig – överallt!” säger Aftonbladet 27 mars 2000, ty ”Sverige bevakas av 18 845 kameror”.

Krönikören Larry Magid, i Upside Magazine, konstaterar att vi måste betala mer t o m för våra matvaror om vi inte använder ”förmånskort” som gör det möjligt för livsmedelskedjan att kartlägga alla våra inköp. Och vi kartläggs inte bara i ”den verkliga världen”; också på Internet lämnar vi finger- och fotavtryck. Bland ett urval från de mest besökta webb-sajterna i USA samlar 93 procent in uppgifter om besökarnas namn eller adresser, medan 57 procent sparar minst någon demografisk uppgift; uppgifterna kan säljas eller bearbetas vidare för att skapa mer träffsäker marknadsföring – och ännu mer detaljerade databaser.

Internet och personlig integritet är temat för denna rapport. ”Privatliv och Internet – som olja och vatten?” har författats av författaren och journalisten Anders R Olsson och utges i programmet Telematik 2004 som drivs av KFB (Kommunikationsforskningsberedningen) och TELDOK. Anders R Olssons syfte är att ”reda ut förutsättningarna för diskussionen om ett rättsligt skydd” för vad som kan kallas personvärn eller dataskydd, främst på det snabbt föränderliga Internet.

Anders R Olsson kan konkludera att det (ännu?) förefaller finnas bara få exempel på att enskilda råkat ut för svåra integritetskränkningar via Internet. Det kan förstås också bero på att ”empiriska studier nästan helt saknas”, något som gör frågan svår att diskutera och hantera, och som får Anders R Olsson att (i avslutningskapitlet) skissera en rad lämpliga åtgärder. Diskussionen fortsätter!

KFB och TELDOK startade våren 1999 programmet Telematik 2004 för att att finansiera och publicera studier av tidiga IT-användare och användningsområden. Utgångspunkten är de förändringar som

sker i samband med förverkligandet av ”informationssamhället” och vad detta betyder för Sverige. Vilka blir följderna om stora grupper av människor och företag börjar använda den teknik som i nuläget ett mindre antal nyttjar? Rapporter om tidig användning av ”telematik” och IT – sådana rapporter som publiceras inom Telematik 2004 – kan ge vägledning.

Inom Telematik 2004 publiceras två slags skrifter: småskrifter (på som mest 30–50 sidor, baserade på samtal) och rapporter (på cirka 100 sidor, som beskriver och analyserar utvecklingen inom ett visst område). ”Privatliv och Internet – som olja och vatten?” är den fjärde skriften i programmet och den andra ”rapporten”. (Tidigare utgivna titlar förtecknas på omslagets bakre insida.)
Trevlig läsning önskas.

Hans Mohlin
TF generaldirektör KFB

Bertil Thorngren
professor, CIC, Handelshögskolan,
Telia Business and Innovation,
Ordförande TELDOK Redaktionskommitté

Innehåll

Sammanfattning

Frånvaron av kontinuerlig nyhetsrapportering om – och debatt kring – integritetsfrågor beror sannolikt på dessa frågors undanglidande karaktär. Det som behöver belysas och diskuteras sträcker sig in i en framtid vars tekniska, politiska och sociala realiteter vi har svårt att bedöma. Riskerna för att människor drabbas av obehag och skador tycks rent teoretiskt vara mycket stora, för att inte säga överhängande, men de människor av kött och blod som hittills har drabbats av kränkningar är få och/eller svåra att upptäcka. Därtill kommer att de personer som borde uppmärksamma och driva integritetsfrågorna – politiker, forskare, journalister – ofta har svårt att hänga med i den informationstekniska utvecklingen.

I en tid när Internetanvändningen ökar dramatiskt börjar bristen på forskning, folkbildning och debatt i integritetsfrågor bli alltmer besvärande. Fortgår utvecklandet av nya IT-tillämpningar i samhällelig omedvetenhet om riskerna ökar sannolikheten för att man ”hamnar snett”, t ex genom att stora IT-satsningar på ett alldeles för sent stadium döms ut som mänskligt eller demokratiskt oacceptabla. Riskerna föreligger i såväl privat som offentlig sektor.

Integritetsproblematiken är komplex och utvecklingen måste studeras och diskuteras ur flera perspektiv. Föreliggande rapport pekar, för att sammanfatta, på följande trender:

Riskerna

Det är uppenbart att människor som kommunicerar allt mer via Internet och integrerar nätburna tjänster i sin vardag också blir alltmer utsatta i integritetshänseende. Surfar man på Internet lämnar man ”elektroniska spår” på varje webplats, deltar man i gruppdiskussioner eller skickar e-post kan man aldrig veta – såvida man inte krypterat sina meddelanden – vilka som kommer åt informationen. (Och privatpersoner emellan är kryptering idag mycket sällsynt.)

Begreppet Storebror brukar, efter den allseende diktatorn i Orwells roman ”1984”, beteckna överheten i allmänhet och staten i synnerhet. Vittnesmål och analyser baserade på allmänt tillgänglig information

ger starka belägg för att det finns ett internationellt övervakningssystem – vanligen kallat ECHELON – i drift. Några försök att mer detaljerat reda ut vad som är sant och osant i de omfattande skriverierna om ECHELON görs inte i denna rapport. Enligt författarens (Anders R Olsson) uppfattning finns det dock stöd för slutsatsen att stora mängder tele- och datatrafik fortlöpande ”avtappas” från kommunikationsnät över hela världen.
Trafiken matas vidare genom datorer som kan ”slå larm” för vissa ord eller egenskaper i de kommunicerade budskapen. Här har således nationella säkerhetsorgan tagit den nya tekniken i bruk för en kvalitativt ny arbetsmetodik – från domstolsbeslutad avlyssning av brottsmisstänkta individer till generell avlyssning av samtliga medborgare.

Storebrorsproblematiken aktualiseras emellertid också ofta som oplanerade konsekvenser av tekniska system som utvecklats för de mest behjärtansvärda ändamål. Trafikövervakning som syftar till lägre hastigheter, bättre framkomlighet och snabbare upptäckt av olyckor visar sig också möjliggöra en exakt övervakning av enskildas geografiska förflyttningar. Övervakningskameror på allmänna platser får samma dubbla funktion – trygghetsskapande men också potentiellt integritetskränkande. Trådlös datakommunikation (telefon, Internet) är ytterligare ett exempel på något praktiskt och nyttigt som likväl, ur ett annat perspektiv, är djupt obehagligt.

Också för Lillebror – individer eller organisationer i det civila samhället – erbjuder Internet oroande möjligheter. I värsta fall fungerar nätet som ett gigantiskt, väl indexerat klotterplank där individen A har stora möjligheter att skada och spionera på individen B.

Den kommersiella verksamhet som brukar sammanfattas med begreppet e-handel aktualiserar en rad svåra frågor. En tydlig trend är att företagen får ökande behov av kunskap om såväl etablerade kunder – för att tillmötesgå deras alltmer detaljerade önskemål – som potentiella. Om de förra måste man skaffa alltmer individanknuten kunskap, till de senare måste kunna sända ut reklambudskap med ökad precision. E-handelns producentintressen får således starka ekonomiska incitament att bedriva närgången kartläggning av konsumenter.

Den rättsliga utvecklingen

Debatten om hur personlig integritet bäst skyddas har pågått i mer än 30 år. Under lång tid har man i västvärlden försökt lösa problemen

med generella regler om hur ”personuppgifter” får hanteras. EU:s direktiv från 1995 om skydd för persondata, som resulterat i den svenska Personuppgiftslagen, är ett sent exempel på sådan lagstiftning. Av flera skäl är dock generella bestämmelser utomordentligt svåra att tillämpa på ett rimligt sätt, och särskilt svåra i en rättstradition som den svenska. Trenden förefaller nu vara att man oftare utformar integritetsregler anpassade efter olika samhällssektorer och/eller uttrycksformer. Myndigheter får sina bestämmelser, företag och organisationer andra och enskilda medborgare åter andra. Här föreligger dock en betydande osäkerhet om färdriktningen, bl a därför att problemet med okunnighet inom främst politiker- och journalistkårerna är stort inte bara i Sverige.

Den tekniska utvecklingen

Jämsides med ansträngningarna att lösa integritetsproblemen på rättslig väg pågår många försök att utveckla rent tekniska skyddsmetoder. De bygger i flertalet fall på krypteringstillämpningar och brukar sammanfattas med begreppet Privacy Enhancing Technologies, PET. Flera PET förefaller ha goda förutsättningar att fungera, särskilt om det bland allmänheten kan skapas en större medvetenhet om integritetsproblematiken, därför att företag kan integrera dem i sin affärsverksamhet och utnyttja detta faktum i sin marknadsföring. I bästa fall slås då företag som i alltför liten grad beaktar integritetsfrågorna ut från marknaden.

PET och tekniska standarder som stöder integritetsskydd kan dock aldrig bli mer än komplement till andra lösningar för integritetsskydd.

Den kulturella/socialpsykologiska utvecklingen

Den svenska debatten om hoten mot personlig integritet fick ett närmast abrupt slut med den s k Metropolit-skandalen 1986. Under 1990-talet har ingen stor debatt eller journalistisk kampanj förts på integritetstemat. Uppenbarligen har någon slags skov inträtt i det allmänna medvetandet som ändrat förutsättningarna för offentlig diskussion i frågan. Det är oroande att debatten i massmedier och politiska fora har tystnat just i den epok då 1970- och 80-talens farhågor – Storebror kommer! – tycks mer befogade än någonsin.

Verkningsfulla åtgärder för starkare integritetsskydd måste bygga

på förståelse för denna socialpsykologiska förändring. Här fordras uppenbarligen en genomgripande humanistisk forskning och debatt kring de förändrade livsvillkoren i IT-samhället. Att vi behöver skydd för den personliga integriteten kan inte betvivlas – men vad är det mer precis vi anser skyddsvärt och vilket ”pris” är vi beredda att betala för skyddet?

Kapitel 1
Inledning

1998 hade flera tidningar notiser om kvinnan som råkade illa ut när hon gjorde slut med – och flyttade från – sin pojkvän. Den försmådde unge mannen lade ut en kontaktannons på Internet i hennes namn, med e-postadress och telefonnummer, i vilken hon förklarade sig intresserad av diverse sexuella aktiviteter. Ett 30-tal intresserade män hann höra av sig innan annonsen togs bort. Den f d sambon dömdes småningom för grovt förtal. (Hovrätten i Nedre Norrland, mål nr B 444/96)

Förtalaren gick denna gång att spåra som avsändare av annonsen. Med större teknisk skicklighet hade han kunnat försvåra eller t o m omöjliggöra identifieringen. Får vi med Nätet i praktiken en informations- och yttrandefrihet som är total och därmed utan nåd? Raseras med den nya informationsteknologin, IT, våra möjligheter att värna den personliga integriteten?

Hämtar man all sin kunskap ur den dagliga nyhetsrapporteringen får man lätt det intrycket. Internet beskrivs ofta som ett revolutionerande ”fritt” medium. Det upphäver nationsgränser och är oåtkomligt för rättslig reglering. Den ”nakna” eller ”drabbade” individen är också tacksamt stoff för journalistik. När beslutsfattare på lokal, nationell eller internationell nivå likväl försöker att i någon mening reglera Internet ligger den motsatta, också säljande vinkeln nära till hands: då handlar det om ”maktens” angrepp på yttrandefriheten. Nyheter och reportage där Internet står i centrum tar gärna sats i den ena eller andra hot-föreställningen. (Därmed inte sagt att sådana vinklingar generellt skulle vara omotiverade eller farhågorna obefogade.) Också politiska utspel i dessa frågor – ofta tillspetsade för att passa nyhetsförmedlingens dramaturgi – tenderar att stärka polariseringen mellan ont och gott, frihet och tvång, civilisation och barbari.

Avsikten med denna studie är att reda ut förutsättningarna för diskussionen om ett rättsligt skydd för personlig integritet. Utifrån dessa förutsättningar diskuteras vilka handlingsalternativ som står de samhälleliga aktörerna – lagstiftaren, företag, intresseorganisationer och medborgare – till buds.

Resonemangen måste i viktiga avseenden föras med ett internationellt perspektiv på utvecklingen. De metoder man i övriga världen väljer för integritetsskydd, liksom hur skyddet prioriteras gentemot andra samhälleliga intressen, påverkar utvecklingen inom områden som elektronisk handel, brottsbekämpning och IT-stödd förändring av demokratiska processer. Andra länders nationella lagstiftningsstrategier, liksom internationella överenskommelser med konsekvenser för integritetsskydd kommer att delvis bestämma vad som blir möjligt respektive omöjligt att göra & besluta i Sverige.

1.1 Avgränsning

”Personlig integritet” är, som snart kommer att framgå, ett svårfångat ämne. I Sverige tycks numera enstaka, väl avgränsade integritetsproblem ge upphov till debatt, t ex polisens åsiktsregistrering eller arbetsgivares krav på att drogtesta de anställda. Bredare perspektiv på integritetsfrågan anläggs dock ytterst sällan i den offentliga debatten. Orsaken är inte att människor tvistar om värdet av personlig integritet. Däremot råder oklarhet och/eller oenighet om 1) hur problemen ska beskrivas idag, 2) vilka mål som det är BÅDE önskvärt och realistiskt att sträva mot, och 3) vilka metoder man då ska använda. Överhuvudtaget uppträder sällan någon debattör som har skaffat sig en genomtänkt uppfattning i frågorna 1-3.

Att studien avser personlig integritet just i relation till Internet innebär visserligen en avgränsning men gör inte problematiken så mycket mer lättfångad. Internet utvecklas och förändras fortlöpande. Det är en teknisk plattform för kommunikation, varken mer eller mindre. Det går inte att förutsäga ens på medellång sikt hur samhällets ”stora elefanter” kommer att utnyttja den rikedom av möjligheter som plattformen erbjuder – eller hur enskilda gör det. Vi vet t ex inte hur vanligt det blir att utnyttja Nätets potential för spontana kontakter och mänskligt nätverksbyggande. När man år 2010 behöver kontakt med någon – en förälder till ett MS-sjukt barn, någon som vet hur man fixar förgasaren till en Volvo PV -62, någon som träffat Adolf Eichman – kommer det då att vara vanligt att man skickar ut en efterlysning i cyber-rymden? I den ”globala by” som en del visionärer beskriver räcker det ju att frågan läses av någon som vet mer, och kan hjälpa en vidare, så har man goda förutsättningar att upprätta den där kontakten. Idag använder vissa grupper, journalister och programmerare för att nämna ett par, Internet just på

det viset. Blir det vanligt bland verkligt stora kategorier människor kommer den spontana spridningen av personuppgifter på Internet att öka kraftigt – på gott i många avseenden, på ont i andra.

Innebär avgränsningen till Internet att man kan lämna åt sidan klassiska integritets-problem som t ex motsättningen mellan polisiära intressen av övervakning/informationstillgång och medborgarnas rätt till skydd för privatlivet? Dessvärre inte. Om just denna motsättning igår handlade om åsiktsregistrering och telefonavlyssning gäller den idag också elektronisk övervakning av medborgares meddelanden & agerande på Nätet. På Internet avsätter människor ofta flera och mer avslöjande spår än vid kommunikation och informationssökning med äldre teknik. Här får poliser/säkerhetspoliser/skattemyndigheter/tull/kronofogdar/m fl en rikare källa – potentiellt – att ösa ur än de någonsin tidigare haft i sitt utredande och sin övervakning.

Avgränsningen till Internet innebär dock att jag främst kommer att fokusera på ”dataskydd” istället för ”personlig integritet” i vidare mening. Med vår tids vetenskapliga och tekniska landvinningar följer integritets-problem kring sådant som DNA-testning i olika sammanhang och syften, eller kameror som ”ser” genom kläder, avsedda för bl a säkerhetskontroll på flygplatser. Visserligen kan även dessa integritets-hot i framtiden komma att realiseras via Internet, men för min studie finns redan tillräckligt många problem att behandla vilkas konturer är tydliga. Det saknas anledning att dessutom spekulera kring de risker vi inte riktigt kan urskilja.

Ett annat område som jag avstår från att behandla är sådan information om människor – eventuellt kränkande/skadande – som återfinns på Internet men som har grundlagsskydd enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Många dagstidningar t ex, publicerar helt eller delvis samma material på sina web-platser som i den tryckta upplagan och enligt gällande svensk rätt har båda ”upplagorna” idag samma skydd. Här aktualiseras en viktig diskussion, med stor relevans för personvärnet, om hur yttrandefriheten bäst skyddas. Frågan diskuteras av bl a Mediekommittén (SOU 1997:49) och jag måste av tids- och utrymmesskäl lämna den åt sidan.

Att ämnet ”personlig integritet” är mångfacetterat, ideologiskt kontroversiellt och tidvis tekniskt komplicerat får inte lura oss till passivitet. Att ha/värna sin integritet är ett grundläggande mänskligt behov – ett av flera – och medvetenheten om detta borde genomsyra såväl politiken som all annan samhällelig verksamhet.

Vi kan lika lite avstå från att diskutera och agera i frågor om integritet som vi kan göra det i frågor om ”frihet” eller ”demokrati”. Att sådana termers exakta innebörd är svårfångad och att de problem vi måste tackla är komplicerade gör dem inte mindre viktiga. Med insikten att ”personlig integritet” är ett värde nära besläktat med ”frihet” och ”demokrati” följer också att det inte kan värnas med EN politisk insats, EN rättslig princip eller EN teknisk lösning. Det fordras, för att låna ett uttryck från Cavoukian/Tapscott, ”en mosaik av lösningar” och därtill en beredskap att fortlöpande tänka om, tänka nytt och – särskilt viktigt – tänka tidigt. Att vi nu tycks stå inför så stora och svårlösta integritetsproblem beror delvis på att hela institutioner, lagkomplex och tekniska infrastrukturer hinner byggas upp innan någon på allvar reflekterar djupare över konsekvenserna för personlig integritet.

1.2 Personvärn

En särskild svårighet med integritets-temat i Sverige är rent språklig. Vår term ”integritet” täcker för mycket. Den syftar på privatlivets helgd men också på ”oberoende” och ”självständighet”. (Säger man om t ex en domare att han har integritet är det inte skyddet för hans privata förhållanden som åsyftas.) Juridikprofessorn Peter Seipel har föreslagit att vi, liksom norrmän och danskar, borde tala om ”personvärn” när vi menar ”skydd för privatlivet”. Eftersom jag bedömer att en sådan terminologisk förändring skapar större klarhet övergår jag nu till att använda begreppet personvärn.

En annan svårighet är att innebörden dels ändras över historisk tid, dels skiljer sig en del mellan kulturer i samma tid. I det gamla jordbrukssamhället levde människor fysiskt nära varandra. Många sov i samma rum och arbetade med samma saker på samma plats. För individen var det praktiskt svårt att undandra sig andras blickar och uppmärksamhet. Den sociala kontrollen var oftast (med dagens perspektiv) kvävande stark men samtidigt självklar. Föreställningarna om ”personvärn” präglades av detta.

Med urbaniseringen, den utvecklade industrialismen och en ökande materiell standard ändrades förutsättningarna för personvärn. Det blev möjligt att dra sig undan. I storstaden kunde man gå runt en hel dag utan att bli igenkänd av någon. Lägenheterna blev så stora att t o m barnen kunde få egna rum.

Individen har därtill fått möjlighet att leva i flera, nästan helt sepa-

rerade sociala miljöer. De kan vara t ex familjen, arbetsplatsen, idrottsklubben och det politiska partiet. I dessa miljöer kan man utveckla olika delar av sin personlighet och i åtminstone viss utsträckning välja framtoning, välja ”personlighet”.

Banktjänstemannen, diskret, korrekt och lågmäld på det kvinnodominerade bankkontoret, kan på kvällen förvandlas till en bullrande och skojfrisk ledare för fotbollsklubbens manliga juniorlag. Ytterligare ett par timmar senare kan han glida in genom den anonyma dörren till en av stadens träffpunkter för homosexuella och därmed växla ”personlighet” ännu en gång. Även om den anonymitet som storstaden kan skänka individen också har en baksida – främst i form av isolering och ensamhet – torde ingen längta tillbaka till jordbrukssamhällets tätare, mer kontrollerade livsförhållanden.

Det är heller inte vårt alternativ år 2000. Frågan är snarare om vi vänjer oss vid en utveckling mot i viktiga avseenden svagare personvärn. Flera tecken tyder på att vi lever mer tillgängliga, eller om man så vill mer övervakade, när de nya tekniska systemen integreras i vår vardag. En livlig debatt pågår också om den dialektiska process genom vilken människor formar och formas av det ”nätomspunna” samhället. Hade man för tjugo år sedan frågat medborgarna om de kunde tänka sig att under större delen av sin vakna tid bära en apparat som gjorde det möjligt för andra att följa deras geografiska förflyttningar hade svaret säkert blivit ett bestämt Nej. Idag börjar mobiltelefonen bli var mans egendom. Fördelen att kunna kommunicera med andra varsomhelst, närsomhelst tycks för nästan alla människor uppväga den medföljande försvagningen av personvärnet. Ny teknik är sällan *bara* nyttig eller *bara* hotande. När det är taxichaufförer (som kan utsättas för våld eller hot) eller dementa åldringar som snabbt behöver lokaliseras blir perspektivet på mobiltelefonen ett annat. Att apoteken vill ha mycket information om kunderna – rökare? allergiker? bilförare? etc – för att minska riskerna att de får fel läkemedel är *både* bra och oroande. (Johansson 1998)

Frågorna om hur nya generationer människor lever med/genom nya medier och huruvida detta genererar nya föreställningar om personvärn är komplicerade. De är samtidigt så viktiga att varje diskussion om framtida lösningar förutsätter att deltagarna har en föreställning – åtminstone i vissa grunddrag – om hur de ska besvaras. Min studie kan alltså inte helt förbigå ”mjuka” aspekter på personvärn, dvs de psykologiska och sociologiska perspektiven, men gör självfallet inga anspråk på att här vara heltäckande eller djuplodande. Jag inskränker

mig till att kort diskutera några, som jag uppfattar det, grundläggande teman i kapitel 6.

Att det finns fler komplikationer kring personvärnet än de hittills nämnda kommer att framgå.

1.3 Uppläggning

Det finns inga självklara tematiska grepp om problemkomplexet ”personvärn & internet”. Jag har valt, främst därför att det mesta av litteraturen är skriven enligt det mönstret, att strukturera studien enligt följande:

Kapitel 2. Risker och hotbilder – en översikt över deras utveckling under dryga 30 år. Hur ser de ut idag?

Kapitel 3. Det rättsliga perspektivet: internationell praktik och debatt. Vilken typ av lagar om personvärn – av relevans för Internet – finns i länder jämförbara med Sverige? Hur förändras/utvecklas reglerna? EU:s arbete. Finns tecken till konvergens, dvs en samsyn som på sikt pekar fram mot ett mer omfattande internationellt regelverk?

Kapitel 4. Det tekniska perspektivet. Svensk och internationell diskussion om PET – personvärnsstärkande tekniker. Tillämpningsområden för kryptering, agentprogram. Kort referat av den internationella debatten om hur & när personvärnsproblem har tekniska lösningar.

Kapitel 5. Självreglering. I vilken utsträckning kan eller bör personvärn utformas på mer ideell grund eller i förlitande på marknadsmekanismer? Främst internationella erfarenheter.

Kapitel 6. Den föränderliga människan. Vilket sorts personvärn kommer nästa generation att vilja ha? Diskussion på några teman hämtade ur aktuell litteratur.

Kapitel 7. Sammanfattning och slutsatser.

Denna uppdelning kan synas funktionell, men som snart ska framgå överlappar såväl problem som lösningar varandra. Agentprogrammen, för att nämna ett exempel, utgör såväl hot mot personvärnet som en möjlighet att stärka det.

Av den som vill tackla personvärnsproblem i vår tid krävs en utvecklad förmåga att hålla många bollar i luften.

Kapitel 2

Hotbilden förr och nu

2.1 Bakgrund

När debatten om ”personlig integritet” tog fart i Sverige för 30 år sedan uppfattades datorn i första hand som en maktfaktor. Faran bestod inte i att den ene medborgaren kunde skada den andre utan att samhällets starkaste aktörer – främst staten men också storföretagen – skulle växa sig ännu starkare på alla medborgares bekostnad. Plötsligt uppstod en stark oro för att samhället, med en ökande användning av automatisk databehandling, skulle bli allt mindre demokratiskt.

Åsikten hade spritt sig till Sverige från USA, där den 1965 formulerades slagkraftigt av Alan Westin i boken ”Privacy and Freedom”. Juristen Westin hade lett ett stort forskningsprojekt om framväxande integritetshotande tekniker. Till att börja med stod sådant som hemlig avlyssning och lögndetektorer i centrum för Westins intresse, men han fick snart upp ögonen för databaser och personregister – och det var den delen av studien som väckte nationell och småningom internationell uppmärksamhet. Den svenska utredning som fick till uppgift att söka lösningar på problemet, Offentlighets- och sekretesslagstiftningskommittén, sammanfattade den svenska debatten 1969-1972:

”Insamlingen av uppgifter om människor, deras attityder och levnadsförhållanden kritiserades såsom ägnad att alltför mycket öka myndigheternas makt och möjligheter att styra enskildas handlingar. I informationsbehandlingens förlängning anades konturerna av en oangriplig polisstat med en absolut effektiv och till sina verkningar omänsklig förvaltning.” (SOU 1972:47, sid 41-42)

Varningarna för Storebrorssamhället – syftande på den allseende, allvetande totalitära staten i George Orwells roman ”1984” – varierades under de följande 15 åren i artiklar, debattböcker och offentliga utredningar. Kritik mot den datoriserade statsmakten levererades mest från höger, där man associerade till kommunistiska och andra centralstyrda samhällen, men också tidvis från vänster, enligt den marxistiska uppfattningen om staten som den härskande klassens redskap. Ska något

inlägg särskilt lyftas fram bör det bli boken ”Datamakt” från 1975 av den folkpartiets riksdagsledamot Kerstin Anér. Där jämställs datorn med ömsom en spindel, ömsom en drake. Datorn är ”stark” och samtidigt ”ogenomskinlig”. Anér tycks mena att datorn lockar fram och förstärker kontrollambitioner hos såväl statliga ämbetsmän som hos IBM och andra storföretag.

Tongångarna förblev desamma till långt in på 1980-talet. En bra illustration är debatten om en alternativ folk- och bostadsräkning, FOBALT, 1983. Avsikten var att genomföra delar av folkräkningen genom samkörning av redan existerande statliga personregister. Medborgarna skulle därmed slippa fylla i blanketter och staten skulle spara många miljoner i minskade administrationskostnader.

Protesterna blev våldsamma. Samkörning av personregister för att skapa större FoB-register innebär att ”myndigheterna går bakom ryggen på folk” hävdade den statlige utredaren vid Datainspektionen Rabbe Wrede. Då urholkas förtroendet för myndigheterna vilket är ”ett hot mot demokratin” (SvD 830725). Wrede fick medhåll av sin chef Jan Freese. FOBALT blev politiskt omöjligt och stoppades den gången, medan ett likadant förfarande kunde realiseras tolv år senare utan någon offentlig debatt överhuvudtaget. (Se SOU 1995:74 och prop. 1995/96:90.)

Fram till mitten av 80-talet dominerades diskussionerna av motsättningen mellan å ena sidan myndigheternas behov av information – för t ex samhällsplanering och brottsbekämpning – och å den andra medborgarnas behov av skydd för privatlivet. I februari 1986 avslöjade Dagens Nyheter omfattningen av och inriktningen på det sociologiska forskningsprojektet Metropolit. Där insamlades fortlöpande under 20 år stora mängder data, såväl triviala uppgifter som känsliga, om 15 000 stockholmare födda 1953. Dessa personer informerades aldrig om saken. DN:s artiklar resulterade i en proteststorm och Metropolit blev Sveriges sista ”Storebrorsskandal”. (Olsson 1996)

Det paradoxala är alltså att personvärns-frågan, både i politiken och massmedia, försvann från dagordningen vid samma tid som den tekniska utvecklingen började göra den alltmer relevant för medborgarna. År 2000 finns det betydligt starkare skäl att varna för ”Storebror” än för 15 år sedan, då larmrapporterna och ”registerskandalerna” avlöste varandra.

2.2 Storebror – Polis och säkerhetstjänst

Polisen har under 90-talet givits ökade befogenheter att åsiktsregistrera, kameraövervaka och teleavlyssna, och detta i en tid då de tekniska hjälpmedlen för sådan spaning har utvecklats och förfinats i snabb takt. Regeringen (s) har sedan 1998 också drivit krav på att legalisera hemlig avlyssning, buggning (se SOU 1998:46), men på just den punkten har motståndet från övriga riksdagspartier varit starkt och någon proposition har ännu inte (hösten -99) förelagts riksdagen. Utvecklingen mot ökade polisiära och säkerhetspolisiära befogenheter måste ses mot bakgrund av Sveriges medlemsskap i EU och samarbetet inom ramen för Europol och Schengenavtalet. I dominerande EU-länder som Tyskland, Storbritannien och Frankrike har polisen länge haft de vidare befogenheter som på senare år införts i Sverige. (Däremot skiljer sig länderna åt beträffande rättssäkerhetsgarantier och formerna för politisk-demokratisk kontroll. I Tyskland t ex, ska den person vars telefon avlyssnas alltid i efterhand underrättas om att så har skett.)

Paradexemplet på Storebrors framsteg är utan tvekan den sorts avlyssningsverksamhet som ett stort antal forskare, fristående analytiker och journalister sammanfattar med begreppet ECHELON. Om ECHELON har sagts och rapporterats mycket, men av lätt insedda skäl finns här källkritiska problem.

Regeringar och säkerhetstjänster i de länder som utpekas som ansvariga för avlyssningsverksamheten (USA, Storbritannien, Kanada, Australien och Nya Zeeland) vägrar kommentera flertalet påståenden. De dementerar bara i vissa delar, framförallt att de skulle avlyssna det egna landets medborgare på annat sätt än som medges i lag. Varje mer detaljerad redogörelse för ”projektet ECHELON” måste därmed kompletteras med analyser av olika källors trovärdighet och ofta förses med reservationer. Någon sådan redogörelse finns inte utrymme för i denna rapport.

Författarens (Anders R Olsson) bedömning är emellertid att man på basis av informationen i de öppna källorna vågar påstå åtminstone följande: Det pågår en kontinuerlig avlyssning av tele- och datakommunikation i stora delar av världen. Som spindel i nätet fungerar den amerikanska säkerhetstjänsten National Security Agency, NSA. Med hjälp av myndigheter och teleföretag över hela världen kan NSA komma över väldiga mängder tele- och datakommunicerad information och mata den genom superdatorer som är programmerade att ”slå larm” för vissa ord, koder eller egenskaper i kommunicerade budskap. Tekniken används

för såväl vanliga telefonsamtal som fax och e-post. (Se bl a Davies 1999. ACLU, American Civil Liberties Union har fyllig information på: http://www.aclu.org/echelonwatch/index.html. Där finns också länkar till de uppmärksammade rapporterna om ECHELON till EU-parlamentet.)

Utan att kunna bedöma effektiviteten i sådan övervakning av allmänt tillgängliga kommunikationsnät måste man säga att verksamheten är djupt obehaglig ur personvärnssynpunkt. Att statliga organ går från avlyssning, godkänd av domstol, av misstänkt brottsliga individer till generell avlyssning av alla medborgare är ett principiellt allvarligt steg. Det finns f ö uppgifter om att avancerad övervakning av tele- och datakommunikation förbereds – med projektnamnet ENFOPOL – inom ramen för det europeiska polissamarbetet. (Se bl a Tallmo 1999.)

Några officiella bekräftelser av sådana uppgifter föreligger inte, och med tanke på att de handlar om en verksamhet som ännu inte har påbörjats är det särskilt svårt att bedöma sanningshalten. (Den intresserade läsaren söker lämpligen på ENFOPOL på Internet och gör en egen värdering av tillförlitligheten i olika utsagor och dokument.)

Ett annat modernt Storebrorsproblem utgör de övervakningskameror för polisiärt bruk som blivit allt vanligare under 1990-talet …

2.3 Lillebror

Framtidens personvärn måste konstrueras med utgångspunkt från att datorer är var mans redskap, inte längre bara de stora samhällsaktörernas. Datorer och datakommunikation integreras allt djupare i såväl individers som institutioners vardagliga verksamhet. Informationsflöden av många slag, bl a om människor, blir med Internet tillgängliga för vem som helst.

Begreppet Lillebror får i denna rapport stå för all civil, icke-kommersiell, personvärnshotande uppgiftshantering. Även denna gränsdragning är självfallet problematisk. De personuppgifter som hanteras ”civilt” eller ”kommersiellt” är vanligen tillgängliga för polis/säkerhetstjänst också – om inte direkt så vart fall genom domstolsbeslut. Förflyttar man sig med mobiltelefonen påslagen registreras de geografiska rörelserna hos teleoperatören. Det blir allt vanligare att polisen i brottsutredningar utnyttjar teleoperatörernas information om var en viss telefon har använts vid en viss tidpunkt.

Någon given skiljelinje mellan kommersiell och icke-kommersiell verksamhet finns heller inte. (Är t ex registrering av bilister vid vägtul-

lar – avsedda att finansiera vägbyggen – ”kommersiellt”? Därtill kommer att åtskillig hantering som uppenbarligen är ”civil”, låt säga inom en rockstjärnas fan-club, gärna utnyttjas av kommersiella aktörer, i detta exempel skivbolag och arrangörer av rock-konserter.) Likväl skiljer sig de utpräglat kommersiella aktörerna så markant både vad gäller målsättning med databehandlingen, ekonomiska resurser och arbetsmetoder att de förtjänar ett eget avsnitt.

Även kameraövervakning är på väg att bli ett ”lillebrorsproblem”. Att koppla ihop videokameran med datorn och sända direkt på nätet är redan praktiskt möjligt. I Aftonbladets IT-bilaga (augusti -99) publiceras adresserna till 80 web-kameror som sänder ständigt nya stillbilder eller rörliga bilder från platser som Paris, Montreal, Gibraltar, Ålesund och Bogotá. Web-kameror kan för övrigt vara ett ”kommersiellt” personvärnsproblem, t ex när restauranger ”sänder direkt” för att kunderna ska kunna se hur etablissemanget ser ut och få reda på om det finns några lediga bord.

Satellitburna kameror ser ut att kunna bli ytterligare ett problem. ”*Spionbilder säljs på webben*” rapporterar Dagens Nyheter 991202. Satellitbilder med bildupplösningskapacitet på en meter saluförs via Internet.

För illasinnad ryktesspridning är Internet självfallet ett bra redskap i vissa avseenden. A kan skada B genom att sprida kränkande påståenden via en hemsida eller e-post, men kränkningen kan lika gärna bestå i att A sprider meddelanden – rasistiska eller på annat sätt obehagliga/provocerande – undertecknade med B:s namn. Ryktesspridaren behöver inte blotta sig själv i det ögonblick som kränkande uppgifter ”offentliggörs”, dvs läggs ut på nätet. (Att den vanligaste platsen för vanligt klotter är låsbara offentliga toaletter beror naturligtvis på att klottraren vill skydda sin identitet.) I praktiken är det dock inte lätt att sopa igen spåren efter sig i elektroniska miljöer. (Se bl a Ilshammar/Larsmo 1999, Svärdcrona 1999.) Om en person i Sverige sprider nedsättande uppgifter via Internet är brottsbalkens regler om förtal tilllämpliga.

Det faktum att alla utom de mest avancerade nätanvändarna lämnar elektroniska spår efter sig är ur personvärnsynpunkt både positivt och negativt. Vetskapen om att källan kan spåras har säkert en återhållande effekt på potentiella missdådare, men för alla andra utgör spåren problem eller åtminstone obehag. Att skicka meddelanden med e-post kan jämställas med att skicka dem på vykort – ett stort antal personer som administrerar e-posthanteringen kan i prak-

tiken läsa breven. Därtill finns risken, i praktiken liten men dock en realitet, att någon utomstående ”hackar” sig in i de servrar som används längs e-brevets väg.

Även den som ”surfar” på Internet lämnar spår. Det är bl a uppgifter om vilken typ av dator man har, vilka program man använder för att ta sig fram på nätet, vilken ISP (Internet Service Provider) man är kund hos och vid vilken tidpunkt man besökte en viss web-plats. (En utförligare beskrivning av dessa spår finns på: http://users.westnet.gr/~cgian/spy.htm) Informationen lämnas automatiskt, som ett visitkort, vid varje webplats man besöker.

Webplatserna kan dock ”begära” mer information om surfaren, t ex med hjälp av cookies. En cookie är en liten mängd information, kodad till en datasträng, som kan överföras från en hemsida på Internet till hårddisken på surfarens dator. Tekniken används i praktiken oftast i kommersiellt syfte. Man kan jämföra med att surfaren går runt i Gallerians butiker. I musikaffären tittar han på soul och Verdioperor. När han går ur butiken klistras diskret en liten lapp (en cookie) på hans rygg: ”soul, Verdi”. Vid besök i nästa musikaffär – eller samma affär dagen efter – kommer utbudet från Atlantic Records och drivor av italiensk opera att ligga läckert exponerat för just denna kund. I virtuella butiker kan man anpassa utbudet individuellt för varje besökare, bara man känner vederbörandes preferenser. Den motorintresserade surfaren skulle alltså möta mer reklam för Teknikens Värld, Goodyear och Audi, medan den idrottsintresserade skulle bombarderas med erbjudanden från Nike och Eurosport.

Cookies har många tillämpningar. De kan öppna en hemsida som annars kräver lösenord, vilket gör surfandet smidigare, men de kan också läsas av andra ”där ute” i syften som man inte känner till. Att Internet överhuvudtaget möjliggör för ägaren till en webplats (A) att använda surfaren B:s dator utan att B ens får kännedom om saken utgör onekligen ett personvärns-problem i sig. (Se vidare om agent-program i kap 4.)

Integritetsskydd har heller aldrig på något stadium funnits med i konstruerandet av Internet. Det världsomspännande nätverket har ”växt fram” genom en serie programtekniska upptäckter och bedrifter. ”Ett laboratorieförsök som rymde” lär någon integritetsexpert ha kallat det.

Nätanvändaren lockas också av ständigt nya finesser som roar eller underlättar, men som ofta skapar ytterligare sprickor i personvärnet. Med programmet ICQ (utläses I seek You – jag söker dig) i datorn kan

X få reda på om Y för ögonblicket är uppkopplad – och skicka ett meddelande. Det är skojigt om X och Y är kamrater, men kanske inte lika skojigt om relationen är en annan.

2.4 Den utsatte konsumenten

Personvärnsproblematiken kom att vidgas under 1980-talet i takt med att allt fler företag och privatpersoner började utnyttja informationsteknologin i allt fler sammanhang. Så hamnade t ex konsumenten i fokus för en ny personvärnsdebatt när användare av kredit- och betalkort började avsätta alltfler spår i databaser hos företag som VISA och Master Card.

Gårdagens kontantbaserade ekonomi erbjöd en hög grad av anonymitet. Idag har individen, till skillnad mot igår, alla möjligheter att dölja sina sexuella snedsteg, men så fort han/hon tankar bilen med kontokortet eller ringer tandläkaren med mobiltelefonen registreras detaljerna i databanker.

Människors köp- och konsumtionsbeteende kunde under 80-talet kartläggas med allt större precision, till glädje främst för de direktreklamföretag som nu började ”vaska fram” de mest lovande potentiella kunderna till producenter av olika varor och tjänster. USA har hela tiden varit ledande i utvecklingen mot effektivare exploatering av kundinformation, och det var också där som personvärnsaspekterna på hanteringen först började diskuteras. (Larson 1992)

På 90-talet har kortanvändningen ökat ytterligare. Varje större detaljhandelskedja har eget kort och oavsett om det är mat, bensin eller biobiljetter man köper med dem så sparas uppgifter om individens konsumtion någonstans. ”*Kreditkortet, mer än ID-kortet, orsakar oss personvärnsförlusterna*” skriver Manuel Castells. (1997)

Datorer i nätverk, tillgängliga för flertalet medborgare, ändrar förutsättningarna för detaljhandeln – liksom för nästan all kommersiell verksamhet. Penningströmmarna övergår i elektronisk form. Allt fler av de tjänster och produkter (text, bilder, musik, spel, datorprogram m m) som kan ges digital form säljs och förmedlas via nätverk. Den elektroniska handeln har redan börjat revolutionera kommersiella processer och företag i praktiskt taget alla branscher är mitt uppe i en kapplöpning om att etablera sig först & bäst på Nätet. Det är full realistiskt att i en nära framtid se hur köpare med hjälp av s k agentprogram automatiskt söker fram en produkt med önskade egenskaper, t ex en viss sorts dator

till lågt pris, beställer och betalar för den i en helt automatisk process. (Se vidare kap 4) Flertalet analytiker hävdar att de förändringar i ekonomins funktionssätt vi nu står inför blir så djupa och omfattande att de får avsevärda sociala och kulturella konsekvenser, dvs ändrar det sätt på vilket människor lever och tänker. (Se bl a Toffler 1997, Tapscott 1996.)

Förändringarna kan beskrivas i olika termer och på olika nivåer. En tendens är att man går från massmarknad till ”atomiserad” marknad. Exemplet ovan med cookies utgör en illustration. Många företag hoppas att med interaktiva kanaler kunna upprätta ”relationer” med kunder. De ”trogna” köparna ska få bättre information, lojalitets-poäng som ger lägre priser eller belöningar av annat slag.

En viktig förklaring till ”atomiseringen” är att man börjar kunna skräddarsy alltfler produkter. Istället för att övertala stora mängder konsumenter att köpa identiskt lika varor – ofta svårt därför att människors önskemål/behov kan variera åtskilligt – kan kunden få sina individuella önskemål tillgodosedda. (Samarajiva 1998) Med en smidig och i hög grad automatiserad tillverkningsprocess kan bilar, möbler, hemelektronik och leksaker produceras enligt konsumentens önskemål. CD-skivan kan rymma just de musikstycken han/hon vill ha, chipsen i påsen kan ges önskvärd sälta, osv.

Denna utveckling genererar kraftigt ökande behov hos företagen av kunskap om såväl kunder – för att tillmötesgå deras alltmer detaljerade önskemål – som potentiella kunder. Om de förra måste man skaffa alltmer individanknuten kunskap, till de senare måste kunna sända ut reklambudskap med ökad precision.

”*Med den allt större bandbredden in i hemmen i form av kabel-TV och andra trådbaserade system, liksom direktsändande satelliter och annan trådlös kommunikation, blir de alltmer konkurrensutsatta medieföretagen oförmögna att erbjuda annonsörerna en masspublik*.” (Samarajiva 1998, egen övers.)

Den alltmer splittrade mediekonsumtionen stärker ytterligare företagens behov av att ”få syn” på sina potentiella kunder och finna vägar att nå just dem med reklambudskapet. Enbart i USA satsar företagen idag motsvarande 250 miljarder kr på direktreklam. Med manuell utdelning kostar där varje reklamblad ca 85 öre/st. Att använda e-post skulle bli så mycket billigare att företagen med oförändrad budget kunde skicka varje amerikansk konsument 11 000 reklambudskap om dagen. (Hurley 1999)

Detta illustrerar företagens möjligheter – men också deras problem.

Reklam via e-post kommer inte att fungera. I USA har delstaterna Kalifornien, Washington och Nevada redan lagstiftat mot sådan SPAM, dvs oönskad e-post för kommersiella syften. (Lov&Data nr 58, juni 1999) Den verkliga bristvaran, ur företagens synpunkt, är konsumentens uppmärksamhet. Att dränka honom/henne i reklambudskap får inte önskad effekt eftersom budskapen kastas olästa. Företagens strategi går därför ut på att 1) mycket noggrannare än förr ringa in den verkligt lovande målgruppen och sedan 2) koncentrera företagets resurser på att verkligen nå fram till dessa utvalda. Både 1) och 2) rymmer problem ur personvärnssynpunkt.

Med den e-handel som nu börjar skjuta fart (snabbast i USA) samlar företagen allt mer och allt intimare kunskap om sina kunder. De tenderar att suga åt sig all kundinformation de kommer över i hopp om att bättre kunna urskilja människors egenskaper/önskemål. Ofta ter det sig oskyldigt – man vill hitta barnfamiljer att sälja blöjor till och bilintresserade att sälja motortidningar till – men någonstans börjar det bli känsligt. Deodoranttillverkaren vill veta vilka som har armsvett. Porrproducenten vill ha information om människors sexuella preferenser. Tidningar, förlag, politiska partier och lobbyorganisationer är på jakt efter individers intressen, åsikter och värderingar.

Vad beträffar sådana data som på ett mer uppenbart sätt är känsliga ur personvärnssynpunkt ter sig problemen tydliga – vilket inte betyder att de skulle vara lätta att lösa.

Litteraturens överflyttande från pappers- till nätmiljön tycks visserligen ge stora fördelar i form av större utbud, högre tillgänglighet och lägre pris – men också stora avbräck vad personvärnet beträffar. Hur många av oss slinker inte in i bokhandeln när vi får några minuter över för att bläddra i böcker? Det kan vi göra diskret och anonymt. När handeln med text & bild flyttar till Nätet kommer vi inte att kunna ”bläddra” i något utan att först uppge namn och kontokortsnummer. För att skydda copyright-innehavarna måste litterära verk som lämnas ut via Nätet förses med individuell märkning. (Krypteringsteknik för detta finns redan.) Man får all världens böcker att välja bland – men läsvanorna registreras i ett ECMS, Electronic Copyright Management System.

Det finns också exempel på att företag (och myndigheter) försöker utnyttja till synes harmlös och/eller irrelevant information för sina syften. Det komplicerar personvärns-problemet ytterligare.2.4.1 Data mining

”*Kreditkortsföretaget visste att Jennifer och John skulle skiljas – tre veckor innan de själva visste det. Båda hade allt oftare tagit ut allt större summor från sina konton. Beteendet matchade statistiken över havererade äktenskap och gav prognosen skilsmässa. Bäst att vara uppmärksam.*

Skrämmande? Hursomhelst redan en verklighet i ett USA som alltid skrutit med att sätta individens frihet i första rummet.” (Willebrand 1999). Tekniken att ringa in ”typiska” människor genom analyser av till synes irrelevanta data har många tillämpningar, såväl kommersiella som polisiära. De brukar sammanfattas som ”profilering” och går normalt ut på att analysera kända data om, för att ta ett exempel, kända terrorister för att lättare identifiera de ännu icke kända. (se bl a Cavoukian 1998) Visar data om kända terrorister att en oproportionerligt stor andel av dem – jämfört med befolkningen som helhet – har universitetsstudier i sociologi bakom sig samt har bytt arbetsgivare minst tre gånger på fem år kan alla medborgare som uppfyller båda kriterierna väljas ut för närmare granskning. En annan möjlighet är att flygbolagens bokningssystem förses med ”larmklockor” så att bagage tillhörande individer ur den ”potentiellt farliga” gruppen undersöks särskilt noggrant.

Grundidén är i själva verket gammal, med datormått mätt. Amerikanska skattemyndigheter började redan på 60-talet teckna ”profiler” av skattefuskare för att med datorernas hjälp sortera ut de självdeklarationer som hade vissa, var för sig oskyldiga kännetecken för närmare studium. (På 1990-talet har även svenska skattemyndigheter börjat tillämpa den tekniken.)

”Profilering” kan principiellt inordnas under det vidare begreppet ”Data mining”, ett redskap som utvecklades inom AI-forskningen under 70- och 80-talen. (AI = Artificiell Intelligens) ”Data mining” är enkelt uttryckt en teknik som används för att utvinna dold eller tidigare okänd information ur stora databaser. Lyckad ”data mining” gör det möjligt att upptäcka mönster i eller nya samband mellan data. Enligt Cavoukian kan fem olika sorters information utvinnas med hjälp av Data mining.

1. Samband mellan enstaka händelser. En livsmedelsbutik kan upptäcka t ex att en kund som köper chips i 65 procent av fallen också köper Coca Cola, om man inte erbjuder rabatt vid köp av båda varorna – då Coca Cola köps i 85 procent av fallen.

2. Samband mellan händelser över tid. Av de som köper ett hus kom-

mer, kan en studie visa, 45 procent att köpa en ny spis inom en månad och 60 procent att köpa ett nytt kylskåp inom två veckor.

3. Klassificering/profilering. Ett företag kan kartlägga t ex hur de kunder beter sig som man är på väg att förlora, så att särskilda rabatter eller specialerbjudanden i tid kan riktas till just dem. Med tiden kan företaget också öka sin kunskap om vilka rabatter som ”fungerar” på olika typer av kunder, så att man inte offrar mer pengar än nödvändigt för att behålla en kund.

4. ”Hopklumpning” av data (eng: clustering), upptäckt av samband som ingen upptäckt därför att ingen letat efter dem. Tekniken kan användas för att hitta så skilda saker som svaga punkter i en tillverkningsprocess eller avgränsade grupper av individer som är särskilt mottagliga för reklambudskap om en ny sorts kreditkort.

5. Förutsägelser. Även om informationstyperna 1-4 ovan alla kan läggas till grund för förutsägelser, t ex huruvida en kund kommer att förnya ett abonnemang eller inte, avses här förutsägelser av mer specifikt slag. Det kan handla om att förutse, baserat på analyser av historiska data, förändringar i en aktiekurs eller i en försäljningsvolym.

”Data mining” ger således företag incitament att samla på sig så mycket information som möjligt. Man vet aldrig var den kunskap ligger dold som kan ge ett litet övertag i konkurrensen. Hellre några gigabyte kunddata för mycket än för lite. Enligt Cavoukian beräknas minst hälften av företagen på tidskriften Fortunes lista över världens 1 000 största företag att använda ”Data mining” år 2000.

Fenomenet öppnar för en rad svåra frågor.

Hur allvarligt ska man se på denna hantering? Ska jag känna mig kränkt över att ICA efter analys av mitt köpbeteende betraktar mig som särskilt mottaglig för reklam om olivolja eller tournedos? (Om produkterna är t ex porrtidningar, kondomer, sprit eller apoteksvaror blir svaret mera givet.) Är jag utsatt för manipulation när butiken ger mig särskilda rabatterbjudanden just när jag funderar på att sluta handla där?

Eller ligger risken mindre i den rent kommersiella användningen av persondata och mer på det samhälleliga planet? Kommer t ex säkerhetspolisen att använda samma data enligt sin egen logik? Den kanske

kan bevisa att individer som konsumerar stora mängder linser och grönt te, alternativt köper både tunga kängor och läderjackor med nitar, statistiskt sett oftare har extrema politiska uppfattningar och därför kontinuerligt bör granskas.

Om detta ter sig stötande, hur ska man se på användningen av IBM:s Data-mining-system FAMS (Fraud and Abuse Management System)?

”*…Empire Blue Cross and Blue Shield, ett sjukförsäkringsföretag i New York, avslöjade en läkare som skickat företaget räkningar på 1,4 miljoner dollar för luftrörsoperationer som aldrig hade utförts. Programmet lade märke till att läkaren påstod sig utföra en operation i veckan på samma patienter, och markerade förhållandet som ´ovanligt´ därför att luftrörsoperationer normalt bara utförs en eller två gånger under en patients livstid.*” (Brodley/Lane/Stough 1999)

Det är svårt att finna argument mot sådan användning av Data mining-tekniken, och frågan tycks bli var/hur man ska dra gränsen. Om risken är att polis, skattemyndigheter, kronofogdar eller privata företag drar långtgående slutsatser baserat på ”Data mining” och som en följd därav utsätter vissa kategorier människor för särskild kontroll – utan annan grund för brottsmisstanke – hur kränkande är det? Beror svaret bara på vilka metoder staten/företagen då använder? Om kontrollen ÄR kränkande – är problemet då de väldiga databaserna? ”Data mining”-tekniken som sådan? Eller de normer som ligger till grund för myndigheternas/företagens agerande?

2.4.2 Smarta tjänster

Med ”smarta tjänster” på Nätet, som att överlåta åt agentprogram som vet ”allt” om oss söka fram den information konsumenten behöver men inte har tid/lust att leta efter själv, blottar han/hon sig ytterligare. (En avgörande fråga blir vem som kontrollerar sådana program, se vidare kap 4.)

De nätburna ”smarta” tjänsterna blir allt fler. Användaren kan få alltmera utfört automatiskt:

- köp eller försäljning av varor/tjänster,
- information om nya webadresser, tidningsartiklar eller diskussionsinlägg vars innehåll kan vara intressant för honom/henne,
- utväxling av koder så att han/hon fritt kan surfa bland webplatser som annars kräver lösenord,

- meddelanden om att det kommit nya versioner av de program han/hon använder.

Detta är bara början. Utan tvekan kan vi som medborgare och konsumenter ha nytta av tjänster som dessa. De är oftast gratis i pengar räknat, men priset kan bli desto högre i form av personvärnsförluster. Det som görs automatiskt ”för A” görs oftast hos B, och det primära syftet är inte att gynna A. Forskaren vid SICS (Swedish Institute for Computer Science) Sverker Janson pekar på Netscape som exempel.

”– För att jag ska få hjälp att hitta/surfa till fler webplatser som intresserar mig finns en funktion som kallas ”What’s Related”.

Om jag begär ”What’s Related”-information skickas den nuvarande och de tre följande adresserna man besöker till Netscape. Detta är ”default”. Man kan stänga av tjänsten, eller utöka den så att alla adresser skickas. Funktionen kan i bästa fall hjälpa mig att surfa ”smartare”. Samtidigt får Netscape en väldig mängd personlig information om mig och mina intressen.

– Jag vill inte demonisera Netscape och andra aktörer – som t ex ICQ, som ser exakt när jag använder min dator och vilka vänner jag har. De försöker bara behålla kontrollen över sin tjänst för att därmed tjäna pengar.

– Men skulle vi vilja att ett företag videofilmande vartenda steg vi tar för att kunna tipsa oss om bättre ställen att gå till, även om vi blev lovade att banden inte användes till annat? Knappast.” (DN 990624)

Tidvis har det, främst i USA, flammat upp protester mot de stora IT-företagens agerande. Microsoft har tidigare haft programfunktioner som inneburit att information om användarna automatiskt skickats till företaget över nätet, men efter omfattande kritik ändrade man dessa program. Sverker Jansson:

”– En viss kunskapsöverföring sker dock fortfarande. Väljer man att utnyttja en tjänst som ”Windows Critical Update Notification” kollas fortlöpande om det har kommit någon förändrad version av programmet. I samband med uppdatering får användaren en fråga om han/hon går med på en inspektion av redan installerade program. Informationen sänds nu inte till Microsoft utan ”kontrollen” sker i klientdatorn.

– Faktum är dock att hela proceduren ger Microsoft en god bild av vilka versioner av deras program som finns installerade hos kunderna och en ungefärlig bild av datoranvändningen.

Det är fullt begripliga kommersiella motiv som främst driver på utveck-

lingen, påpekar Sverker Janson. Tillverkaren av ett datorprogram har ett starkt behov av att veta hur många användarna är, vilka funktioner i programmet de utnyttjar och vilka problem de har. Med sådana kunskaper kan tillverkaren se både hur programmet bör förbättras och hur det kan marknadsföras effektivare." (DN 990624)

2.5 Riskernas mångfald

Att allt fler uppgifter – av alla tänkbara slag – om människor lagras i datorer och kommuniceras i nät är uppenbart. Det ser ut att vara den oundvikliga följden av ett IT-samhälle i vilket vi arbetar, umgås, köper och konsumerar på distans och där vi överhuvudtaget vill få alltmer att hända "automatiskt" eller som ett resultat av några knapptryckningar.

Hur kommer dessa uppgifter att användas? Varningsropen för att de kan brukas i olämpliga, eller åtminstone kontroversiella syften blir allt vanligare. Det är lätt att säga att vi ska göra en avvägning från fall till fall, men avvägningarna är besvärliga eftersom fördelar och nackdelar inte kan vägas med samma mått – det råder inte alltid konsensus om vad som egentligen är nackdel respektive fördel. Genom att via Nätet förse andra aktörer med uppgifter om oss själva kan vi tjäna tid eller pengar, men så länge vi inte kan säga mer om riskerna har vi ett dilemma: *Vilken* information kommer i fel händer? *Vems/vilkas* händer? *När* inträffar det? *Hur* används den då?

Kapitel 3

Lagstiftning – den klassiska metoden

3.1 Ska vi alls lagstifta?

Med Internets framväxt fick en närmast utopisk idé-strömning – en del skulle beteckna den som nyliberal, andra som anarkistisk – luft under vingarna. Dess grundtanke brukar ibland sammanfattas med slagordet ”Information ska vara fri!” En av initiativtagarna till Electronic Frontier Foundation, EFF, den kanske mest uppmärksammade lobbyinggruppen i USA, heter John Perry Barlow. Han har sagt om ”cyberspace”:

”Vi arbetar målmedvetet på att skapa en plats som i grunden är omöjlig att regera och det går ganska bra för oss.” (citerat ur Wallin 1994, sid 51, egen översättning).

Föreställningar av det slaget förefaller 1999 att vara på tillbakagång. Dels torde de flesta nu vara överens om att en plats som inte regeras blir ett paradis för de starka och ett helvete för de svaga. Dels är nu näringslivet och politiken på väg in i ”cyberspace” och då släpas utan tvekan advokaterna, poliserna och domstolarna med. I den mån ”cyberspace” alls kan beskrivas som en ”plats” så är frågan inte *om* den ska regeras utan *hur*.

Den frågan är dock desto mer svårbesvarad. Om risken för några år sedan tycktes vara att det fanns för få eller otillräckliga lagar i ”cyberspace” kan faran snart mycket väl vara den motsatta – för många, för krångliga eller för restriktiva regler. Många behjärtansvärda motiv kan åberopas för hård eller omfattande lagstiftning – motiv som handlar om personvärn, upphovsrätt eller behoven att stoppa t ex barnpornografi eller rasistisk propaganda. Effekten av en överreglering kan bli negativ på två sätt:

– Alltför hårda/rigida regler om t ex hantering av personuppgifter kan vara skadlig för såväl demokratin (genom att de inskränker yttrandefriheten och hämmar medborgarnas kunskapsuppbyggnad) som den

ekonomiska utvecklingen (genom att stå i vägen för nya affärs- och marknadsföringsidéer).

– Alltför många eller för hårda regler kan också försvaga tilltron till statens möjligheter/ambitioner att kontrollera efterlevnaden. Den svenska datalag som skrevs 1973 med utgångspunkt från att datorn var ett exklusivt redskap, förbehållet staten och storföretagen, fick med utvecklandet/spridningen av små, billiga datorer allt märkligare effekter och betraktades med allt större skepsis. I sitt slutbetänkande 1993 uppskattade Datalagsutredningen att det fanns mellan 500 000 och 1 000 000 personregister i Datalagens mening, men konstaterade samtidigt att Datainspektionen sedan tillkomsten 1974 bara hade gett tillstånd till – eller utfärdat licens för – sammanlagt 50 000 register. (SOU 1993:10) Uppenbarligen fann en överväldigande majoritet bland datoranvändarna lagen så orimlig att de helt enkelt ignorerade den. De ansökte inte om statligt tillstånd för skriva resultatlistor från idrottstävlingar eller förteckningar över rockstjärnor. Såväl lagens som Datainspektionens trovärdighet tog skada av detta. Problemet har med införandet av Personuppgiftslagen, PUL, inte blivit mindre. (Se vidare avsnitt 3.5)

3.2 De första lagarna

När den moderna integritetsdebatten tog fart i slutet på 60-talet uppfattades datorn som både värdefull och farlig. Den var, liksom bilen eller flygplanet, avsedd att användas i högst lovvärda syften men risker fanns uppenbarligen också att den brukades slarvigt eller illvilligt, dvs så att människor skadades. Väg- och flygtrafiken hade redan sina fungerande regelverk. Slutsatsen att dator-användning borde lagregleras låg nära till hands. (se SOU 1972:47)

Den tyska delstaten Hessen antog i oktober 1970 den första ”datalagen” i världen. I denna Datenschutzgesetz reglerades inte mer än delstatens egna personregister – då uppfattades också främst myndigheternas hantering av personuppgifter som det stora problemet. Delstatsparlamentet saknade därtill befogenhet att reglera databehandling i privat regi eller på förbundsplanet. Tyngdpunkten i Hessens lag kom att ligga på tillsyn snarare än tillstånd. En Dataombudsman inrättades med uppgift att kontrollera lagens efterlevnad. Kort efteråt antogs liknande lagar av delstaterna Bayern, Rheinland-Pfalz och Baden-Würtemberg. (Freese 1976)

På det nationella planet var Sverige först med en lag. Den kom också att täcka avsevärt mer än de tyska delstaternas. 1973 års Datalag innebar att personuppgifter inte fick lagras, bearbetas eller på annat sätt hanteras med dator såvida inte den nyinrättade tillsynsmyndigheten, Datainspektionen, gett sitt tillstånd. Endast personregister – som var lagens grundbegrepp – som beslutats av riksdag eller regering undantogs från tillståndstvånget. Avsikten var att staten skulle hålla datorregistrerandet av personuppgifter i strama tyglar. To m när de registrerade uttryckligen hade gett sitt medgivande måste enligt 1973 års lag Datainspektionen utfärda tillstånd.

Det närmast heltäckande kravet på tillstånd från Datainspektionen måste dock under 1980-talet, med det snabbt ökande antalet datorer/register, ersättas av enklare licensförfaranden och generella tillstånd. Regelverkets bärande principer (se nedan) bibehölls dock ända fram till 1998 då Datalagen ersattes av Personuppgiftslagen, PUL.

Flertalet av västvärldens länder följde efter Sverige med dataskyddslagar: Österrike 1974, Nya Zeeland 1976, Västtyskland 1977, Frankrike, Danmark och Norge 1978, Canada 1983, Storbritannien 1984, Finland 1987, Japan och Nederländerna 1988. USA valde dock att inte stifta någon datalag, vilket har fått konsekvenser på det internationella planet som strax ska diskuteras. Där nöjde man sig med en Privacy Act från 1974 med vissa riktlinjer för hur federala myndigheter skulle hantera personuppgifter. (Många av USA:s delstater har också egna datalagar för sina myndigheter.)

Denna första våg av regelverk för personvärn uppvisar stora likheter rent innehållsligt, dvs i uppfattningen om vad som var skyddsvärt, men skiljer sig också åt i vissa avseenden. Bennet (1998) nämner tre:

1. Samhällelig täckning. De europeiska länderna valde genomgående att ta ett större grepp, dvs att inkludera såväl offentlig som privat sektor i samma regelverk. USA, Canada, Australien och Japan valde däremot att tillämpa generella regler endast inom myndighetssfären. Inom privat sektor växte i dessa länder fram en kombination av speciallagar inom vissa branscher (t ex kreditupplysning, sjukvård eller videouthyrning) och frivilligt antagna etiska normer inom andra.

2. Materiell täckning. Flertalet länder valde att skriva teknik-oberoende lagar. De skulle tillämpas såväl på datoriserad registerföring som manuell. Här utgjorde Sverige, Österrike och Storbritannien undantag genom att reglera endast automatisk databehandling, ADB.

3. Efterlevnadskontroll. Intresset av att säkra genomslag för lagregler av denna typ kan tillgodoses på flera sätt. Här skiljer sig traditionerna åt inom olika delar av västvärlden. Man kan tala om en skala från ett tämligen strikt registrerings- och tillståndsförfarande i länder som Sverige och Storbritannien till ett system som bygger mera på rådgivning och på respekt för särskilt tillsatta personvärns-ombudsmän (Privacy Commissioners). Exempel på den senare modellen återfinns i Tyskland, Canada och Australien.

3.3 Lagarnas innehåll – utgångspunkter

Arbetet med att utforma lagar och andra regelverk för personvärn påbörjades alltså på 1970-talet som en reaktion på debatten om stora ”databanker” och farhågor om ett framväxande ”kontrollsamhälle”. Målet var att reglera hanterandet av personuppgifter, framförallt statens, och i det arbetet fanns inga förebilder. De internationella konventioner om mänskliga rättigheter som FN (1948) och Europarådet (1950) antagit nämnde visserligen enskildas rätt till skydd för privatlivet, men bara i allmänna termer.

Nu krävdes preciseringar. 1973 presenterades, oberoende av varandra, två regelverk för behandling av persondata som kom att bli stilbildande. Det ena var Datalagen i Sverige. Det andra var en ”Code of Fair Information Practices” – till svenska fritt översatt ”god registersed” – utvecklad av USA:s socialdepartment (Dept of Health, Education and Welfare). Utredare inom departementet hade fått i uppdrag att granska effekterna för personvärnet av datoriseringen inom sjukvården, framförallt frågan om skydd för medicinska journaler.

De bärande idéerna i båda regelverken kan sammanfattas i fem punkter (Givens, 1997):

1. Begränsad insamling. Det får inte finnas några personregister vars själva existens är hemlig.
2. Insynsrätt. Individen måste kunna få reda på vilken information som samlats om honom/henne och hur den används.
3. Avgränsade ändamål. Individen måste kunna förhindra att information om honom/henne som insamlats för ett visst ändamål används – utan individens medgivande – för ett annat.
4. Rättelse. Det måste finnas en rätt för individen att få felaktig eller ofullständig information korrigerad/kompletterad.

5. Kvalitet och säkerhet. Den som förfogar över personregister måste försäkra sig om att uppgifterna duger för sitt ändamål och att de inte kommer i fel händer.

På denna grund byggdes under 70- och 80-talen också nationella, regionala och lokala ”datalagar” världen över.

Att det fanns ett behov av internationella överenskommelser inom personvärns-området konstaterades redan i utredningen (SOU 1972:47) som presenterade förslaget till Datalagen. Såväl FN som de rika ländernas ekonomiska samarbetsorganisation OECD och Europarådet började under 1970-talet att diskutera frågan. 1980 enades Europarådet om en ”Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter”, och samma år antog OECD sina ”Riktlinjer för integritetsskydd och gränsöverskridande flöden av persondata”. Även om Europarådets regelverk ansågs något restriktivare och OECD:s mer inriktat på att möjliggöra ett internationellt dataflöde vilade båda på den grund som hade lagts med ”Code of Fair Information Practices”. (Freese 1982)

I ljuset av Internet ter sig idag OECD:s arbete något modernare – eller mindre omodernt. Givens (1997) sammanfattar det i åtta principer:

1. Principen om begränsad insamling. Det ska finnas gränser för insamlandet av persondata och sådana data ska anskaffas med lagliga och ärliga (”fair”) metoder och, när det är rimligt, med individens vetskap eller medgivande.
2. Datakvalitetsprincipen. Personuppgifter ska vara relevanta för de syften de används till och, så långt det är nödvändigt för dessa syften, korrekta, kompletta och aktuella.
3. Ändamålsprincipen. Det ändamål för vilket persondata anskaffas ska senast vid insamlingstillfället preciseras och senare användning av uppgifterna ska begränsas till detta ändamål eller andra som inte är oförenliga med det ursprungliga ändamålet och som preciseras varje gång det ändras.
4. Principen om användningsbegränsning. Persondata ska inte lämnas ut, göras tillgängliga eller på annat sätt användas för andra syften än sådana som preciseras på det sätt som anges i dessa ”Riktlinjer” utom:
   (a) med individens samtycke; eller
   (b) med stöd i lag.

5. Datasäkerhetsprincipen. Persondata ska i den utsträckning som förefaller rimlig skyddas från olovlig åtkomst, utradering, användning, ändring och spridning.
6. Öppenhetsprincipen. En grundläggande princip om öppenhet ska råda vad gäller förändringar, praktisk användning och regler med avseende på persondata. Det ska vara lätt att konstatera förekomsten av persondata och för vilka syften de används, liksom identiteten hos innehavare av persondata och vederbörandes adress/hemvist.
7. Principen om individuellt deltagande. Individen ska ha rätt att:
   (a) få besked från innehavare av persondata om huruvida uppgifter om honom/henne finns i materialet,
   (b) ta del av dessa data
      1. inom rimlig tid
      2. mot en avgift som, om den alls ska tas ut, inte är hög
      3. på ett för mottagaren rimligt sätt; och
      4. i sådan form att informationen lätt kan förstås;
   (c) vid vägran att tillmötesgå önskemål om insyn enligt (a) och (b) erhålla motiv för avslaget och möjlighet att begära omprövning av beslutet;
   (d) ifrågasätta och begära prövning av de data som relaterar till honom/henne och, om man vid en sådan prövning finner brister, få data utraderade, korrigerade eller kompletterade.
8. Ansvarsprincipen. Den som förfogar över persondata ska hållas ansvarig för att de behandlas så att ovannämnda principer får genomslag.

Med självklarhet byggde 70- och det tidiga 80-talets regelverk på föreställningen om ett begränsat antal stora databaser. Dessa var visserligen funktionella instrument för den framväxande välfärdsstaten och i storföretagens effektivisering men de associerades samtidigt till totalitära regimers strävanden efter kontroll över individen. Lagstiftarens metod för att undanröja farhågorna var att ge medborgaren vissa nya rättigheter gentemot databas-innehavarna. Den som samlade på sig persondata ålades motsvarande skyldigheter.

Redan på detta stadium, dvs före persondatorn, var åtminstone en

grundläggande konflikt mellan ”persondataskydd” och redan etablerade medborgerliga fri- och rättigheter fullt synlig. Den svenska offentlighetsprincipen har aldrig kunnat förenas med regler om ändamålsbegränsning för personuppgifter. Myndigheter samlar på sig uppgifter om enskilda för vissa syften – som må vara polisutredningar eller handläggning av ansökningar om byggnadslov – men medborgarna har rätt att ta del av materialet utan att uppge identitet eller syfte. Att medborgaren vill läsa andras ansökningar om byggnadslov kan bero på t ex (a) att han/hon fått avslag på sin egen ansökan och vill kontrollera om andra behandlas likadant, (b) missnöje med något som grannen har byggt, (c) misstanke om korruption eller svågerpolitik i byggnadsnämnden, eller bara på (d) att han/hon står i begrepp att själv ansöka och vill veta hur man formulerar sig för att ”gå hem” i byråkratin. Inget av dessa tänkbara syften har dock med den persondata-ansamlande myndighetens att göra.

Denna principiella konflikt mellan krav på ändamåls-bestämning och krav på informationsfrihet är fortfarande central och olöst. Att en myndighet eller ett företag som samlar in känsliga data om enskilda för något angeläget ändamål inte – utan de berördas medgivande – ska få nyttja uppgifterna till annat tycks närmast självklart. Om låsningen till ett ändamål däremot ska gälla för alla typer av personuppgifter och äga giltighet även när den enskilde medborgaren ansamlar uppgifter blir priset högt i form av inskränkt yttrande- och informationsfrihet och svårigheter för individen att hävda sin rätt. (Huruvida en inskränkt yttrande- och informationsfrihet – som innebär att medborgaren får svårt att skaffa kunskap om andras livsvillkor – verkligen gagnar personvärnet diskuteras i Olsson 1996 och Thelin m fl 1998.)

3.4 Persondatorn komplicerar bilden …

Med den lilla och billiga datorns, persondatorns, uppdykande ändrades under 1980-talet förutsättningarna för rättslig reglering. De nationella lagar och internationellt överenskomna principer för persondataskydd som avsåg att skydda medborgaren från makthavares missbruk av stora databaser kom nu att vändas, där de tillämpades enligt bokstaven, mot medborgaren själv.

Medan det föreföll motiverat att medborgare A hade rätt till information om vilka uppgifter om honom/henne som Riksskatteverket, regeringskansliet och byggnadsnämnden förfogade över – liksom rätt

att i vissa fall kräva radering, ändringar och kompletteringar – var det betydligt svårare att förklara varför Riksskatteverkets generaldirektör, statsministern och byggnadsnämndens ordförande nu skulle ha samma rätt gentemot medborgare A.

Medvetandet om de framväxande och skärpta konflikterna mellan personvärnsregler å ena sidan och yttrandefrihetsintresset å den andra var länge svagt. Trots att tillämpningen av datalagen i vissa fall fick absurda konsekvenser kom problemen aldrig upp till seriös diskussion. Så var det under en period 1987 regeringens och Justitiekanslerns, JK, uppfattning att alla personer som figurerade i Eko-redaktionens register över sända inslag, inklusive sådana som Ronald Reagan, Saddam Hussein och Madonna, måste informeras om detta samt upplysas om rätten att bli struken ur registret. (Regeringsbeslut 1987-05-21, dnr Ju 3533-86)

Först i början av 90-talet uppstod i Sverige en rättslig tvist som tydligt illustrerade motsättningen mellan Datalagen och Tryckfrihetsförordningen, dvs mellan de bärande principerna för personvärn respektive yttrandefrihet. Denna skrifts författare fick 1990 Svenska Journalistförbundets uppdrag att skriva en handbok för journalister i yttrande- och tryckfrihet, i princip täckande all den medierätt som en reporter kunde behöva känna till. Datainspektionen hävdade vid denna tidpunkt att dess ansvarsområde inte inskränktes genom TF:s regler utan att myndigheten i princip kunde gå in på en tidningsredaktion och med stöd av datalagen kräva att få läsa, radera och ändra i ännu opublicerade artiklar. Fullt så utmanande former hade inspektionens ”tillsyn” i praktiken inte tagit sig, men den hade dock rört sig inom TF:s område. Bl a hade den förbjudit journalister att bedriva datorstödd research och utfärdat hårt begränsande regler för tidningars utnyttjande av sina databaser med publicerade artiklar, s k ”elektroniska klipparkiv”. (Olsson 1996)

För att skapa klarhet om rättsläget ansökte jag i januari 1991 om Datainspektionens tillstånd att skriva mitt bokmanus på dator. Boken skulle inte komma att innehålla särskilt många personuppgifter, mest referenser till/citat från auktoriteter inom tryckfrihetsrätten men också enstaka integritetskänsliga uppgifter i redovisningen av principiellt viktiga förtals-mål. Enkelt uttryckt ställdes myndigheten inför valet att avstå från att tillämpa Datalagen inom TF-sfären eller att förbjuda en författare att skriva om yttrandefrihet. Beslutet dröjde. Jag arbetade med texten under 1991 och i maj 1992 kom boken (Olsson 1992) ut i handeln.

Först i juli 1993, efter att JO hade kritiserat inspektionen för den långa handläggningstiden, kom myndighetens beslut: ”*Datainspektionen lämnar ansökan utan bifall.*” (Dnr 306/91) Mitt bokskrivande var brottsligt. Beslutet överklagades till regeringen som efter åtta månaders betänketid ändrade det. TF, som är grundlag, tar över i händelse av normkonflikt med Datalagen, som är vanlig lag, konstaterade regeringen. (Justitiedepartementet, dnr 93-3260)

3.5 … och Internet

På hösten 1995 antog EU:s ministerråd ett direktiv ”om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter” (dir 95/46/EG). Medlemsländerna fick tre år på sig att implementera direktivet, dvs anta nationell lag om personvärn som uppfyllde EU:s krav.

Också EU-direktivet utgår från den ”Code of Fair Information Practises” som utvecklades 20 år tidigare. I själva verket inledde dåvarande EG sina ansträngningar att skapa ett regelverk för ”harmonisering” av medlemsländernas personvärnslagar redan på 70-talet. Svårigheterna att enas var dock betydande och arbetet bedrevs på sparlåga under hela 1980-talet. Först när den tyske kommissionären för bl a industrifrågor Martin Bangemann satte sin tyngd och prestige bakom direktivet kunde det drivas igenom.

Regelverket mötte också kritik för att vara föråldrat redan när det antogs. Det utgår från föreställningen om databehandling som en aktivitet i maktens centrum, något medborgarna ska skyddas mot. Grundprincipen är att all hantering av personuppgifter – oavsett vilken teknik som används – är otillåten till dess berörda individer lämnat sitt samtycke. Från principen medges ett antal undantag, flertalet syftande till att möjliggöra för myndigheter att sköta sina uppgifter. Yttrandefrihetsintresset tillmötesgås endast genom att direktivet medger undantag för ”*behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande*” (art. 9). Vidare sätter direktivet (art. 25) snäva gränser för ”*överföring av personuppgifter till tredje land*”, dvs land utanför EU. Sådan överföring är tillåten endast om ”tredje land” har en ”adekvat skyddsnivå” för personuppgifter. Regeln är formulerad som om sådana uppgifter normalt ”postades” av en enskild person från punkt A till punkt B. Författarna har inte beaktat hur kommunikationsnätverk som Internet fungerar.

Den svenska riksdagen valde att implementera direktivet genom en ny lag, PUL. Den ligger på alla punkter utom en mycket nära direktivet – i stora delar rör det sig snarast om en översättning. Det enda inslaget i PUL som, vid en jämförelse med direktivet, ter sig kontroversiellt är undantaget för offentlighetsprincipen. I §8 heter det att ”*Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter*.” Flera jurister, bl a lagrådet i sitt remissvar, har förklarat sig tvivla på att den formuleringen är förenlig med EU-direktivet. Uppenbarligen har Sverige här pressat de undantag från behandlings-förbudet som EU-direktivet medger mycket långt. Man kan i skrivande stund (hösten 1999) bara spekulera om huruvida den högsta rättsliga instansen, EG-domstolen, vid en prövning skulle godta PUL:s §8.

Frågan om EU-direktivet/PUL contra offentlighetsprincipen har ytterligare en aspekt. Det som PUL med §8 slår vakt om är utlämnandet av allmänna handlingar som rymmer personuppgifter. Vad den medborgare som tar del av uppgifterna sedan får göra med uppgifterna diskuteras inte i lagens förarbeten. Eftersom ”behandling” av personuppgifterna är förbjuden och begreppet är heltäckande…

”*Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t ex insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandlahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring*” (3§ PUL).

… förefaller medborgaren alltså kunna ta del av uppgifterna hos myndigheten men därefter inte kunna göra något med dem – inte organisera, inte lagra, inte bearbeta, sprida … etc. Medborgaren får andas in, men inte andas ut.

Åtskilliga myndigheter har börjat göra allmänna handlingar tillgängliga via den egna web-platsen. Uppenbarligen realiseras därmed de ideal som bär upp offentlighetsprincipen. Insyn i sådana handlingar underlättar insyn i myndigheternas verksamhet, bidrar till ökad rättssäkerhet och fördjupar medborgarnas kunskap om det egna samhället. Samtidigt skärps motsättningen mellan öppenhetskrav och regelverket för personvärn.

Överhuvudtaget kan medborgarnas utnyttjande av Internet inte för-

enas med principerna för personvärn så som de beskrivs i ”Code of Fair Information Practises” att:

1) enskilda i en nätomspunnen värld skulle garanteras kunskap om de register/databaser där uppgifter om dem lagras, att
2) sådana uppgifter skulle användas enbart för ett i förväg definierat syfte, att
3) individen skulle kunna driva krav på rättelse/komplettering/ radering av uppgifter i tusentals databaser världen runt, och att
4) någon skulle vara ”ansvarig” för hur uppgifter som en gång publicerats på t ex en web-plats sedan används

– allt detta ter sig uteslutet.

Varken enskilda, företag eller myndigheter som sprider information via Internet kan leva upp till sådana krav.

1970-talets idéer om personvärn förutsatte centraliserad och effektivt kontrollerad databehandling. Sådan finns visserligen och kommer inte att minska, men samtidigt sker alltmer datakommunikation i helt eller delvis öppna nät. Redan med Internet har möjligheterna att generellt tillämpa 70-talets ”Code of Fair Information Practises” försvunnit. Däremot återstår självfallet möjligheten att lagstifta enligt en ”Code” för enskilda rättssubjekt (myndigheter, företag, organisationer) som hanterar persondata i slutna/kontrollerbara informationsmiljöer.

Att det är svårt att förnuftigt reglera alla typer av databehandling med generella personvärnsbestämmelser är ingen ny insikt. Sverige har sedan länge haft särskilda ”registerlagar” för bl a polisens, skattemyndigheternas och försäkringskassornas hantering av personuppgifter, liksom en kreditupplysningslag för företag som säljer uppgifter om enskilda. Starka skäl talar för att man måste gå vidare på den vägen.

Meyer-Schönberger (1998) pekar på en tendens till ”sektorisering” som kännetecknar den modernaste formen av dataskyddslagar och som har utgått från de nordiska länderna. Norges, Danmarks och Finlands personvärnslagar har särskilda paragrafer för sådant som forskning, direktreklam och kreditupplysning. Artikel 27 i EU-direktivet ålägger, påpekar han, medlemsstaterna att ”uppmuntra utarbetande av uppförandekodexar” som tar hänsyn till ”de särskilda förhållandena på olika områden” så att implementeringen av nationella lagar om personvärn underlättas.

Även om denna tendens till ”sektorisering” av personvärnreglerna – deras anpassning till specifika förhållanden i olika delar av samhället – kan sägas återspegla en framväxande insikt om att generella/heltäckande bestämmelser fungerar dåligt, pekar den inte fram mot en lösning för det nätomspunna samhället. Även ”sektoriseringen” som rättslig lösning vilar på förutsättningen att databehandling sker centralt och i kontrollerbara former. Internet är per definition sektors-överskridande och användningen okontrollerad.

3.6 Lag om farlig verksamhet eller om enskilds rättighet?

Man kan, anser åtminstone vissa debattörer, med en närläsning av lagtexter och domar visa att det sedan 70-talet ändå har skett en viss omorientering i synen på det rättsliga skyddet. Att EU-direktivet skulle bygga på en 20 år gammal ”Code of Fair Information Practises” är inte hela sanningen. (Mayer-Schönberger 1998)

De första datalagarna utgick från tanken på databehandling som en farlig verksamhet. Sådan behandling antogs äga rum i samhälleliga maktcentra och lagar stiftades för att begränsa och demokratiskt kontrollera den. Med mikroelektronikens genombrott blev datorn småningom var mans egendom och databehandling var mans verksamhet. Det rättspolitiska ”svaret” på denna utveckling blev inte särskilt tydligt, men man kan spåra en förskjutning från rättslig kontroll av databehandling till garantier för personvärn som en medborgerlig rättighet. Den rätt som tidigare var konkret och handlade om att ta del av egna uppgifter i dataregister och få dem ändrade/kompletterade/strukna utvecklades till en mer generell rätt för den enskilde att utöva kontroll över uppgifterna om honom/henne oavsett sammanhang.

Sitt tydligaste uttryck fick denna ”utvecklade” rättighet i en dom i västtyska författningsdomstolen av den 15 december 1983. Målet handlade om det lagenliga i en planerad men hårt kritiserad folkräkning.

Domstolen skriver att ”*en fri utveckling av personligheten under de förhållanden som följer med modern databehandling förutsätter ett skydd för individen mot obegränsat insamlande, lagrande, användande och spridande av hans/hennes personuppgifter*”. Och vidare att:

”*… en oberoende dataskydds-myndighet är en oundgänglig förutsättning för individens effektiva skydd för sin rätt att bestämma hur hans/hennes personuppgifter används, den s k ´grundläggande rätten till informations-*

mässigt självbestämmande´." (cit ur Flaherty 1989, egen övers från engelska.)

Domstolen tolkar alltså den västtyska (numera tyska) författningen så att den i princip tillerkänner medborgarna "informationelle selbstbestimmung" (informationsmässigt självbestämmande). Den påpekar samtidigt att individens rätt, med tanke på konkurrerande samhälleliga värden, inte kan vara utan undantag. Poängen är att självbestämmandet bör vara utgångspunkten och att insamlande och övrig behandling av personuppgifter bara ska ske med stöd i lag – och inte vilka lagar som helst utan sådana som uttrycker ett starkt allmänintresse.

Lagstiftare världen över anstränger sig idag att så långt möjligt göra "samtycke" till nyckelord för personvärnet. Problemet med den linjen är inte bara att "Storebrors-institutionerna" – polis, säkerhetstjänster, skattemyndigheter, kronofogdar m fl – med slagkraftiga argument ständigt utverkar undantag från samtyckesprincipen. Även inom områden där kravet på samtycke formellt görs gällande saknar människor i praktiken ofta valmöjlighet. I allt fler yrken förutsätts användning av t ex mobiltelefon och Internet. Därmed inlemmas människor ofrånkomligen i en teknisk infrastruktur där data om dem samlas i allt större mängder på allt fler ställen.

Det rimliga/lämpliga i att lägga "informationsmässigt självbestämmande" som grund för personvärnets rättsliga konstruktion diskuteras i kap 7. Här ska bara konstateras att en rätt till "informationsmässigt självbestämmande" är lika oförenlig med Internet-miljön som en "Code of Fair Information Practises". Är personuppgiften väl är ute på Nätet, på en hemsida eller en allmänt tillgänglig distributionslista för e-post, finns inte längre någon möjlighet att säkert "få grepp" om den. En medborgerlig rättighet att behärska/besluta om sådana uppgifter vore rent illusorisk.

Däremot kan en "Code" eller lagregler göras tillämpliga för företag, institutioner eller enskilda som nyttjar Internet för kommunicering av uppgifter men som förvarar/behandlar dessa uppgifter under skyddade och kontrollerade former. När kunderna beställer böcker via hemsidorna hos Amazon eller Bokus kan företagen göras ansvariga för vad som händer med kunddata. (Mer om "informationsmässigt självbestämmande" ur konsumentperspektiv i kapitel 5.)

En del debattörer går via "informationsmässigt självbestämmande" ytterligare ett steg och hävdar att individen bör tillerkännas en "ägan-

derätt" till de egna uppgifterna. Med en sådan utgångspunkt skulle man, hävdar de, kunna bygga ett enklare och effektivare regelverk för personvärnet. Svårigheten med en sådan lösning, som blir uppenbar så fort man försöker formulera de faktiska lagreglerna, är att allt socialt liv bygger på ett i grunden okontrollerbart utbyte av "personuppgifter". Så fort man visar sig för andra människor får de kunskaper om en. Hur en rättsligt grundad "äganderätt" till personinformation skulle utformas eller tillämpas har aldrig klarlagts mera konkret. (Thelin/Olsson/Seipel 1998)

3.7 Konvergens?

Som tidigare påpekats insåg man behovet av internationell samordning kring personvärn redan på 1970-talet. De principer och internationella konventioner som de rika (datortäta) länderna kunde enas om hade dock ingen rättsligt tvingande kraft. De fungerade som stöd för nationell debatt och lagstiftning, men inte mer. När Internet vid mitten av 1990-talet växte fram som bred, världsomspännande kommunikationskanal framstod behovet av internationellt rättsligt samarbete som än mer uppenbart. Det blev för en svensk nästan lika enkelt att behandla personuppgifter med en dator i Bahamas som i Sverige. Frågan måste ställas om nationell lagstiftning överhuvudtaget kan ha någon effekt i framtiden?

Man kan betrakta utvecklingen med optimism eller pessimism. Optimisten pekar främst på det faktum att regimer med alltför starka kontrollambitioner pga Internet förlorar möjligheterna till censur och ingrepp i informationsflöden. Det blir betydligt svårare att tysta ned övergrepp eller smyga igenom orättfärdiga reformer. Ansvariga för våldshandlingar och förtryck kan "hängas ut" med namn och bild. Sociala rörelser/opinioner som är stora i människor räknat men som har svårt att få utrymme i massmedier kan "samlas" på Nätet, samordna sina aktioner och äntligen göra sig hörda. (Truedson 1999)

Pessimisten betonar den laglöshet som riskerar att breda ut sig. Traditionell brottslighet blir svårare att bekämpa. Kriminella organisationer av alla slag får ett nytt praktiskt kommunikationshjälpmedel. Även om man ofta (inte alltid) kan finna den persondator med vilken t ex förtal, rashets eller barnpornografi har lagts in på Nätet återstår svårigheten att bevisa vilken fysisk person som begått brottet. På just personvärnets område tycks risken bestå i att de länder som har lägst

skyddsnivå utvecklas till ”informationsparadis”, en parallell till redan existerande ”skatteparadis”. Sådana länder kan dra till sig företag, organisationer och individer som med sin hantering av personuppgifter riskerar att skada enskilda över hela världen.

Den kanadensiske forskaren Colin J Bennet har följt och analyserat framväxten av personvärnslagar världen över och funnit tydliga tecken på konvergens, dvs de tenderar att bli alltmer lika varandra. (Bennet 1998) Han diskuterar frågan huruvida det finns anledning att tro på en rättslig reglering med global räckvidd inom en överblickbar framtid. Det förefaller, åtminstone vid första anblicken, vara den enda utväg som pessimisten ovan kan hoppas på – men är enigheten världen över tillräckligt stor? Bennet ger inget entydigt svar.

Å ena sidan förefaller EU:s direktiv från 1995 – det första internationella regelverket för personvärn, rättsligt bindande för 15 länder och i praktiken tvingande för betydligt fler – vara ett första steg i utvecklandet av en global reglering. Av direktivet framgår att de länder som vill ha ett utbyte av personuppgifter med något land inom EU måste ha en ”adekvat skyddsnivå” för personuppgifter. Det råder visserligen ingen klarhet om vad som menas med ”adekvat skyddsnivå” men utan tvekan sätter EU härmed en press på omvärlden att anta personvärns-lagar. Det som allmänt antas bli framtidens handel – e-handeln – förutsätter just ett fritt utbyte av personuppgifter och EU utgör därvidlag en gigantisk marknad.

Å andra sidan vägrar den i särklass största nationen, USA, att acceptera direktivet i denna del. Diskussionen om en federal, heltäckande personvärnslag har förts i USA i 25 år, och även om förespråkare för en sådan lag alltid har funnits har motståndarna varit fler och starkare. För offentlig sektor finns redan personvärnslagar på såväl federal som delstatlig nivå, och i Washington råder en tämligen bred enighet om att personvärns-problem i privat sektor ska lösas område för område. För t ex telefoni, kreditupplysning och videouthyrning finns således särskilda ”Privacy Acts”. Också den ur svenskt perspektiv exotiska ”Employee Polygraph Protection Act” om personvärn för anställda i samband med lögndetektor-test är värd att nämna. (Rotenberg 1999)

Huvudalternativet för privat sektor i USA är dock inte lagstiftning utan självsanering. Inom många branscher har utarbetats en egen ”Code of Fair Information Practice” och enskilda företag och organisationer som handskas oetiskt med personuppgifter förväntas bli ”bestraffade” genom att konsumenter/medlemmar vänder dem ryggen. I juni 1998

deklarerade närmare 50 amerikanska företag som bildat ”The Online Privacy Alliance” att man avsåg att utveckla en strikt ”privacy policy” för företag som gör affärer via Internet. (Swire/Litan 1998) En för privat sektor heltäckande personvärnslag skulle också med stor säkerhet förklaras ogiltig – vad gäller effekterna för enskilda medborgares hantering av personuppgifter – av amerikanska domstolar. Ett regelverk som EU-direktivet ter sig oförenligt med första tillägget till USA konstitution, det som garanterar yttrandefriheten. (Swire/Litan 1998)

Konflikten mellan EU och USA förefaller utomordentligt svår att lösa. EU har inte heller handskats med frågan särskilt skickligt, rent diplomatiskt. Ministerrådet fattade beslut om sitt direktiv enbart med utgångspunkten att EU-medborgares personliga integritet inte fick kränkas genom databehandling i andra länder – därav kravet på ”adekvat skyddsnivå” i länder som vill utväxla persondata med EU. För USA framstår direktivet emellertid som ett försök av EU att påtvinga andra länder lagregler som de inte vill ha. Åtskilliga amerikanska företrädare finner det upprörande att EU försöker diktera hur USA:s företag ska bedriva sin affärsverksamhet i USA, bara därför att de har dotterbolag eller kunder i Europa. Det är heller inte orimligt att från amerikansk sida uppfatta EU:s försök att diktera personvärnsregler för omvärlden som ett sätt att gynna europeisk Internet-handel på USA:s bekostnad. Tonen i diskussionerna mellan den amerikanska regeringens företrädare och EU-kommissionen har också varit hård. (Mer information kring konflikten finns bl a hos hemsidan för ”The Transatlantic Business Dialogue”, en organisation bildad gemensamt av amerikanska och europeiska företag: http://www.tabd.com/.) Vid den internationella konferensen om ”Privacy and Personal Data Protection” i Hong Kong, 13-14 september 1999 ställde jag frågan till flera närvarande experter och höga tjänstemän med insyn i diskussionerna. Ingen av dem såg några öppningar eller trodde att frågan skulle lösas inom en snar framtid.

I diskussionerna – som inte får kallas ”förhandlingar” eftersom EU inte kan förhandla om innebörden av sina lagar, sådana ska endast tolkas av domstol – innebär USA:s linje att EU bör acceptera en s k ”säker hamn”-lösning (safe harbour). USA:s handelsdepartement har formulerat förslag till principer för personvärn som företag och organisationer kan välja att ansluta sig till. (http://www.ita.doc.gov/ecom/shprin.html) Principerna utgör en ”Code of fair information principles” av traditionellt slag med krav på ändamålsbestämning och datasäkerhet, med rätt för individen att bli informerad, att få rättelser/kom-

pletteringar/strykningar etc, och följer nära EU-direktivet. Företag och organisationer som ansluter sig till ”safe harbour”-principerna ska sedan kunna delta i ett fritt datautbyte med EU-länderna. (Rotenberg 1999) EU har hittills avvisat denna typ av lösning.

Diskussionerna mellan EU och USA handlar således om hur gårdagens databehandling – den som enskilda individer eller institutioner kan ha kontroll över – ska regleras. Frågan om internationellt verkande rättsregler för informationshantering i öppna nätverk finns ännu inte på bordet.

3.8 Principiella frågor

Ytterligare några frågor på temat personvärn/lagstiftning är värda uppmärksamhet. De är av rättspolitisk natur och rymmer betydande komplikationer. Avsikten är här främst att peka ut några principiellt viktiga problem. Författarens åsikter må skymta fram på någon punkt, men avsikten är inte att borra djupare eller föreslå svar/lösningar.

Den första frågan handlar om samhällelig stabilitet och förutsägbarhet. Lagstiftning om medborgerliga fri- och rättigheter tar sikte på förhållandet mellan stat och medborgare. Så talar tryckfrihetsförordningen bara om den enskildes garantier mot att myndigheter ingriper i processen att framställa/sprida tryckta skrifter. Om andra än myndigheter – t ex företag eller individer – försöker hindra medborgaren att framställa en tryckt skrift är det inte mot tryckfrihetsförordningen de bryter utan mot andra lagar, i första hand brottsbalken. De kan göra sig skyldiga till stöld, egenmäktigt förfarande, misshandel, olaga hot eller liknande.

När medborgarens garantier gentemot staten ska preciseras uppstår därmed frågan ”vilken stat?”. Är det dagens förhållandevis lugna samhällsklimat man ska utgå från – eller ett framtida, bistrare?

Just tryckfrihetens historia har, särskilt under efterkrigstiden, fungerat som lärostycke. I den samlingsregering som ledde Sverige under större delen av andra världskriget satt bara övertygade demokrater, inga yttrandefrihetens fiender. Likväl beslöt denna regering att undertrycka det fria ordet. Under politisk press från Tyskland försökte den att på flera sätt – bl a med beslag och transportförbud – stoppa antinazistiska skrifter. Vid 40-talets början vidtog man åtgärder som, om de föreslagits i samma personkrets fem år tidigare, enhälligt och indignerat hade avfärdats som demokratiskt oacceptabla. Efter kriget framstod också dessa åtgärder som skamliga, och den nya tryckfrihets-

förordning som trädde i kraft 1949 konstruerades med utomordentligt starka garantier mot sådana ingrepp.

Hade tyskarna under kriget ockuperat även Sverige, eller om militärledningen hade gjort statskupp, skulle självfallet inga grundlagsparagrafer ha kunnat rädda tryckfriheten. Skyddet ska istället, det är lärdomen, konstrueras så att det håller när en demokratiskt legitim, men hårt pressad statsledning känner akut behov av att tysta enskilda opinionsbildare eller få stopp på vissa informationsflöden. Att en svensk regering åter kan hamna under starkt tryck – hot av något slag – är inget man kan utesluta för framtiden. Utifrån ett sådant ”worstcase”-scenario måste skyddet för de medborgerliga fri- och rättigheterna utformas.

Utan att närmare gå in på diskussionen om rättigheternas ”natur”, räckvidd eller rättsliga konstruktion ska här bara konstateras att alla rättigheter inte rimligen kan tillmätas samma betydelse/dignitet. Att skyddet måste vara grundlagsfäst och starkt gäller definitivt sådant som yttrandefrihet, föreningsfrihet och förbud mot tortyr, däremot inte rätten till socialbidrag eller till fem veckors semester. (Frågan om personvärnets värde – dess relation till andra mänskliga och samhälleliga värden – är mycket komplex. Något diskuteras detta i kapitel 6.)

Nästa fråga blir då: har personvärnet – i betydelsen skydd för personuppgifter – sådan grundläggande betydelse för människovärdet och demokratin att det måste ha starkast möjliga skydd? Har persondataskydd ett värde i nivå med yttrandefrihetens, eller ligger det närmare socialbidragets?

Ur lagstiftarens perspektiv tycks det, så länge diskussionen handlar om ”personuppgifter” generellt, svårt att finna ett rimligt svar. Visst kan man tänka sig situationer när staten krossar en individ – ekonomiskt, socialt, psykologiskt – genom att behandla uppgifter om vederbörande på ett slarvigt eller illvilligt sätt. Uppgifter i vissa sammanhang, t ex förtroliga samtal mellan individen och en läkare, alternativt en psykolog eller advokat, måste ha ett starkt skydd. Uppgifter av visst slag (som ger social stigmatisering) likaså. Om man dock med hänvisning till att det finns sådana känsliga uppgifter utsträcker skyddet till alla sorters persondata kommer det att täcka ofantliga mängder information där något skyddsbehov knappast går att upptäcka. Risken är då uppenbar att respekten för lagreglerna, som i fallet med den svenska Datalagen (se avsnitt 3.1), snabbt eroderar och att skyddet inte fungerar ens där det verkligen behövs.

Kapitel 4

Tekniska lösningar

4.1 ABC om kryptering

Flertalet idéer om tekniska lösningar på personvärnsproblem inkluderar kryptering. Någon fördjupning i tekniska eller praktiska aspekter på kryptering kan det inte bli fråga om i denna rapport – det saknas såväl utrymme som kompetens hos författaren. Några elementära upplysningar om dels kryptering som sådan, dels de politiska turerna i ämnet är dock på sin plats.

De flesta barn lär sig någon gång prata rövarspråket, eller hittar på egna chiffer genom att byta plats på alfabetets bokstäver: F betyder A, G betyder B, H betyder C, osv. Om mottagaren känner till chiffrets princip kan hemliga meddelanden utbytas öppet – bara de invigda kan ”dekryptera” och läsa.

Finessen med att låta datorer sköta krypterandet är att de utför sina logiska operationer så snabbt att chiffrets princip kan göras oerhört komplicerad – så komplicerad att chiffret blir omöjligt att knäcka t o m för den som tar hjälp av de kraftfullaste datorerna i världen.

IT-samhällets behov av kryptering är enormt. Förutom att 1) skicka hemliga meddelanden – sådana som bara ”rätt” mottagare kan läsa – behöver man 2) ”underteckna” och 3) ”äkthetsstämpla” dokument. Med dokument menas här allt som kan förmedlas i digital form: text, bild, film eller ljud.

Att människor, företag, organisationer och myndigheter i många sammanhang vill kommunicera diskret/hemligt är inget konstigt. Vårt samhälle genomströmmas sedan århundraden av privata meddelanden, företagshemligheter och diplomatpost: material som är avsett för endast en mottagare. Med datorkommunikation och kryptering kan det ske både snabbare och säkrare. Så fort parterna har utväxlat ”krypto-nycklar” eller fått tillgång till en annans öppna nyckel som gör det möjligt att koda och avkoda meddelanden kan de kommunicera förtroligt via datornätverken.

Krypterandet som sådant är en urgammal metod att hantera hemligheter, men att använda krypton för ”signaturer” och ”äkthetsstämp-

ling" är möjligt endast med dator. Med en elektronisk signatur bekräftar avsändaren A för alla mottagare att A och ingen annan är den som signerat meddelandet. Med en elektronisk signatur garanteras även att ett dokument har exakt den utformning som sändaren av meddelandet gav det.

Den kod ("nyckel") som används för signerandet är avsändarens hemlighet – väl skyddad, förhoppningsvis – men avsändarens dekrypterings-nyckel som gör det möjligt att verifiera signaturen kan hanteras öppet och spridas utan restriktioner. Vid omvandlingen av meddelandet från klartext till kryptotext – för att skydda konfidentialiteten – används mottagarens öppna kryptonyckel för konfidentialitet. Endast mottagaren kan sedan omvandla kryptotexten till klartext med hjälp av sin privata kryptonyckel för konfidentalitet.

Det faktum att man kan läsa en text efter att ha verifierat den med t ex Riksskatteverkets, RSV, öppna nyckel bevisar att texten kommer från RSV.

Praktiskt taget alla bedömare är ense om att vi i framtiden kommer att leva/agera i en teknisk miljö som integrerat kombinationen hemliga kryptonycklar för signering/öppna kryptonycklar för signering samt motsvarande omvända nycklar för konfidentialitet. Den engelska förkortningen för en sådan miljö är PKI (Public Key Infrastructure). Modellen förutsätter då samtidigt utvecklandet av betrodda "tredje parter" som utfärdar certifikat för kryptonycklar, så att B kan kontrollera att A:s öppna nyckel verkligen är A:s och inte någon bedragares. "Tredje parter" kan vara myndigheter men lika gärna t ex advokatbyråer eller banker.

PKI-lösningar väntas ligga till grund för merparten av den framtida kommersiella verksamheten i datornäten, där köpare X måste vara helt säker på att säljare Y verkligen är Y, och vice versa. Inte bara som konsumenter utan också som medborgare kommer vi att behöva våra kryptonycklar: för att rösta, deklarera eller överklaga i elektronisk form. Mycket talar idag för att vi har nycklarna i "smarta kort", dvs kort med inbyggd kapacitet att bearbeta data.

Det är en rimlig förutsägelse att signaturer och kryptonycklar för skydd av konfidentialitet kommer att få en snabbt växande betydelse för personvärnet. Många av de mest illvilliga attackerna på individer har hittills skett genom spridandet av meddelanden i andras namn. (Se t ex denna rapports inledande exempel.) I princip kan vem som helst sprida, med e-post eller via en web-plats, rasistiska texter eller hot och

underteckna med namnet hos den person man vill skada. I ett mera ”IT-moget” samhälle där kommunikationen baseras på PKI blir sådana attacker svåra eller omöjliga att genomföra. Om Anders R Olsson i PKI-miljö vill sprida en kontroversiell text så kommer han att signera den. Vill han sprida texten anonymt kan han sannolikt göra det, även om de framtida möjligheterna att publicera sig anonymt är avhängiga en rad politiska och tekniska beslut och därmed svårbedömda. Att Anders R Olsson skulle sprida något kontroversiellt meddelande under eget namn, men osignerat, vore närmast uteslutet. Sådana meddelanden skulle därmed självklart betraktas som någon annans illvilliga klotter.

4.2 Politiska strider

Alltfler digitala dokument får bevisvärde, kan fungera som urkunder. Det gäller avtal, kvitton och bokföring, liksom domar och andra myndighetsbeslut. Många av IT-profeternas framtidsvisioner – elektroniska pengar, den ”friktionsfria” marknaden eller elektronisk demokrati – förutsätter säker kryptering. Teoretiskt och tekniskt är problemen lösta. Åtskilliga myndigheter (i Sverige var tullen först) och företag använder redan digitala dokument.

För att utvecklingen ska skjuta fart på allvar fordras dock internationella standarder och överenskommelser av olika slag – och billiga, lättanvända datorprogram för kryptering. En stridsfråga i den rika (datortäta) världen som är högst relevant ur personvärns-perspektiv är om dessa krypterings-program ska tillåtas bli riktigt säkra, eller säkra för alla utom polis/säkerhetspolis. Ska den som skickar krypterad information via dator, med avsikten att bara en mottagare ska kunna dekryptera, tvingas deponera krypto-nyckeln hos staten? Militära och polisiära intressen i USA och flera av EU:s medlemsstater trycker på för att säkra möjligheten att ”avlyssa” nätet. Maffian och terroristerna skickar ju också e-post. Blir krypteringen fri kan de stänga militär/polis ute, är argumentet.

Sverige har, liksom de flesta länder i Europa och Nordamerika, inga nationella restriktioner för kryptering. Man får använda vilka krypton som helst och inga nycklar behöver deponeras. Den amerikanska regeringen har gjort flera försök att inom USA genomdriva nyckeldeponering – mest känt är de s k Clipper Chip-initiativen – men hittills utan större framgång. Medborgarrättsorganisationerna

har protesterat våldsamt. Misstron mot sådan statlig kontroll är djupt och brett förankrad.

Internationellt däremot, finns starka restriktioner på krypteringsområdet. Framförallt USA försöker på olika sätt hindra spridning av datorprogram för säker kryptering. I bestämmelser om exportkontroll placeras stark kryptografi på samma skyddsnivå som plutonium och avancerad radar, dvs exporten är kontrollerad. Exportreglerna finns nu i den s k Wassenaar-överenskommelsen och i EU:s regelverk.

Kunskapen om hur säkra krypteringsalgoritmer – sådana som idag är ”oknäckbara” – skapas är dock redan vitt spridd, inte minst genom vetenskapliga tidskrifter. Avancerade krypteringsprogram kan hämtas gratis från Internet. Därmed riskerar exportrestriktionerna att få en mer hämmande effekt på hederlig affärsverksamhet än på brottsligheten.

Internet är tillgängligt överallt, för terrorister som icke-terrorister. De ”farliga” länder som exportkontrollen syftar till att avskärma (som kan vara Irak, Nordkorea m fl) är alltså inte så avskärmade som åtminstone USA önskar.

Mycket tycks stå på spel, inte ”bara” personvärn och företagshemligheter utan den allmänna tilltron till ny teknik. I många sammanhang lär kommunikation komma till stånd först när parterna är säkra på att deras meddelanden inte kan komma i orätta händer.

4.3 PET

Med ”personvärns-stärkande teknologier” – jag använder fortsättningsvis den engelska förkortningen för Privacy-enhancing Technologies, PET – menas tekniska koncept som syftar till att skydda identiteter. Praktiskt taget alla sådana koncept bygger på kryptering. (Burkert 1998)

Personvärn diskuteras ofta som en ren datasäkerhetsfråga. Datasäkerhet är en förutsättning för PET men syftar långtifrån alltid till personvärn. Datasäkerhet handlar om att skydda data/databehandling oavsett om verksamheten är laglig eller inte, om den kränker någon individ eller inte. PET handlar om att eliminera användningen av personuppgifter eller att ge individen kontroll över när/hur information om honom/henne blir tillgänglig för andra.

Burkert (1998) urskiljer fyra sorters PET-koncept. Han betonar att inget koncept kan anses färdigutvecklat och att uppdelningen bara syftar till att ge överblick över ett annars lätt förvirrande teknikområde:

A. Subjekt-orienterade koncept.

De syftar till att skydda identiteten hos agerande individer i samband med transaktioner eller i deras relation till befintliga data. Det sker genom att individen förses med en kod som inte alls, eller bara under vissa omständigheter, kan kopplas samman med honom/henne själv.

Ett sådant koncept tillämpat på t ex kreditkort skulle innebära att företag som VISA eller Mastercard ersätter uppgifter om kundernas namn i sina system med ett unikt kund-nummer. Numret korresponderar med uppgifter i en annan, skyddad databas där de riktiga identitetsuppgifterna har placerats. Där kan uppgifterna krypteras så att de blir läsliga (dekrypteras) endast om både databasägaren och individen bidrar med sina krypteringsnycklar. Användaren av kortet skulle därmed kunna använda det utan att hans/hennes identitet röjs. Säljare av varor/tjänster behöver inte uppgifter om köparens identitet, bara garantier för att det finns pengar på det konto som nyttjas.

Agentprogram (se 4.5 nedan) som konstrueras för personvärn är ett annat exempel på subjekt-orientering.

B. Objekt-orienterade koncept.

Här utgår man från det faktum att människor vid transaktioner lämnar identifierande spår och syftet är därför att eliminera sådana spår utan att påverka det som utväxlas genom transaktionen. Det klassiska exemplet på en sådan transaktion är, påpekar Burkert, kontantköpet.

I den elektroniska miljön finns motsvarigheten i t ex det telefonkort man köper i kiosken. Det är ”laddat” med en viss summa som man kan ringa för i en offentlig telefon. Betalning sker utan att betalaren identifieras.

C. Transaktionsorienterade koncept.

Här är tanken att alla identifierande spår av transaktioner automatiskt raderas vid en bestämd tidpunkt. Program för automatiska ”förstörelsemekanismer” finns redan utvecklade för användning inom e-handel. En tillämpning avser försäljning av texter, ljud eller bilder via Internet. Produkten levereras integrerad med att dataprogram som möjliggör för säljaren att radera informationen om betalningen uteblir.

Några PET-tillämpningar av tekniken finns veterligen inte utvecklade.

D. Systemorienterade koncept.

Här avses kombinationer av A, B och C i etablerandet av zoner där människor kan agera anonymt, där information kan hanteras utan att spår av dess ägare/upphovsmän fästes vid den, och där alla data om kommunikation/transaktioner raderas.

En motsvarighet IRL (In Real Life) kan vara den katolska bikten, där en anonym syndare kan möta en anonym Guds tjänare i ett avskilt rum där inget spelas in och inga anteckningar görs. En konstruerad motsvarighet på Internet skulle vara två personer som kommunicerar med e-post som sänds via s k anonymiseringsservrar och där alla spår av meddelandena omedelbart raderas.

På det politiska planet innebär, påpekar Burkert, själva förekomsten av PET att varje beslut där konsekvensen kan bli registrering/lagring av personuppgifter borde motiveras mera grundligt. Eftersom möjligheter numera ofta finns att på en rent teknisk nivå minimera eller helt eliminera personuppgifterna, bör man kräva att argumenten för varje alternativ – antingen man väljer att använda minimering/eliminering eller inte – är tydligt uttryckta och väl underbyggda. Varken i privat eller offentlig sektor kan beslutsfattare längre ”skylla på datorn”. Den kan användas för att dölja likaväl som för att exponera. Den är både penna och suddgummi och vilka funktioner man nyttjar bör motiveras.

Först när medvetandet om IT:s inneboende möjligheter har mognat hos politiska beslutsfattare kan aspekter som ”personvärn” integreras i själva den tekniska infrastrukturen. Internet må vara en enastående konstruktion men den är inte personvärnsvänlig. Inget kommunikationsnät för allmänt bruk borde egentligen generera/lagra så många spår av användarna som Internet gör. Nätets grundfunktioner konstruerades heller inte med tanke på att alla människor skulle använda det till allting.

Forskning och utveckling ska inte (kan heller inte) detalj- eller direktstyras med demokratiska beslut, men vad gäller tekniska system av stor betydelse för samhällelig utveckling och människors livsvillkor måste man via politiken kunna ställa vissa baskrav. Någon möjlighet till ytterligare fördjupning i den viktiga frågan om samband mellan teknisk utveckling och demokratiska beslut finns dock inte här.

4.4 PST

Besläktade med PET är Privacy Sympathetic Technologies, PST. De syftar till att skapa ett personvärn som är tillräckligt för de flesta människor i de flesta situationer men som inte är alldeles heltäckande. Ett klassisk exempel på PST-konceptet kan vara banksekretessen som är sträng men som kan genombrytas under vissa omständigheter – främst i samband med brottsutredningar.

I IT-miljön bygger många förslag till kompromisser mellan individens krav på personvärn och samhällets/kollektiva intressens behov av att utkräva ansvar av enskilda på PST. Ofta talas t ex om att använda ”pseudonymitet” istället för ”anonymitet”, eller ”autentisering utan identifiering.”

En ambitiös modell för PST presenterades vid en personvärnskonferens i Hong Kong i september 1999 av Austin Hill, chef för det kanadensiska företaget Zero-Knowledge Systems Inc. Modellen bygger på att individen registrerar – hos en betrodd ”tredje part” – en pseudonym som i sin tur fungerar i PKI-miljö. Pseudonymen har sin egen privata krypteringsnyckel och en öppen, och kan agera i de flesta sammanhang på nätet. Han/hon kan t ex förses med pengar att handla för och kan delta i alla sorters meningsutbyten. Som journalist eller författare, som lobbyist, som medlem i anonyma alkoholister eller som vanlig medborgare kan individen bygga upp en identitet, ett rykte, utan att för den skull avslöja sin riktiga identitet. Den som så önskar kan låta pseudonymen garantera vissa egenskaper hos den bakomliggande personen: att vederbörande är över 18 år, är man eller kvinna, har en viss utbildning, etc. Endast under mycket speciella omständigheter, i första hand när han/hon misstänks för brott, kan ”tredje parten” tvingas avslöja det riktiga namnet bakom pseudonymen.

4.5 Agentprogram och ”smarta tjänster

”Smarta tjänster” på Internet innebär att datorprogram som ”vet” något om användaren utför arbetsuppgifter automatiskt medan användaren sysslar med annat. (se avsnitt 2.3.2) Automationen kan dock ske på två sätt. Antingen decentraliserat, dvs i varje användares dator, eller centralt hos de stora aktörerna på Nätet.

Ur personvärnssynpunkt vore det en enorm vinst om det skedde hos användarna. Då skulle de undvika att stora mängder data som rör deras intressen och konsumtion lagras hos andra aktörer på Nätet.

Tekniskt är det fullt möjligt att använda s k agentprogram i det syftet – ett slags elektroniska betjänter som användaren kontrollerar och som kan utföra även avancerade sök- och bearbetningsuppgifter. Då uppstår ”marknaden” på nätet genom att användarnas agentprogram kommunicerar direkt med varandra. Programmen kan fungera anonymt, pseudonymt eller öppet, dvs i ägarens riktiga namn.

Förutsättningen är dock att den tekniska infrastrukturen har anpassats för ändamålet – att det finns en allmänt accepterad standard för utveckling av sådana agentprogram. (Ett protokoll, som teknikerna säger.) Först när det är etablerat, och tillräckligt många användare har agentprogram, kan systemet komma igång. Bara en riktigt stor aktör har möjlighet att realisera detta.

Sverker Janson, forskare vid SICS, jämför med GSM-standarden för mobiltelefoner.

– Det krävs att någon först investerar stora pengar i telenät med denna standard, kraftfullt marknadsför mobiltelefoner och subventionerar de första användarna. När detta är gjort, och användarna blivit tillräckligt många, börjar det fungera. Då kan andra aktörer också tjäna pengar på att sälja mobiltelefoner eller tjänster. (DN 990624)

Så länge IT-branschens stora elefanter – t ex Microsoft, eller Telia på den svenska marknaden – inte vill satsa på en standard som ger användarna kontroll över de ”smarta” tjänsterna blir det närmast omöjligt att bygga in förutsättningarna för sådant personvärn i infrastrukturen. Om en positiv utveckling inte kommer på naturlig väg kan krav på statlig styrning bli en politisk fråga.

– Jango är ett bra exempel på vad som nu händer, säger Sverker Janson. Det programmet utvecklades av forskare vid Washington University. Först lanserades det mera försiktigt via nätet som ett program man skulle tanka ner på sin PC. Jango kunde surfa till olika web-platser, fiska fram prisinformation och sammanställa den. Tjänsten var bra utan att vara sensationell.

– Vad hände med Jango? Jo, när upphovsmännen skulle hämta hem vinsten – de sålde sin produkt till Excite, en penningstinn komet inom Näthandeln – förändrades den i ett viktigt avseende. Den ska nu inte längre hämtas hem till PC:n. Istället är den en tjänst hos Excite. Jango hjälper till med prisjämförelser, men allt programmet gör händer på Excites server. Information om vilka produkter som intresserar dig lagras där och som användare har du ingen kontroll.

– Excite tjänar nu pengar på att kontraktera företag vars produkter ska komma med i prisjämförelserna. Konstruktionen innebär att Excite tjänar

några procent på varje affär – och de företag som inte vill dela med sig till Excite får inte vara med i prisjämförelserna.

– Sådana här tjänster beskrivs ofta som att "Du hittar det billigaste på nätet!" Så blir det inte alls. Hur skulle du kunna göra det? Den "smarta" tjänsten arbetar inte i ditt intresse. (DN 990624)

Inte heller de företag som organiserar direktaffärer individer emellan, t ex "eBay" där handeln sker sker i form av auktioner, motsvarar de krav som Sverker Jansson anser bör ställas på användarkontroll.

"Individer – inte Big Business – använder eBay för att köpa och sälja produkter i mer än 1 000 olika kategorier" heter det på eBays hemsida. Där organiseras över en miljon auktioner varje dag. "Om du vill ha en sak, finns säkert någon som säljer den." Även här handlar det dock om ett marknadstorg som ägs och kontrolleras av ett enda företag.

4.6 Kritiska synpunkter på PET och PST

Diskussioner om personvärn tenderar ofta att bli starkt polariserade och argumenteringen därmed förenklande. Tekniker för anonymisering och/eller konfidentialitet kan antingen presenteras som självklart stärkande för personvärnet eller, av den andra sidan i debatten, som hot mot samhället genom att de kan utnyttjas av kriminella eller antidemokratiska element. Riktigt så enkelt är det inte, påpekar Burkert. (1998)

Han ser fyra "interna begränsningar" hos PET, fyra aspekter att beakta när PET-lösningar framstår som realistiska alternativ. (Det betyder inte att han förhåller sig generellt negativ till sådana lösningar.)

1. Enkelriktat skydd

Många (inte alla) PET-koncept vilar på föreställningen att en svagare part behöver skydd mot en starkare, t ex medborgaren mot staten eller konsumenten/köparen mot företaget/säljaren. De vilar således på normativa ställningstaganden: A är värd stöd gentemot B, inte tvärtom.

Sådana ställningstaganden är dock inte alltid så enkla som de i förstone kan te sig. Inom ramen för e-handel t ex, kan köparen mycket väl vara ett storföretag och säljaren en liten enskild firma. Vem som behöver skyddas mot vem är inte givet på förhand. PET är bara tekniska instrument för att skydda identiteter, och som sådana kan de stödja

vilka normativa ställningstaganden som helst. De kan förvisso stärka personvärnet i situationer när vi behöver det, men de kan i princip lika gärna skydda brottslingar och förtryckare. Ingen teknik i världen befriar oss från plikten att göra normativa val, att skilja ut det som är värt skydd från det som inte är det.

2. Vilken information är identifierande?

En del PET-koncept förutsätter att man kan skilja uppgifter om en person från de identifierande uppgifterna. Man vill t ex skilja kreditkortets nummer från ägarens namn så att han/hon kan handla med kortet utan att identifieras. Möjligheterna att realisera sådana lösningar är inte alltid så goda som det i förstone kan tyckas.

Problemet kan illustreras med det s k Metropolit-projektet i Sverige. En forskare i sociologi hade vid mitten av 1960-talet påbörjat en studie av 15 000 stockholmare födda 1953. Stora mängder uppgifter om varje individ, såväl offentliga som sekretessbelagda, samlades och lagrades på datormedium. Projektet pågick i över 20 år innan Dagens Nyheter i februari 1986 slog upp ”nyheten” om det som en stor integritetsskandal. Upprördheten över att så många människor i hemlighet detaljstuderades blev stark och utbredd och Datainspektionen, som dittills hade gett forskaren tillstånd att driva projektet, tvingades besluta om s k avidentifiering. Den stora mängden rådata om varje individ fick sparas, men namn, personnummer och andra identitetsuppgifter skulle raderas.

I praktiken kan ett register av detta slag dock inte avidentifieras. För den som har tillgång till registret räcker det att känna till ett fåtal uppgifter om en individ – t ex kön, längd och skolbetyg – för att hitta vederbörande i registret. Ingen annan har exakt dessa uppgifter i kombination

De register som ofta uppfattas som mest kränkande, de som innehåller många uppgifter om varje individ, är också de svåraste att skydda. Till synes triviala uppgifter som erhållits från annat håll kan fungera som nyckel till den övriga, känsligare informationen.

3. Helhetens problem

Det som är en viktig fördel med PET – att lösningen på personvärnsproblemet formuleras som en teknisk och väl avgränsad uppgift för systemkonstruktörer – kan också vara en begränsning. Att skydda iden-

titetsuppgifterna för en specifik grupp i ett visst sammanhang kan visa sig närmast bortkastat om inte gruppen skyddas lika väl på andra håll. En ambitiös satsning på att hålla HIV-smittades identitet hemlig inom sjukvården förlorar mycket av sitt värde om en lista över ”abonnenter” på information (en sändlista för e-post, t ex) riktad till just HIV-smittade inte skyddas.

Systemkonstruktörer kan ta ansvar för sin del av verkligheten, men så länge ingen tar ansvar för helheten kan hans/hennes möda visa sig bortkastad.

4. Den tekniska utvecklingens snabbhet

PET-koncept vilar ofta på förutsättningen att en viss typ av kryptering är så stark att möjligheten för någon utomstående att ”knäcka” den är rent hypotetisk. På kort sikt tycks sådana bedömningar vara tillförlitliga, men redan i ett medellångt perspektiv ter sig saken betydligt osäkrare. Utvecklingen inom området ”datorstödd kryptering” går snabbt och större/kvalitativa språng kan inte uteslutas.

Burkert identifierar också det han kallar ”externa begränsningar” för PET. Här handlar det således om samhälleliga eller direkt politiska faktorer som kan verka mot användningen av PET.

Den första har med informationsekonomi att göra. När konsumenten idag köper något utgör i praktiken hans/hennes personuppgifter en del av betalningen, låt vara en liten del. Företaget använder kunddata som en resurs i produktutveckling och marknadsföring. Berövas företaget genom PET-system denna resurs tvingas det höja priset för att kompensera den minskade effektivitet som följer av att det dels inte kan hålla kontakt med kunderna, dels får minskad precision i sin marknadsföring. Man kan mycket väl tänka sig ett pris för identifierade kunder och ett något högre för anonyma. Redan idag är det vanligt att registrering av surfarens personuppgifter – adress, intressen, vanor m m – ställs som villkor för tillträde till vissa webplatser eller nerladdning av gratisprogram. Man ”betalar” med sina personuppgifter. Burkert påminner om att direktreklambranschen är stor och kapitalstark och att den ofta har lyckats förhindra begränsande rättslig reglering. Det finns således starka ekonomiska intressen som missgynnas av PET, och det motstånd som kan mobiliseras bör inte underskattas.

Den andra faktorn kallar Burkert ”mobilisering”. I vår tids samhäl-

le är människor – därför att de kan vara det – trolösare än förr. Banden till familj, grannskap, arbetsplats och överheter av alla slag har blivit svagare än någonsin. Individen lever med eller mot sin vilja alltmer frikopplad och anonym. Denna utveckling har genererat motkrafter. ”De politiskt styrande, myndigheter, politiska partier, religiösa samfund, företag, den lokala livsmedelsbutiken, pizzerian och frisören försöker hela tiden nå kontakt med dig *som individ* för att dra in dig i en relation, eftersom relationer numera är så flyktiga att de måste förnyas vid varje tänkbart tillfälle.” *(Burkert 1998, egen övers)*

Denna mobilisering, dessa ständiga försök att upprätta kontakt, är en social kraft som inte heller bör underskattas. Det är inte bara så att ledande politiker vill engagera (ofta dock bara på politikerns villkor) medborgarna i samhällsutvecklingen, medborgarna vill ofta engagera sig i det politiska styret på ett eller annat sätt. Man kan därför vänta sig två utvecklingstendenser. Dels kommer teknikerna för mobilisering att förnyas och förfinas som ett resultat av ansträngningarna (med PET eller på andra sätt) att stärka människors möjligheter att leva anonymt. Dels kommer framtida PET-koncept att rymma ”bakdörrar” som individen kan välja att utnyttja – öppningar som gör vederbörande identifierbar under vissa omständigheter som han/hon har bestämt själv.

Den tredje faktorn är personvärn som politisk/samhällelig företeelse. Burkert ser den föreställning som PET bygger på – att personvärn uppnås genom helt eller delvis skyddande av identiteter – som primitiv och pekar på behovet av ett mer dynamiskt ”politiskt personvärn”. PET måste integreras i sociala system på ett smidigt sätt för att inte låsa medborgaren vid antingen-eller-lösningar. Dels måste möjligheter skapas för medborgarna att delta i/påverka uppbyggnaden av de tekniska system för kommunikation där PET kan utgöra en del. Dels måste PET konstrueras så att de ständigt erbjuder medborgarna alternativ, eftersom bedömningen av huruvida man vill vara anonym kan förväntas växla från dag till dag, från situation till situation, från uppgift till uppgift. En jämförelse med de demokratiska processer som medborgaren idag deltar i, visar att han/hon här blandar anonymitet (vid röstning i allmänna val, som meddelare till journalister) med offentlighet (deltagande i debatter och demonstrationer).

Ett nyckelord är således integration. Tekniska lösningar på personvärnsproblem måste utformas för/i människors sociala verklighet. Biltillverkaren Ferrari erbjuder med 1999 års modeller mycket eleganta tekniska lösningar på ett av vårs tids kommunikationsproblem. Sam-

ma bilar hade dock varit oanvändbara 1899 och kan visa sig lika oanvändbara 2099. De är redan 1999 oanvändbara för människor som aldrig lärt sig köra bil, för människor som bor långt från asfalterade vägar och för människor som inte har råd att köpa bensin.

Här, när resonemangen om de tekniska lösningarna på personvärnets problem börjar handla allt mer om de samhälleliga realiteter med vilka tekniken ska integreras, är det dags att byta perspektiv till ett mer socialt och psykologiskt. Så ska ske i kapitlen 5 och 6.

Kapitel 5

Frivillighetens väg

Om rättslig reglering och tekniska system för personvärn till sin natur är ”hårda” eller tvingande lösningar, centralt beslutade och lika för alla, innebär branschers självreglering och individers fria val ett från politiska utgångspunkter mer lockande alternativ. Varför centralstyra om en samhällelig process utvecklas ”av sig själv” i önskad riktning?

I detta kapitel ligger fokus på relationen säljare – konsument, där den senare normalt har möjlighet att välja mellan flera motparter, men resonemangen kan också ha relevans för andra relationer – t ex den mellan en organisation och dess medlemmar. Personvärnsnivån i medborgarnas informationsutbyte med myndigheter däremot, fordrar i allmänhet reglering genom politiska beslut, och när utbytet sker medborgare emellan ligger frivilligheten s a s redan i öppen dag.

Det ska genast påpekas att gränserna mellan juridiska, tekniska och frivilliga lösningar är flytande. Om individerna i framtiden själva ska få avgöra, så ofta som möjligt, hur uppgifter om dem får behandlas, förutsätter det tekniska system som stöder just en sådan ordning. Att företagen som bedriver e-handel alldeles självmant ska utveckla regelverk och administrativa rutiner som ger konsumenterna bästa möjliga personvärn kan te sig väl optimistiskt – men varför inte med politiska åtgärder ge dem en knuff i rätt riktning? Möjligheterna är många. Staten kan ge företag som lever upp till bestämda krav på personvärn en förmånligare behandling i något/några avseenden, eller bara låta Datainspektionen offentligt betygsätta kommersiella aktörers personvärnsansträngningar och sedan överlåta besluten om vad som är acceptabelt respektive oacceptabelt åt konsumenterna. (Jämför dagens miljömärkning.)

Detta kapitel diskuterar möjligheter och svårigheter med frivilliga lösningar. Det blir relativt kort, helt enkelt därför att vi här mest rör oss på okänd mark. Kunskaperna om hur man rent tekniskt kan stödja frivillig-lösningar utvecklas, främst i USA, men hur konsumenter och medborgare kommer att reagera på erbjudanden om att själva välja personvärns-nivå går inte att bedöma på detta stadium. Att mera vidlyftigt spekulera om vilka val en framtida, mer IT-mogen allmänhet kommer att träffa när den ställs inför alternativ som vi idag inte när-

mare kan beskriva, ter sig mindre meningsfullt.

5.1 Standardisering

Standarder är resultatet av frivilliga överenskommelser mellan parter, vanligtvis på en marknad. Ämnesområdet ”standardisering” är gigantiskt stort eftersom det berör produkter av nästan alla slag och eftersom otaliga organ, på nationell som internationell nivå, arbetar med diskussioner och beslut om standarder – många av dem överlappande och/eller konkurrerande. Därtill ska läggas de-facto-standarder som uppstår helt utan överenskommelser därför att en aktör (t ex Microsoft) har så stor marknadsandel att alla andra tvingas anpassa sig efter dess produkter och tekniska vägval.

Vad gäller Internet-relaterad teknik & programvara bedrivs standardiseringsarbete i ett särskilt högt tempo. Så förutsätter t ex etablerandet av en PKI (Publik Key Infrastructure) att en hel svit standarder vinner allmän acceptans. De starka ekonomiska intressen som driver fram e-handeln har ett uppenbart intresse av att utvecklingen här går snabbt.

I Nordamerika är intresset för och diskussionerna om standarder för personvärn av naturliga skäl – där finns inga generella personvärnslagar tillämpliga på den privata sektorn – betydligt livaktigare än i Europa. Det kanadensiska standardiserings-organet CSA (Canadian Standards Association) antog i september 1995 en ”Model Code” för personvärn inom privat sektor. Det blev den första – och är i skrivande stund fortfarande den enda – standarden i sitt slag.

CSA-modellen bygger på den ”Code of Fair Information Practices” som OECD beskrev med sina ”riktlinjer” 1980 (se kap 3). OECD:s åtta punkter har hos CSA utvidgats till tio.

1. Ansvar. En organisation är ansvarig för de personuppgifter den förfogar över och ska utse en person med uppgift att garantera att organisationen agerar i enlighet med följande principer.
2. Definition av ändamål. Avsikten med att samla in personuppgifter ska klargöras av organisationen vid eller före det tillfälle då insamlande sker.
3. Samtycke. De berörda individerna ska göras medvetna om och samtycka till att personuppgifter samlas in, används eller ges spridning, utom i de fall det är olämpligt. (”except where inappropriate”)

4. Begränsad insamling. Insamlandet av personuppgifter ska begränsas till det som är nödvändigt med hänsyn till det ändamål som organisationen definierat. Insamlandet ska ske med ärliga och lagliga metoder. (”by fair and lawful means”)
5. Begränsad användning, spridning och lagring. Personuppgifter ska inte användas eller spridas för andra ändamål än vad som ursprungligen definierades, såvida inte berörda individer medger det eller det föreligger en rättslig skyldighet. Uppgifterna ska inte sparas längre än vad som är nödvändigt för att uppfylla ändamålet.
6. Datakvalitet. Personuppgifter ska vara så korrekta, fullständiga och aktuella som ändamålet fordrar.
7. Skydd. Personuppgifter ska skyddas med den effektivitet som är rimlig med hänsyn till hur känslig informationen är för berörda individer.
8. Öppenhet. En organisation ska snabbt och enkelt ge enskilda information om sina interna regler och sin praktiska hantering av personuppgifter.
9. Individuell kontroll. Individen ska på förfrågan få veta om organisationen förfogar över uppgifter om honom/henne, hur de används och sprids och därtill själv få se uppgifterna. Han/hon ska ha möjlighet att begära korrigeringar och kompletteringar och, när sådana önskemål är berättigade, få ändringarna utförda.
10. Ifrågasättande av efterlevnaden. Individen ska ha möjlighet att hos organisationens ansvarige klaga över det sätt på vilket organisationen tillämpar regelverket och att få sina klagomål bemötta. (Cavoukian/Tapscott, 1997)

OECD har utvecklat en ”Privacy Policy Statement Generator”, en stödfunktion för företag och organisationer som vill utveckla en personvärnspolicy för sin verksamhet och därefter presentera den på en webplats. (En beta-version av ”generatorn” är gratis och finns på: http://www.oecd.org/scripts/PW/PWHome.ASP. Även den slutliga versionen kommer att vara gratis.)

”Generatorn” har utformats i samarbete med näringsliv, privacyexperter och konsumentorganisationer i OECD:s 29 medlemsländer. Den hjälper användaren i två steg. Först lotsas ansvariga inom organisationen genom processen att utforma en policy, vilket inkluderar en

analys av de egna förutsättningarna och behoven, nationell lagstiftning och etiska normer som bör beaktas. Steg två är avsett som stöd för web-ansvariga när de ska arbeta fram en kort och lättbegriplig beskrivning – den text som ska möta webplatsens besökare – av de personvärnsprinciper som man genom steg ett har utmejslat. I praktiken genererar OECD-verktyget ett förslag till text som den webansvarige sedan får förfina/förbättra.

OECD:s uttalade avsikt är att öka medvetenheten hos såväl webplatsernas ägare (företag, organisationer, myndigheter) som medborgare och konsumenter om hur viktig personvärnsaspekten är i allt agerande på nätet.

5.2 Frivillighetens problem 1: politiken

Att människor själva ska kunna välja – när inga tungt vägande skäl talar mot det – skyddsnivån för de egna personuppgifterna ter sig i högsta grad rimligt. Med den utgångspunkten ställs man förr eller senare inför två problem.

Det ena gäller bestämmandet av vad som ska menas med ”tungt vägande skäl”. Just på denna punkt måste personvärnet – det vore naivt att tro annat – bli politiskt kontroversiellt. Ingen kan nå fram till en slutsats om individens rätta relation till kollektivet, eller medborgarens till staten, som är ideologiskt neutral. Om man för tydlighetens skull renodlar problematiken kan man säga att en nyliberalism som fokuserar enbart på individen står mot ett socialistiskt synsätt som innebär att individen inte helt kan ryckas ut ur sitt sociala sammanhang.

Själva det faktum att nyliberalen vill minimera såväl den offentliga sektorn som politikens sfär, medan socialisten anser att åtskilliga funktioner/områden i samhället bör underordnas demokratiska beslut, öppnar för oenighet. Om nyliberalen hävdar att ägaren till en tomt måste få disponera den fritt och t ex bygga vad han vill på den följer därav att han är motsätter sig dagens ordning med kommunala byggnadslov. Enligt denna uppfattning bör ingen tvingas redogöra för sina byggnadsplaner i ansökningshandlingar till kommunen, och frågan om huruvida sådana handlingar bör vara offentliga hos kommunen behöver aldrig ställas. Socialisten, som hävdar att det måste finnas gränser för vad tomtägaren får bygga, försvarar ansökningsförfarandet och tvingas därmed ta ställning till frågan om ansökningshandlingars (=personuppgifters) offentlighet. Med stor sannolikhet når socialisten i just detta

fall slutsatsen att det råder ”tungt vägande skäl” för att handlingarna ska hållas tillgängliga för allmänheten. Dels behövs offentlighet för att värna rättssäkerheten och medborgarnas tilltro till den kommunala förvaltningen, dels finns i sådana handlingar inga typiskt sett känsliga uppgifter. Tomtägare A, som fått avslag på sin ansökan, måste kunna försäkra sig om att hans fall har bedömts på samma grunder som alla andras. Några risker för integritetskränkningar med en sådan ordning är svårt att upptäcka.

Den ideologiska diskussionen om personvärn ska dock inte fördjupas här. (Olsson 1996, något utvecklas temat också i Thelin/Olsson/Seipel, 1998)

5.3 Frivillighetens problem 2: praktiken

Det andra problemet är att skapa praktiska möjligheter för alla människor att med tillräckligt liten ansträngning göra sina individuella val. Häri ligger en svår utmaning.

Ytterligt få svenskar kan redogöra för det konsumenträttsliga skyddets innebörd eller omfattning. De allra flesta gör sina köp och tecknar sina avtal (om försäkringar eller teleabonnemang) utan att mera noggrant studera säljarens/motpartens villkor – även när relativt stora belopp står på spel. Man förlitar sig i hög grad på att det finns skyddsmekanismer i samhället som garanterar att ingen ska råka riktigt illa ut.

Finns det mot den bakgrunden någon anledning att tro att konsumenterna vill ägna tid/möda åt att studera en säljares ”personvärnspolicy” innan han/hon via Internet köper en bok, en cd-skiva eller ett datorprogram? Blir inte sådant bara ytterligare en mängd finstilt text som köparna hoppar över, vilket i praktiken innebär att de obesett väljer ”default”-nivån för personvärn – alltså den skyddsnivå som säljaren från sina utgångspunkter anser rimlig eller normal? Frivilligheten riskerar att bli en chimär därför att så få konsumenter tycker sig ha tid och motivation att göra den ansträngning som fordras för ett medvetet val.

De lösningar på problemet som idag anses mest lovande bygger på automation. Om web-platser för e-handel kan förmås att presentera sin personvärns-policy i standardiserad form så kan denna policy också ”läsas” och ”bedömas” av datorprogram som är integrerade med köparnas s k browsers, sökprogram för www. Köparen definierar sina

krav på personvärnsnivå innan han/hon ger sig ut för att handla på Internet, och programmet varnar sedan för varje web-plats där en säljare inte motsvarar dessa krav.

Ett förslag till standard för sådan automatisk kommunikation mellan säljare och köpare har utarbetats inom projektet The Platform for Privacy Preferences, förkortat P3P. Projektet har initierats av The World Wide Web Consortium (W3C). (Cranor 1999. Se också http://www.w3.org/) Inom ramen för en sådan standard kan sedan flera former av automatisk interaktion mellan köpare och säljare utvecklas, där köparen själv avgör vilka uppgifter om honom/henne som ska lämnas ut – och till vem.

I teorin och på försöksstadiet finns här således lösningar på viktiga personvärnsproblem. Dessa lösningar, liksom flera andra som diskuteras i föreliggande rapport, förutsätter att Internet tekniskt och praktiskt anpassas efter människors önskemål om personvärn – OCH att dessa människor själva börjar använda datorprogram med vars hjälp uppgifter kan skyddas. Huruvida vi får en sådan utveckling lär i hög grad bero på hur människor framöver visar sig resonera om personvärn. I vilka avseenden vill vi skärma av våra liv från omvärlden? Vilka metoder kommer vi då att föredra? Vilka uppoffringar i form av försvagat/obefintligt personvärn är vi beredda att göra för vinna trygghet, rättvisa eller något annat viktigt?

Kapitel 6

Mjuka frågor: kunskap och kultur

Vi saknar distans till fenomenet Internet. Det tycks ha potential för att inom något decennium drastiskt förändra hela vår ”informationsmiljö” och det är knappast möjligt att förutse hur vi reagerar på och förändras med den utvecklingen.

”Varje ny teknologi måste absorberas av samhällskulturen. Det är egentligen inte individer som funderar ut hur den ska utnyttjas, det är kulturen som helhet. Människor undersöker teknologins möjligheter, klagar över dess nackdelar, iakttar samtidigt varandra, lyssnar till historier, och gradvis når människors känsla för proportioner jämnvikt på en ny nivå.” (Philip Agre i det elektroniska nyhetsbrevet Red Rock Eater News 990813, egen övers.)

6.1 Kontroll av kontrollanterna

Tekniska hjälpmedel för diskret övervakning – ljud- och bildupptagning i kombination med allt snabbare datakommunikation – utvecklas och förfinas i hisnande takt. På sikt har vi egentligen bara två alternativ. Vi kan få det öppna samhället där människor vet det mesta om varandra, eller det slutna där bara de mäktigaste ständigt ser oss.

För den dystopin står amerikanen David Brin, rymdfysiker och science fiction-författare, med sin bok ”The Transparent Society – Will Technology Force us to Choose Between Privacy and Freedom?”. (”Det genomskinliga samhället – Kommer den tekniska utvecklingen att tvinga oss välja mellan personvärn och frihet?”)

Han målar två framtidsbilder på temat ”livet i din stad om 20 år”. Gemensamt för båda visionerna är att den tekniska utvecklingen har varit fortsatt snabb, särskilt inom datakommunikation. Gemensamt är också att brottsligheten på gator och allmänna platser har kunnat nedbringas till noll, praktiskt taget.

Båda städerna har små rörliga, diskreta kameror och mikrofoner uppsatta överallt. I stad nummer ett skickar de sina signaler till polisiära centra där de avläses av datorprogram som ”känner igen” stulna

fordon och ansikten på efterlysta personer. Programmen kan också ”slå larm” om trafikbrott, våldshandlingar eller människor som ropar på hjälp.

I stad nummer två går samma signaler till polisen där de bearbetas på samma sätt. Skillnaden är att signalerna samtidigt är allmänt tillgängliga via Nätet och att de elektroniska ögonen/öronen finns också inne på polisstationerna. Även övervakarna är övervakade. Vilken medborgare som helst kan koppla upp sig till vilken kamera som helst – och själv kontrollera t ex att polisen använder tekniken till brottsbekämpning och ingenting annat.

Trots de yttre likheterna representerar dessa städer radikalt olika föreställningar om relationen mellan medborgare och styrande. Vår spontana reaktion är nog att vi inte vill leva i någondera staden, men om vi nu måste välja – föredrar vi inte den senare?

Måste vi verkligen välja? Brins argumentering är inte lätt att avfärda. Såväl tekniskt som politiskt ter sig hans framtidsvision fullt möjlig.

Den nation som leder utvecklingen mot kameraövervakade samhällen är, kanske något förvånande, Storbritannien. Det började för tio år sedan i staden Kings Lynn, drygt tio mil norr om London. 60 rörliga, fjärrstyrda kameror sattes upp för att övervaka stadens ”stökigaste” platser. Resultatet överträffade allas förväntningar. Brottsligheten vid övervakade gator, torg och parker minskade till en bråkdel. Den vinst som polisen gjorde genom minskat patrulleringsbehov var så stor att den på ett par månader hade tjänat in hela kostnaden för inköp & installation av den tekniska utrustningen.

Exemplet spred sig. 1998 fanns i Storbritannien över 300 000 övervakningskameror i drift, kopplade till ett hundratal polisiära larmcentraler. Överallt är effekten, enligt Brin, kraftigt minskad brottslighet och ökad uppklarande-procent för de brott som faktiskt begås. (Enligt Madeleine Blixt vid svenska BRÅ är de brittiska erfarenheterna något mer blandade. Tidskriften APROPÅ 5-6/98.)

I maj 1997 löpte fotbollslaget Newcastle´s fans amok i stadens centrum. Polisen kunde med hjälp av videoupptagningarna identifiera 152 ansikten på våldsverkare, berättar Brin. Fotografier på 80 av dem publicerades i lokalpressen och inom några dagar var samtliga identifierade.

Andra länder tar redan efter, som Japan, Thailand och Singapore. Till och med i USA, landet där privatlivet och de medborgerliga rättigheterna värnas med större frenesi än kanske någon annanstans, är övervakningskamerorna på väg in. Storstaden Baltimore har dem i samt-

liga 106 gatukorsningar i centrum. I New York började man 1997 montera upp dem i Central Park, i tunnelbanan och på andra offentliga platser. Visst höjs det kritiska röster, men än så länge tycks folkmajoriteten uppfatta kamerorna som mera trygghetsskapande än integritetshotande. Proteststormarna har uteblivit.

Kamerorna blir också ständigt mindre, rörligare och får allt bättre bildskärpa. USA:s militär har sedan flera år använt flygande kameror som sänder trådlöst. Den första generationen sådana ”spionfåglar” kostade en miljon dollar styck, men nästa är redan i produktion och blir betydligt billigare. Brin spår att den relativt snart får – om den dessutom massproduceras för den civila marknaden – ett för medelinkomsttagaren överkomligt pris. Efterfrågan på avancerad övervakningsteknik är stor, åtminstone i USA, och utbudet av ”James Bond-prylar” ökar. Främst är det föräldrar som vill försäkra sig om att barnen har det bra och kontrollera vad barnvakten egentligen har för sig. (Alltfler daghem i USA ”direktsänder” f ö sin verksamhet via Internet.) Skulle vi inte vilja kontrollera att gamla mormor på långvården får den hjälp hon behöver? Att tonåringen inte mobbas på skolgården? Att hantverkaren inte snokar i lådor och skåp? Att …

Arbetsgivarna vill kontrollera sina anställda. Butiksägarna sina kunder. Alla kanske inte kan titta på alla i framtiden, men väldigt många kommer att kunna titta på väldigt många. I stor utsträckning kommer det att ske via Internet, eftersom videokameror så enkelt kan kopplas till nätanslutna datorer.

Självfallet blir framtidens ”övervakning” inte bara fysisk, inte bara en fråga om kameror, påpekar Brin. Den handlar också om data/personuppgifter och tvingas i hög grad på oss via Nätet. Det är ytterligt tveksamt om vi kan hemlighålla vad vi köper, vad vi läser, vilka vi känner och vilka åsikter vi har. Idag förbehålls sådan kunskap ett litet fåtal – nätadministratörer, ISP-företag och polisen, när den är intresserad – och vi har inga möjligheter att kontrollera hur detta fåtal egentligen hanterar information om oss.

Att nya potentiellt integritetshotande tekniker får utvecklas och etableras utan egentlig debatt ter sig olämpligt i flera avseenden. Det förefaller dubbelt olyckligt om vi får 1) ett kraftigt ökande flöde av personuppgifter som också sparas i väldiga databaser, 2) en omfattande och komplicerad lagstiftning syftande till sekretess och skydd för dessa uppgifter, och 3) en allmänhet utan praktiska möjligheter att överblicka eller lära sig systemets funktioner.

Med en så omfattande och i stor utsträckning dold persondatahantering skapas förutsättningarna för såväl missbruk – svårt att upptäcka t o m för en Datainspektion som måste arbeta med enstaka stickprovskontroller i en nät-miljö präglad sekretessregler och krypteringsrutiner – som diverse larmrapporter om Storebrors förehavanden. Här framträder konturerna av ett samhälle med bästa tänkbara grogrund för både faktiska konspirationer och ogrundat konspirationstänkande.

Brin är inte så extrem att han helt bejakar en ”värld av glas”. Även han vill värna det mest intima i sitt privatliv och i vissa avseenden tror han också att det blir möjligt. För att söka intimitet eller ensamhet måste vi kunna dra oss undan. Åtminstone hemmet bör utgöra en skyddad sfär, anser han. Som huvudlinje bör vi dock välja det mycket öppna samhället framför det – i personvärnets namn – mycket slutna. Storstadens helt anonyma tillvaro är på väg att ersättas med en mänsklig miljö som i vissa avseenden påminner om den lilla byns – och det har vi anledning att bejaka:

”Idag läser vi om gamla människor som hittas döda i sina hem flera månader efter att någon senast såg dem i livet, och om barn som kränks och misshandlas i åratal utan att grannarna förstår vad som händer eller gör något åt saken. Sådant kommer inte att hända mer när byn åter blir verklighet. Viktigpettrar kommer att skvallra, men du kommer att känna till deras hemligheter också – och du kommer att kunna lämna dörrarna olåsta. Ditt sovrum kommer med elektronikens hjälp att vara skyddat från insyn, men ett viktigare skydd blir rädslan hos voyeurerna och övriga nyfikna för att ertappas med att snoka. Dina mellanhavanden med skattemyndigheterna må bli allmänt kända, men det blir också varje misstänkt affär som politiker eller finansvärldens storfräsare gör. Vem som helst kan ta reda på hur mycket du betalade för den där näsoperationen, eller vilken salladsdressing du brukar köpa; och din reaktion på det blir: ´Vem bryr sig?´. Det är inte märkvärdigare än att människor vet färgen på den tröja du bär.” (sid 334)

Visst ligger det en lockelse i anonymiteten, erkänner Brin. Väljer vi personvärnsfanatikernas och krypteringsfantomernas väg kan anonymiteten bibehållas och t o m utvidgas – särskilt för de resurstarka och de tekniskt kunniga. Allt detta hemlighetsmakeri har dock ett pris, hävdar Brin.

”*En sak är jag säker på. Människor med onda avsikter kommer att kunna göra betydligt större skada i en värld av hemligheter, masker och slöjor än i ett rike där ljuset sakta tilltar, överallt.*” (sid 334)

Han betonar genom hela boken att frågan i dess undertitel – *Kommer teknologin att tvinga oss att välja mellan personvärn och frihet?* – egentligen är fel ställd. Det är visserligen fråga om två skilda värden, båda högst eftersträvansvärda, men de står i grunden inte mot varandra.

”*Istället härrör det ena uppenbarligen från det andra. Fria människor må kunna begära och förverkliga ett mått av personvärn (…) även i den tilltagande kameraövervakningens tidevarv. Men först, för att kunna göra det, måste de ha försäkrat sig om en stabil grund för sin frihet.*” (sid 201)

Brins viktigaste poäng är att han kan peka på värdet – för personvärnet! – av öppenhet. Hemlighetsmakeri är lösningen bara på vissa integritetsproblem.

”*Vi må agitera och lagstifta. Men kan verkligen ´datalagar´ förhindra att övervakningsredskapen blir mindre, mobilare och ´smartare´? I form av datorprogram kommer de att verka på våra elektroniska motorvägar. Tekniska lösningar för att skydda hemligheter kommer visserligen också att utvecklas, men en rustningskapplöpning mellan de övervakande och de övervakade kan knappast gynna ”den lilla människan”. De rika, de mäktiga, polismyndigheterna och IT-samhällets kunskapselit kommer alltid att ha ett försprång.*” (sid 13)

Frestelsen att begå övergreppet minskar betydligt när förövaren måste göra det inför mängder av vittnen. Lusten att sprida illvilligt skvaller eller kränkande omdömen om andra avtar säkerligen med vetskapen att man i efterhand måste stå för och motivera sina uttalanden. Att människor beter sig anständigare i offentlighetens ljus gäller också de rika, de mäktiga, polismyndigheterna och IT-samhällets kunskapselit. Brin ser IT-redskapen som en möjlighet att för första gången i världshistorien göra makthavarna fullt synliga och verkligt ansvariga inför folket. En svaghet i Brins bok är, som tidskriften The Economist påpekar i en lång uppskattande artikel om den (990501), att Brin inte diskuterar svårigheterna med att hålla ett öppet samhälle öppet. Ska hemlighetsmakeri bli brottsligt i sig? Att lagstifta fram en vid öppenhet är kanske inte så mycket lättare än att – som EU gjort med sitt direktiv om skydd för persondata – lagstifta om närmast maximal sekretess.

Brins plädering för en ”minimalistisk” hållning i personvärnsfrågan låter delvis bekant för en svensk som intresserat sig för offentlighetsprincipen. Att en teknisk utveckling oundvikligen skulle föra oss in i ett samhälle där vi i alltfler sammanhang kan iakttas av andra må vara ett nytt argument, men att maktens institutioner måste vara genom-

skinliga och att demokratin förutsätter att medborgarna har tillgång till åtminstone viss information om varandra (se t ex avsnittet om byggnadslov i kap 5) är närmast vardagsmat i Sverige.

6.2 Teknisk oundviklighet?

Författaren och redaktören för den elektroniska tidskriften The Art Bin, Karl-Erik Tallmo, ser också – utan att ta ställning för eller emot – en utveckling mot större genomskinlighet som fullt realistisk:

”Möjligen går vi mot en värld där publicering och offentliggörande inte längre är de aktiva processerna. Publicering skulle helt enkelt vara normaltillståndet, en självklar biprodukt av allt dagligt liv, såväl arbete som fritid. Den aktiva handlingen skulle då snarast bli tillbakahållandet, skapandet av hemliga, privata rum, lösenordszoner eller helt enkelt sammanhang där vi helt undviker all elektronik.” (Tallmo 1999)

Huruvida utvecklingen mot ett mer genomskinligt samhälle verkligen är oundviklig kan självfallet diskuteras. Den tekniska utveckling som frambringar nya övervakningsinstrument ger oss rimligen också redskap som skyddar och skärmar av. Frågan är kanske, som Brin är inne på, om medborgarna i gemen verkligen kan hänga med i en kapplöpning mellan ständigt mer sofistikerade övervaknings- och skyddstekniologier? Effektiva krypteringsprogram som PGP har funnits gratis tillgängliga på Internet i flera år utan att allmänheten har visat något större intresse av att använda dem. Möjligen får krypteringsprogrammen ett genombrott den dag de blir verkligt användarvänliga – här går utvecklingen framåt men den har en bit kvar.

En annan aspekt på utvecklingens ”oundviklighet” är de politiska besluten i frågor kring teknisk infrastruktur. Internet är närmast en mardröm ur personvärnssynpunkt. Dels därför att varje människa som vill sprida uppgifter om andra så lätt når ut med dem via www, nyhetsgrupper, chat-miljöer eller distributionslistor för e-post, dels därför att vanlig e-post från person A till person B är så svagt skyddad. Varje informations-bit som strömmar genom Nätet kopieras och lagras i serverdatorer mellan avsändare och mottagare. Vilka dessa server-datorer blir kan man i avsändningsögonblicket inte avgöra. Självfallet måste inte ett globalt kommunikationsnät fungera just så. Här finns möjligheter att stärka förutsättningarna för personvärn. Hur, när och

var de politiska kraven på förändringar i den tekniska infrastrukturen ska ställas är dock, milt uttryckt, svåra frågor.

6.3 Social oundviklighet?

En fritt samhälle, med ett levande politiskt och kulturellt liv är alltid statt i förändring. I ljuset av ny kunskap och som ett resultat av offentliga diskussioner omvärderas – ofta i tämligen långsamma processer – människors föreställningar. Det förut oacceptabla (t ex homosexualitet) kan accepteras och det tidigare normala (t ex barnaga) kan bli oacceptabelt.

Alla omvärderingar är naturligtvis inte av godo. Om medborgarna i gemen anpassar sig till ett mer ”genomskinligt” samhälle utan att ha fått konsekvenserna av en sådan förändring belysta eller har ställts inför alternativa möjligheter, då utgör det ett misslyckande för demokratin. (Och, kan man tillägga, om majoriteten av människorna i vår del av världen faktiskt väljer att leva mer synliga/övervakade så följer av detta inte nödvändigtvis att minoriteten i varje läge ska tvingas acceptera detsamma.)

Britten Simon Davies, färgstark ordförande för lobbyorganisationen Privacy International, pekar på det paradoxala i att människor å ena sidan oroar sig mer än någonsin för integritetskränkningar (sådan är enligt Davies trenden i opinionsmätningar i den rika delen av världen) medan å andra sidan de organisationer, särskilt i Europa, som kämpar för ett starkare personvärn sedan åtminstone tio år har förlorat i kraft och folkligt stöd. Davies anser sig kunna spåra en förskjutning i själva föreställningen om personvärn. Från att under 60- och 70-talen ha uppfattats som en medborgerlig rättighet diskuteras det idag oftare som en ”tjänst” eller ”produkt” bland andra.

”*Med personvärnets överflyttande från den politiska sfären till konsumentsfären integreras det i en annorlunda uppsättning värden och relationer. Placerar man det på den fria marknaden som en valmöjlighet bland flera – storlek? färg? hållbarhet? – får vi en situation där privatlivs-skydd är ett tillvalsalternativ som kostar extra*.” (Davies 1998)

Nedvärderingen, i det allmänna medvetandet, av personvärnets betydelse är också förklaringen till att det i Storbritannien har blivit möjligt att bygga ut de väldiga system av övervakningskameror som Brin beskriver.

– Vi börjar redan tala om dessa poliskameror som ytterligare en bekväm-

lighet, något man drar in överallt. Vatten, avlopp, el och övervakning, sa Davies vid den internationella konferensen om ”privacy” i Hong Kong i september 1999.

Därmed sker också förskjutningar i den demokratiska grundstrukturen, i medborgarnas relation till staten. Davies redogör för flera fall i Storbritannien där polisen i utredningen av grövre våldsbrott har erbjudit alla människor i en viss kategori – alla vuxna män boende i ett visst område, alla ägare till en bil av viss modell, etc – att frivilligt lämna DNA-prov. ”Bara så att vi kan avföra Er från vår undersökning” försäkrar polisen. Konsekvensen för den som inte lämnar något prov blir att vederbörande utsätts för en desto mer noggrann undersökning. (Davies 1998) Man tar ett steg från principen ”oskyldig tills motsatsen bevisats” i riktning mot ”misstänkt tills Du bevisat Din oskuld”.

Davies fullföljer, kan man säga, 60- och 70-talens mobilisering mot Storebror. (1996 publicerade han f ö en bok med titeln ”Big Brother. Britain´s web of surveillance and the new technological order”.) Jämfört med hur situationen var på 60- och 70-talen förefaller varningarna idag, med alltfler övervakningskameror och gigantiska avlyssningssystem i drift, avsevärt mer befogade. Frågan är om våra livsvillkor – eller vår tolkning av dem – har förändrats så att vi ändå inte uppfattar hoten som särskilt allvarliga?

Anlägger man t ex den franske filosofen Michel Foucaults perspektiv på utvecklingen tycks en obehaglig bild framträda. Människor som med IT befrias från tunga och farliga arbetsuppgifter, och som med Internet får drastiskt förbättrade möjligheter till utbildning, kommunikation och underhållning, blir de i just denna process alltmer disciplinerade och maktlösa tjänare i stora, teknikburna sociala system? Att IT blir vår befriare är kanske inte självklart. I vilken utsträckning och i vilken betydelse behärskar vi egentligen de automatiska processer som nu integreras i såväl våra fysiska som våra intellektuella aktiviteter? Hur är den ”nödvändighet” konstruerad som drastiskt ändrar – och förmodligen försämrar – förutsättningarna för personvärn? (För diskussioner av detta slag, se bl a Lyon, 1994.)

6.4 Elände som underhållning

En paradox i vår tid är att behovet av personvärn officiellt erkänns som berättigat och viktigt, samtidigt som journalistiken och underhållnings-

branschen alltmer febrilt exponerar dolda, obehagliga eller direkt skrämmande sidor av samtida, levande människors privatliv. Medan möjligheterna att med rättsliga och tekniska metoder avskärma delar av våra liv har förbättrats – storstadens anonymitet har hittills utgjort en tacksam miljö för sådana ansträngningar – tycks intresset växa för såväl kända som okända människors hemligheter. Länge gällde nyfikenheten mest s k kändisars drogmissbruk och relationsproblem, men under de senaste tio åren har Oprah Winfrey, Jerry Springer m fl pratshow-värdar överbjudit varandra i exponerandet av vanliga människors ”privata” elände.

Det mesta handlar direkt eller indirekt om sex. Inför studiopublik konfronteras en man med upplysningen att han inte är far till det barn som hans hustru snart ska föda. Nästa dag i samma studio anklagar dottern sin far för sexuella övergrepp. Tredje dagen berättar sonen för sin mamma att han sedan flera år prostituerar sig och numera är HIV-smittad. Om dessa program har ett gemensamt budskap så är det att samhället under en någorlunda polerad yta rymmer nästan hur mycket svek, lögn och hyckleri som helst. Och, vilket är det nya och anmärkningsvärda, det råder ingen brist på människor som vill berätta detaljerna – för hela världen.

Vad säger oss detta om hur synen på, och behovet av personvärn utvecklas i vår tid?

Psykoanalytikern Janna Malamud Smith resonerar i boken ”Private Matters” om hur människan, i grunden en social varelse som tenderar att bli bokstavligen tokig om han/hon inte blir sedd, reagerar på det moderna livets ändrade villkor. Om vuxna för ett par generationer sedan, i det socialt tätare samhället, sällan kunde hemlighålla t ex sexuella snedsteg eller annat socialt oaccepterat beteende är det fullt möjligt för flertalet idag. Den funktion som skvallret i tvättstugor och trappuppgångar fyllde förr, fyller åtminstone delvis Oprahs m fl pratshower idag. Människor får bekräftat att andras privatliv, bakom fasaderna, är minst lika kaotiskt och problemfyllt som deras eget. När familjefadern som i åratal misshandlat och förtryckt hustrun och barnen ”hängs ut” i TV som det svin han är, får hans offer ett slags upprättelse. Andra kvinnor och barn i samma situation kan känna ett moraliskt stöd och, kanske i några fall, få den skjuts de behöver för att ta initiativet och lämna sin plågoande.

Samtidigt, hävdar Malamud, är dagens skvallermodell, i jämförelse med gårdagens, hänsynslös och exploaterande. Det människor igår

berättade för varandra i tvättstugor och omklädningsrum baserades åtminstone i någon mån på personligt förtroende (”det här berättar jag inte för vem som helst”) och ansvar (”jag litar på att Du kan handskas med den här informationen på ett förnuftigt sätt”). Pratshowernas offentliga skvaller avpersonifierar och renodlar och blir därmed råare. Tittaren ser främlingars elände och kan därmed förfasa sig och fördöma helt reservationslöst. Showen blottar moralisk och känslomässig misär lösryckt ur sitt sammanhang. Även om det fyller en viktig funktion blir skvallret degraderande för alla inblandade.

”*Om vi fortsätter att så generöst blottlägga andra människors privatliv skadar vi både dem och oss själva, vi berövar privatlivet dess värde och vi bidrar till att skapa en social atmosfär präglad av ömsesidig exploatering. Låt mig utttrycka det på ett annat sätt: Få saker i livet är så värdefulla som friheten att uttrycka och göra sådana saker med människor man älskar som man aldrig skulle uttrycka eller göra om någon utomstående var närvarande. Och få upplevelser är så fundamentala för frihet och personlig autonomi som att upprätthålla kontroll över när, hur, till vem och var man avslöjar det djupt personliga.*”

”*Ironiskt nog måste*” skriver Malamud på ett annat ställe i boken ”*försvaret av privatlivet också bygga på insikten att övervakning faktiskt bidrar till säkerhet. En paradoxal fråga måste ställas: Hur mycket och vilken sorts övervakning är nödvändig för att hindra det rena missbruket av personvärn? Självinsikt, hedersbegrepp och kärlek har bevisligen inte alltid en tillräckligt återhållande verkan. I vilken utsträckning behöver vi vara socialt synliga för att kunna hålla våra våldsimpulser, vår girighet, vårt ljugande, våra destruktiva kontrollbegär, vår vrede och vårt njutningsbegär under kontroll? När Oprah inbjuder misshandlade kvinnor till sin show använder hon, delvis, televisionen för att öka medvetenheten om att dolt maktmissbruk förekommer. (…) Frihet…realiseras nog inte bäst när vi undviker all övervakning utan när vi har möjlighet att påverka vem som övervakar oss, och när och hur.*” (Malamud 1997)

Alla behöver kunna ”*planera sitt offentliga liv*”, alla bör få ”*chansen att konstruera ett liv som de känner igen som sitt eget*”.

(…)

”*Den djupare frågan…är huruvida vi kan värna vårt privatliv och realisera dess möjligheter utan att förfalla till ett sentimentalt perspektiv på den mänskliga naturen. Svaret beror i sin tur på om vi lyckas organisera samhället så att det stöder ett rimligt mått av säkerhet och frihet i både det offentliga och det privata. Alltför ofta beskrivs dessa båda behov som motstri-*

diga, men i själva verket utgör de inbördes beroende kammare i samma hjärta. Maktmissbruk i den ena kammaren ger upphov till sjukdomar som sprider sig till den andra. Socialt förtryck, fattigdom och orättvisa begränsar människors tillgång till sina inneboende mänskliga resurser; undergräver självaktningen och försvagar därmed det självförtroende som ger möjlighet att glädjas åt privatlivets värden. När vår förståelse av psyket blir alltmer sofistikerad, kan vi då inte skapa en offentlig miljö i vilken kunskapen om hur människor skapas och knäcks är bättre integrerad?"

Dessa referat av och citat ur Malamuds bok är bara axplock. Alla hennes resonemang är f ö inte invändningsfria. Avsikten är här främst att lyfta fram, in i debatten om personvärn, en sorts kunskap som inte rymts där tidigare. Diskussioner om "rätt" personvärns-nivå måste föras på många samhälleliga arenor, och på åtskilliga av dem är de gamla vanliga argumenten om "individens rätt" contra "kollektivets behov" helt enkelt för primitiva. Lyckas vi inte, i det allmänna medvetandet, kvalificera förståelsen av problemets natur kommer vi heller aldrig vidare.

Kapitel 7

Slutsatser och förslag

7.1 Kunskapsbrist

Exemplen på att enskilda har råkat ut för svårare integritetskränkningar via Internet tycks ännu vara få. Någon mer omfattande ”inventering” av sådana fall har inte kunnat göras inom ramen för denna studie, men det förefaller vara nödvändigt – bl a med tanke på den snabba tekniska utvecklingen – att sådana inventeringar verkligen genomförs. Helst bör de då omfatta så många olika medier och sammanhang som möjligt. Behovet av empirisk kunskap om var, när och hur kränkningar faktiskt sker är stort. Olika medier och samhällsområden bör jämföras med varandra så att eventuella åtgärder kan vidtas först där de mest behövs.

Att empiriska studier nästan helt saknas är en av flera orsaker till att frågan om allmänna personvärns-regler tidvis har varit så svårhanterad i Sverige. Såväl debatten som lagstiftningsarbetet har i hög grad byggt på teoretiserande och ideologiserande. Till skillnad från de specifika reglerna till skydd för enskildas integritet i sekretesslagen, där varje bestämmelse i princip kan relateras till enskildas agerande i konkreta sammanhang och effekterna förutses, bygger PUL (och gamla datalagen) på föreställningar om ”hot” av mera obestämt slag. Närmare verkligheten än enkäter om hur människor ”upplever” stora databaser hos myndigheter, eller om de ”känner obehag” vid användning av personnummer har man inte kommit. Någon mera ambitiös undersökning om konkreta kränkningar, med uppföljning av enskildas uppgifter om sådana, har veterligen aldrig genomförts. (Därmed inte sagt att endast sådana kränkningar som människor själva känner till är av intresse. Den s k personalkontroll som sker i SÄPO:s regi är ur personvärnssynpunkt uppenbarligen riskabel, men de individer som utsätts för kontrollen får normalt ingen kunskap om vad som händer. Se bl a Töllborg 1986, och Forsberg 1990.)

Insikten om hur angeläget det är att kunskap om personvärnsrisker – och skyddsmöjligheter – finns med i underlagen för viktiga beslut i såväl offentlig som privat sektor leder till upptäckten av en annan brist. Kunskapen finns inte att få tag på i Sverige. Ingen myndighet, organi-

sation eller ”think-tank” arbetar med framtidsfrågor av det slaget. Närmast till hands ligger Datainspektionen, men den myndigheten är genom sin konstruktion och sitt uppdrag vänd bakåt i tiden. Hela verksamheten är inriktad på att tillämpa lagregler formulerade med föregående decenniums tekniska lösningar för ögonen. I sitt tillsynsarbete studerar inspektionen system som redan är i drift och reagerar på allmänhetens klagomål om kränkningar som redan har ägt rum. Verksamheten genererar inte den kunskap om framtida hot och möjligheter som medborgarna och den politiska debatten skulle behöva.

En studie- och forskningsverksamhet vänd framåt skulle skapa betydligt bättre förutsättningar för en förnuftig personvärns-politik. Ur teknisk, juridisk, sociologisk och psykologisk synvinkel borde man studera vad forskare över hela världen sysslar med, hur den internationella personvärns-debatten utvecklas och vilka möjligheter som föreligger att påverka utvecklingen i Sverige i rätt riktning.

Utan en bättre karta blir det oerhört svårt för alla inblandade – forskare, journalister, politiker, jurister, kommersiella aktörer och vanliga medborgare – att orientera sig i ett landskap så fullt av risker och möjligheter.

7.2 En första överblick: arenorna

Ett sätt att överblicka hanteringen av personuppgifter på Internet är att dela upp den i fyra kategorier, alla med sina förutsättningar att regleras eller på annat sätt påverkas:

• FÖR DET FÖRSTA en öppen, okontrollerad kommunicering av uppgifterna via web-platser, chat-miljöer, diskussionsgrupper eller distributionslistor för e-post som är tillgängliga för alla. Här förefaller den enda realistiska möjligheten vara rättsliga ingripanden i efterhand mot kränkningar, t ex i form av förtal eller intrång i upphovsrätt.

När en personuppgift väl är ute på Nätet, t ex har gjorts tillgänglig på en hemsida, kan ingen längre kontrollera vad som händer med den: hur många ”exemplar” det finns av den, i vilka datorer den lagras, för vilka ändamål den används, etc. En lagfäst medborgerlig rättighet att ”kontrollera” sådana uppgifter vore rent illusorisk.

En lag om personvärn som bygger på hanteringsmodellen, dvs att endast sådan behandling av personuppgifter ska vara tillåten som lagstiftaren i särskild ordning har godkänt, ter sig också oacceptabel av

såväl yttrandefrihetsskäl som rättssäkerhetsskäl. Att förbjuda allt, men sedan se genom fingrarna med nästan allt, är i en rättsstat knappast rimligt.

Informationsflödena i denna helt öppna del av Internet erbjuder således betydande problem ur personvärns-synpunkt. Nätet kan här jämställas med ett gigantiskt, väl indexerat klotterplank. Kränkande uppgifter om en person kan ”klottras” med liten risk för upptäckt, antingen genom att spåren till klottrarens dator sopas igen (vilket är svårt men inte omöjligt) eller genom att klottraren använder en dator som är tillgänglig för många.

Utvecklandet av enkla program för elektroniska signaturer och äkthets-stämpling av elektroniska dokument minskar dock utrymmet för kränkningar. Åsiktsyttringar eller meddelanden från individen A som inte är elektroniskt signerade av A kommer naturligen att uppfattas som falsarier. Falska sex-annonser t ex, av den typ som relateras i inledningen till denna rapport, kommer knappast att fungera. Eftersom elektroniska signaturer gör det möjligt för alla människor som vågar stå för sina ord offentligt att säkert identifiera sig, kommer icke-signerade meddelanden naturligen att betraktas med stor skepsis. Sådant anonymt ”klotter” kan säkert i många fall ändå skada, men vi har länge levt med möjligheterna att skicka brev utan avsändare, att sätta upp texter utan undertecknare på anslagstavlor, att lämna anonyma meddelanden per telefon, att klottra på väggar osv. Att ”Internet-klotter” på ett väsentligt sätt skulle försvåra problemet är åtminstone inte självklart.

Att stödja utvecklingen av elektroniska signaturer och möjligheter att använda pseudonymer är således viktiga insatser för det framtida personvärnet. Praktiskt taget alla debattörer säger sig betrakta yttrandefrihet som en av förutsättningarna för ett demokratiskt samhälle. Med den utgångspunkten förefaller det rimligt att lagstiftaren går fram med största möjliga försiktighet, och således avvaktar med inskränkningar i det fria ordet även på Internet tills effekten av en utbredd användning av signaturer/pseudonymer börjar bli tydlig.

Den komplicerade relationen mellan frihet och personvärn går med det ”okontrollerbara” Internet åter i dagen.

Min egen uppfattning är att en vid yttrande- och informationsfrihet är så avgörande för demokratin att när missbruket av denna frihet kan beivras endast genom ytterligare inskränkningar i den – då måste man redan efter ett fåtal steg stanna upp, dvs avstå från att beivra. Man måste leva med en del missbruk.

En sådan principiell ståndpunkt innebär inte att man ”accepterar” rasistisk propaganda eller personliga kränkningar. (Att man motsätter sig kraftfulla åtgärder för att minska medborgarnas möjligheter att använda bil betyder inte att man ”accepterar” att hundratals människor dör och tusentals lemlästas i trafiken varje år.) Det utgår från åsikten att ett samhälle där man juridiskt garanterar staten möjlighet att effektivt ingripa mot varje skadande eller obehagligt yttrande vore outhärdligt att leva i. Ett sådant samhälle förutsätter en polisiär kontroll över all informationsbehandling som inte gärna kan förenas med demokrati eller medborgares personvärn. En yttrandefrihet som är så reglerad att den inte kan missbrukas är ingen yttrandefrihet.

• FÖR DET ANDRA en i någon grad kontrollerad kommunicering. Tillgången till information via en web-plats kan av ägaren begränsas med hjälp av lösenord. Medverkan på en distributionslista för e-post kan godkännas efter individuell prövning och/eller informationsutbytet kan vara modererat, dvs en ansvarig person granskar och godkänner det som sprids via listan.

Här öppnar sig flera möjligheter för personvärnet. På ”arenor” där människor måste identifiera sig för att bli insläppta, och vet att de kan bli utslängda igen, fungerar uppförande-koder eller andra etiska regelverk oftast väl. Ställer man på sådana web-arenor också krav på att meddelanden ska vara elektroniskt signerade bör utsikterna till ansvarsfullt beteende vara särskilt goda. I en framtida teknisk miljö där ”pseudonymitet” är ett etablerat fenomen – där personens riktiga identitet i alla lägen utom vid välgrundad brottsmisstanke skyddas hos en s k betrodd tredje part – kanske det också blir möjligt att kombinera anonymitet med ansvarskänsla.

Vad gäller modererade diskussioner finns också möjligheten att koncentrera det rättsliga ansvaret till moderatorn, som då får samma funktion som den ansvarige utgivaren för en tryckt skrift. Analogin kan fullföljas så att deltagare i diskussionen på denna web-plats eller diskussionslista generellt kan beviljas straffrihet och rätt till anonymitet, precis som dagens meddelare och skribenter i en tryckt skrift. (En sådan modell föreslogs redan av Mediekommittén, SOU 1997:49 men har hittills inte accepterats som grund för lagstiftning.)

• FÖR DET TREDJE en kommunicering som är helt sluten, där personuppgifter sänds från punkt A i Nätet till punkt B och där avsikten

är att inga andra än människan/människorna vid A respektive B ska få tillgång till informationen. Detta gäller såväl vid individuell e-postförmedling, vid web-baserade transaktioner mellan konsument och säljare som vid medborgares kommunikation med myndigheter i form av inkomstdeklaration, sjukanmälan etc.

Här är det uppenbarligen möjligt och i många fall nödvändigt att urskilja – och skriva särskilda regelverk för – de ansamlingar av personuppgifter som blir resultatet av kommunicerandet. Regelverken kan utformas enligt en ”Code of Fair Information Practices” där ändamål, tillåtet innehåll, de registrerades rätt till information och rättelser m m preciseras.

Vad beträffar myndigheter finns i Sverige redan en serie sådana s k registerlagar – för polisens, skattemyndigheternas, socialförsäkringens m fl verksamheter. Inget hindrar att fler sådana utvecklas. Här bör man dock observera att offentlighetsprincipen inte låter sig kombineras med någon strikt ändamålsbegränsning. Att kommunförvaltningen samlar kommunalrådets kontokortsnotor för representation i syfte att sköta bokföringen så som lag och interna regler föreskriver får inte hindra att medborgarna läser notorna och använder informationen i syften som de bestämmer själva.

Även beträffande företags hantering av kunddata och uppgifter om de anställda finns olika möjligheter att stärka personvärnet. Lag baserad på en ”Code of Fair Information Practices” kan stiftas, antingen i form av generella bestämmelser för all kommersiell verksamhet eller för olika branscher allteftersom problem eller risker kan urskiljas. (För kreditupplysningsverksamhet finns redan lag.) Här kan man också argumentera för en försiktig linje där möjligheterna till branschvis självreglering, personvärnsstärkande tekniska lösningar eller standarder bör undersökas först och rättsliga inskränkningar i informationsfriheten blir den sista utvägen.

För individuell e-post gäller självfallet detsamma som för pappersbrev förmedlade av Posten. Det är inte statens sak att styra eller granska innehållet. Var gränsen sedan ska dras mellan ”individuell” e-post och sådan e-post som har så många adressater att avsändaren får anses gå utöver den privata sfären kan diskuteras. På detta område finns dock en tradition inom yttrandefrihetsrätten att bygga vidare på, och problemet ska inte diskuteras närmare här.

• FÖR DET FJÄRDE den hantering av uppgifter – nästan helt auto-

matiserad – som följer av själva administrationen av Internet. Vem som helst kan med lätt tillgänglig programvara, en hyggligt kraftfull PC eller Mac-dator och en fast (=alltid öppen) uppkoppling skaffa sig en www-server. För just denna hantering av personuppgifter är det svårt att på kort sikt se några lösningar på personvärns-problemen. Den som kontrollerar en sådan server kan, om illviljan finns, skaffa en del kunskap om ”surfare” som kopplar upp sig mot den – inklusive kunskap om vilka andra web-platser de har besökt.

Med e-post-servers (SMTP) är saken mer komplicerad. Författaren av denna rapport har inte tillräckliga kunskaper om den tekniska miljön för att kunna diskutera problematiken i detalj, men utan tvekan är det en dyrare och svårare operation att starta och driva en e-post-server än en www-dito. F n sköts e-posthanteringen av Internet-branschens stora och medelstora aktörer, vilket kan ge anledning till ett visst hopp om ansvarsfullt uppträdande. Telia och Tele2 dominerar starkt vad gäller marknaden för privatpersoner och småföretag. Större företag, organisationer och myndigheter sköter ofta sin egen e-posthantering. Samtidigt är betydelsen av ett fungerande personvärn särskilt stort just vad beträffar e-post. I SMTP-servers över hela världen lagras under längre eller kortare tid elektroniska kopior av det som kommuniceras, inklusive uppgifter om avsändare och mottagare.

Större ISP-företag (Internet Service Provider) i den rikare delen av världen har anledning att sköta sig väl ur personvärnssynpunkt. Det företag som får rykte om sig att strunta i kundernas personvärn eller slarva med säkerheten riskerar att förlora marknadsandelar. De flesta har också en egen policy för hur kunderna ska skyddas. Samtidigt är den information som en större ISP kan samla på sig om kunderna omfattande och representerar stora värden. (se kap 2) Frestelsen att exploatera uppgifterna blir därmed betydande, och det kan ske lagligt genom att förfogandet via finstilta paragrafer i abonnemangs-avtalen överförs på ISP-företaget. Vidare måste man beakta att ”tröskeln” som kunderna ska över för att byta ISP är relativt hög. Att göra det omgående kan kosta pengar – beroende på hur länge man har bundit sig i avtalet med den ISP man vill lämna – och möda. Diverse inställningar i datorn ska ändras. Eventuellt måste man byta e-post-adress och nå ut till ett stort antal människor och institutioner med den upplysningen.

Ingen kedja är heller starkare än sin svagaste länk. Det räcker att säkerheten brister hos någon av landets större ISP-företag, eller att

någon av de anställda som sköter e-post-hanteringen låter sig mutas eller blir hotad, för att stor skada ska uppstå.

En typ av server-ägare utgör särskilda problem, nämligen polisiära eller militära organ som driver server-verksamhet i jakten på relevanta (för dessa organ) uppgifter. Envisa rykten omger t ex de s k anonymiserings-servers som enskilda kan använda för att ”tvätta bort” avsändar-uppgifter från e-post. CIA uppges driva flera SMTP-servers av den typen. Någon bekräftelse på att så sker finns givetvis inte, man kan bara konstatera att verksamheten vore förhållandevis billig och välmotiverad ur polisens och militärens perspektiv.

Att stifta en lag som på olika sätt begränsar serverägares rätt att handskas med personuppgifter är en möjlighet. Svårigheterna att kontrollera en sådan lags efterlevnad är dock uppenbara. Det fordrar sannolikt någon slags anmälningsplikt för serverägare och en myndighet (Datainspektionen?) som ges rätt att kontrollera innehåll, loggar m m i sådana servers. Kontrollen måste kunna genomföras vid endast svag misstanke om oegentligheter – kanske bara en anmälan från den missnöjda eller oroliga individen X. Vill man inte ge staten så långtgående befogenheter gentemot enskilda datorägare återstår, för den som vill känna sig någorlunda säker på brevhemligheten, att kryptera sina meddelanden.

För att närmare analysera risker och möjligheter för personvärnet relaterade till den tekniska strukturen hos Internet fordras således både kunskaper och utrymme som författaren saknar. Åtminstone i teorin finns möjligheter att i framtiden dela upp Internet i ”zoner” eller ”nivåer”. Man kan tänka sig fria men otrygga/okontrollerbara ”zoner” kompletterade med mer kontrollerade men tryggare ”områden”. Av uppenbara skäl är det angeläget att kunskap om alternativen samlas och läggs till grund för offentlig debatt innan avgörande beslut fattas om den tekniska infrastrukturen.

7.3 En andra överblick: möjliga åtgärder

Anden kan inte stoppas tillbaka i flaskan. Den tekniska utvecklingen är i full gång och även om den i viss utsträckning kan påverkas demokratiskt kan den inte kontrolleras i djupare mening. Politiken måste rida på vågen. Den måste vara beredd till omprövningar utan att för den skull ge upp försvaret för grundläggande mänskliga och sociala värden.

Agre (1998) urskiljer åtta olika ”policy-instruments”, åtta metoder för samhälleligt stöd för personvärn. Uppdelningen – att det blir åtta istället för sju eller nio – kan diskuteras. Gränserna för vad som kan och inte kan göras på politisk väg i form av ”stöd”, ”uppmuntran” etc är också oklara, men som översikt är Agre´s sammanställning klargörande:

1. Personvärnslagar i kombination med statlig tillsynsmyndighet eller ombudsman som ska övervaka efterlevnaden.
2. Krav på, eller åtminstone uppmuntran till, användning av PET. Visserligen är det svårt att på politisk väg bestämma eller styra utvecklandet av den tekniska miljö i vilken PET ska fungera, men en politik för stärkt personvärn kan ändå bidra på många sätt. Det offentliga kan stödja forskning och standardiseringsarbete, finansiera praktiska försök, föregå med gott exempel inom myndighetssfären och se till att frågan om PET integreras i all undervisning där den har relevans.
3. Krav på, eller stöd för kommunikationsprotokoll som medger individuell ”förhandling” om persondatahantering. Här avses standarder av typen P3P (se kap 5). Målet är en enkel, helst automatisk interaktion mellan individ och omvärld där individen själv avgör/kontrollerar vilka uppgifter om honom/henne som ska lämnas ut, till vem och på vilka villkor.
4. Kriminalisering eller reglering av vissa tekniker. Precis som avtal idag kan förklaras ogiltiga av domstol därför att de innehåller oskäliga villkor kan man tänka sig att vissa tekniska lösningar förbjuds eller åtminstone begränsas därför att de ger upphov till relationer i vilka den enskilde har svårt att hävda sina legitima intressen.
5. Utvecklandet av olika etiska normsystem för persondatahantering anpassade efter förhållandena i de samhällssektorer där de ska verka. Kunskapsspridning om existensen och innebörden av normerna är viktig liksom uppföljning av hur de tillämpas.
6. Breddande av den rättsliga basen för personvärn. Om vi med den nya tekniken får hot- eller kränkningssituationer som inte täcks av ett äldre regelverk kan nya lagar eller förändringar i rättspraxis behövas.
7. Utvecklande av standarder för personvärn. Även om sådana standar-

der utvecklas och administreras av oberoende organisationer, kan lagstiftaren/staten stödja dem – t ex genom att vid offentlig upphandling kräva att de tillämpas av varje anbudsgivare.

8. ”Botten upp”-utbildning av systemutvecklare, anställda med ansvar för hantering av personuppgifter – och av allmänheten. Oavsett hur välformulerade lagar eller etiska regelverk vi har, förutsätter ett fungerande personvärn att alla inblandade förstår hur integritets-problem uppstår i vardagslivet. Medborgarna behöver kunskap om hur personuppgifter kan utnyttjas och vilka rättigheter de har.

   Ett förslag som ligger nära till hands är att införa obligatorisk redovisning av ”personvärnskonsekvenser” i alla reformförslag som i något avseende får effekter för hur personuppgifter genereras, lagras, bearbetas eller kommuniceras.

7.4 Slutord

Det är lätt att avskräckas inför stora, komplicerade tekniska system, men också lätt att förföras av deras möjligheter. Ett nyckelord för många av de mest eftertänksamma debattörerna inom personvärnsområdet är ”förtroende”. Ytterst finns inga tekniska lösningar som överbryggar problemet med förtroende. Paradoxen är väl känd: man kan ordna övervakning av människor för att försäkra sig om att de beter sig anständigt, men sedan måste någon övervaka övervakarna, och vem ska därefter övervaka dem som övervakar övervakarna? Något mått av risk måste den acceptera som vill leva bland människor, och för att dessa risker ska vara hanterbara måste vi ha möjlighet att etablera förtroendefulla relationer med såväl människor som institutioner.

Burkert skriver apropå PET:

”Vi kanske betraktar PET som en teknisk uppfinning med vars hjälp vi kan lösa en uppsättning socio-politiska problem. Implementeringen av PET tvingar oss dock – och det kan visa sig vara deras mest betydelsefulla effekt – att bli socialt uppfinningsrika för att få dem att fungera. Här framträder således huvuduppgiften för oss som är vetenskapsmän på det sociala området, jurister, lagstiftare eller personvärnsförsvarare – att acceptera den utmaning som ligger i den nya informationsteknologin som en utmaning i just social uppfinningsrikedom.” (Burkert 1998)

Litteraturförteckning

Aftonbladet, IT-bilagan, augusti 1999.

Agre, Philip E/Rotenberg, Marc (edts). Technology and Privacy: The New Landscape. MIT Press 1998.

Anér, Kerstin. *"Datamakt"*. Gummessons 1975.

Bennet, Colin J. Convergence Revisited: Towards a Global Policy for the Protection of Personal Data? Agre/Rotenberg (edts), The MIT Press 1998.

Bennet, Colin J/Grant, Rebecka (edts). *"Visions of Privacy. Policy Choices for the Digital Age"*. University of Toronto Press, 1999.

Bing, Jon. *"Personvern i faresonen"*, Cappelen 1991.

Blixt, Madeleine. *"Kamera på rätt plats kan förebygga brott"*. BRÅ Apropå nr 5-6/98.

Brin, David. *"The Transparent Society"*. Addison-Wesley 1998.

Brodley, Carla E/Lane, Terran/Stough, Timothy M. *"Knowledge Discovery and Data Mining"*. American Scientist, vol 87. Jan-feb 1999.

Burkert, Herbert. *"Privacy-Enhancing Technologies: Typology, Critique, Vision"*. Agre/Rotenberg (edts) 1998

Burnham, David. *"The Rise of the Computer State"*, Vintage Books 1984.

Castells, Manuel. *"The Rise of the Network Society"*. Blackwell 1996. (Volym 1 i samlingsverket *"The Information Age: Economy Society and Culture"*)

Castells, Manuel. *"The Power of Identity"*. Blackwell 1997. Volym 2)

Castells, Manuel. *"End of Millenium"*. Blackwell 1998. (Volym 3.)

Cavoukian, Ann/Tapscott, Don. *"Who Knows: Safeguarding Your Privacy in a Networked World"*. McGraw-Hill, 1997

Cavoukian, Ann. *"Data Mining: Staking a Claim on Your Privacy"* Information and Privacy Commissioner/Ontario, Canada 1998. http://ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/datamine.htm

Cruz, Caroline. *"Forskningsregister och den personliga integriteten"*, IRI-rapport 1987:9. (IRI = Institutet för Rättsinformatik, Stockholms universitet.)

Datainspektionen. *"Rätten att få vara ifred – tio år med datainspektionen"*, Studentlitteratur 1983.

Davies, Simon. *"Big Brother. Britain´s web of surveillance and the new technological order"*, Pan Books 1996.

Davies, Simon. *"Re-Engeneering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity"*, Agre/Rotenberg (edts) 1998.

Davies, Simon. *"Big Brother at the Box Office. Electronic Visual Surveillance and the Big Screen"*. Paper, 21:st International Conference on Privacy and Personal Data Protection, Hong Kong 13-15 september 1999.

Electronic Privacy Information Center. *"Privacy & Human Rights. An International Survey of Privacy Laws and Developments."* 1999

Flaherty, David H. *"Protecting Privacy in Surveillance Societies"*, The University of North Carolina Press 1989.

Forsberg, Christer. *"Klarar Du kontrollen?"* Statstjänstemannen nr 9/90.

Freese, Jan. *"Data och livskvalitet"*, Publica 1976.

Freese, Jan. *"Kommentar till datalagen"*, Publica 1982.

Freese, Jan. *"Den maktfullkomliga oförmågan"*, Wahlström & Widstrand 1987.

Freese, Jan. *"Makt och ADB"* ur Maktutredningens antologi *"Miljö media makt"*, Carlssons 1990.

Freese, Jan. *"Legitimitet och kontroll"* ur antologin *"Världens största maskin"*, Carlssons 1995.

Givens, Beth. *"The Foundation of Privacy Public Policy"* 1997 www.privacyrights.org

Hixson, Richard F. *"Privacy in a public Society – Human Rights in Conflict"*, Oxford University Press 1987

Hurley, Deborah. Anförande vid *"21st International Conference on Privacy and Personal Data Protection"*, Hong Kong 13-14 sept 1999. Hur-

ley leder ett stort forskningsprojekt om den elektroniska infrastrukturen vid Harvard-universitet, USA.

Ilshammar, Lars/Larsmo, Ola. *"Hur man snärjer Nätets skurkar"*, DN 990309.

Inness, Julie C. *"Privacy Intimacy and Isolation"*. Oxford University Press 1992.

Johansson, Astrid. *"Apoteket vill ha personregister"*. DN 980823.

Larson, Erik. *"The Naked Consumer"*, Penguin 1992.

Lov&Data nr 58, juni 1999. (Skandinavisk tidskrift för rättsinformatik.) *"Nye amerikanske regler mod spamming"*.

Lyon, David. *"The Electronic Eye. The Rise of Surveillence Society"*. Polity Press 1994.

MacNeil, Heather. *"Without Consent. The Ethics of Disclosing Personal Information in Public Archives."* The Scarecrow Press 1992.

Meyer-Schönberger, Viktor. *"Generational Development of Data Protection in Europe"*. Agre/Rotenberg (edts) 1998.

Moore, Barrington. *"Privacy – Studies in Social and Cultural History"*, Sharpe 1984.

OECD. *"Privacy and Data Protection: Issues and Challenges"*, OECD 1994.

Olsson, Anders R. *"Spelrum"*, Askelin & Hägglund 1985.

Olsson, Anders R. *"Yttrandefrihet & tryckfrihet"*, Tiden 1992, ny omarb uppl 1997.

Olsson, Anders R. *"IT och det fria ordet – myten om Storebror"*. Juridik & Samhälle 1996.

Olsson, Anders R. *"Elektronisk demokrati"* Publicerad som SOU 1999:12

Pool, Ithiel de Sola. *"Technologies of Freedom"*, The Belknap Press of Harvard University Press 1983.

Prop 1995/96:90. *"Registerbaserad folk- och bostadsräkning år 2000 m.m."*

Rotenberg, Marc. *"The Privacy Law Sourcebook 1999"*. Electronic Privacy Information Center, 1999.

Samarajiva, Rohan. *"Interactivity As Though Privacy Mattered"*. Ur Agre/

Rotenberg (edts). Technology and Privacy: The New Landscape. MIT Press 1998.

Seipel, Peter (red). *"From Data Protection to Knowledge Machines"* Norstedts 1990.

Seipel, Peter. *"The Technology of Insight: Computers and Informed Citizens"*, Chicago & Kent Law Review vol. 69, no 2.

Seipel, Peter. *"Juristen och datorn. Introduktion till rättsinformatiken"* 5:e uppl, Norstedts Juridik 1994.

SOU 1972:47 *"Data och Integritet"*

SOU 1978:54 *"Personregister-datorer-integritet."*

SOU: 1990:61 *"Skärpt tillsyn – huvuddrag i en reformerad datalag."*

SOU 1993:10. *"En ny datalag"*

SOU 1995:74 *"Lägenhetsdata."*

SOU 1997:49 *"Grundlagsskydd för nya medier."*

SOU 1998:46 *"Om buggning och andra hemliga tvångsmedel"*

Statskontoret. *"Offentlighet & IT"*, Statskontoret 1995.

Svärdkrona, Zendry. *"Så spårar du anonym e-post"*, gräv-SCOOP nr 3/99.

Swire, Peter P./Litan, Robert E. *"None of Your Business. World Data Flows, Electronic Commerce, and the European Privacy Directive"*. Brookings Institution Press 1998.

Tallmo, Karl-Erik. *"Den personliga uppgiften – offentlig, uthängd eller skyddad?"* Tidskrift för Folkets Rättigheter 2/99.

TeknologiNævnet (för Folketinget). *"Hvem ved hvad – og bør de det?"*, TeknologiNævnet 1993.

Thelin, Krister/Olsson, Anders R/Seipel, Peter. *"Klarar den svenska offentlighetsprincipen mötet med Cyberrymden?"*. KFB-rapport 1998:3 och TELDOK Rapport nr 118.

Toffler, Alvin/Toffler, Heidi. *"Tredje vågens samhällsbygge"*. Svenska Förlaget, 1997.

Truedson, Lars. *"Internet och demokratin"*. Världspolitikens Dagsfrågor nr 6/1999. Utrikespolitiska Institutet.

Töllborg, Dennis. ”*Personalkontroll*”, Symposion 1986.
Wallin, Anders. ”*Kriminella teknikzonen*”, IRI-rapport 1994:2.
Willebrand, Peter. ”*IT-spionen*”. Tidskriften Dolly, september 1999.
Åkerman, Nordal (red). ”*Kontroll av individen*”, Prisma 1972.

Telematik 2004 genomförs i samarbete mellan KFB och TELDOK. Programmets utgångspunkt är de förändringar som sker i samband med att Sverige omvandlas till ett informationssamhälle. En viktig aspekt är att IT väntas övergå från att vara expertteknik till att bli massteknik, och de följder detta får.

Programmet bygger på att mycket i informationssamhället år 2004 kan skönjas och granskas i verkliga livet och i demonstrationsmiljöer flera år före år 2004. Inom ramen Telematik 2004 produceras småskrifter och rapporter. Småskrifterna på cirka 30-50 sidor dokumenterar rundabordssamtal och/eller intervjuer där olika åsikter och erfarenheter lyfts fram. Rapporterna på cirka 100 sidor ger en mer heltäckande bild av tidiga användare samt en tydlig framåtblick mot år 2004.

Utgivna publikationer inom programmet Telematik 2004:

Bengt Carlsson	Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier
Sofie Rittfeldt	Allas våra museisamlingar – IT som länk mellan konstmuseers samlingar och allmänheten
Erik Fjellman och Jan Sjögren	Interaktiv underhållning inför framtiden
Anders R Olsson	Privatliv & Internet – som olja och vatten?

telematik 2004

KFB (www.kfb.se) och TELDOK (www.teldok.org) driver fram till mitten av 2001 programmet Telematik 2004 för att finansiera och publicera studier av tidiga användare och användningsområden i ”informationssamhället”. Projekten som finansieras (hittills nio stycken) resulterar i två slags publikationer: ”småskrifter” med samtal och intervjuer (30–50 sidor) samt lite längre rapporter (ca 100 sidor).

Privatliv & Internet – som olja och vatten?

Ju mer vi använder Internet desto fler uppgifter om oss hamnar ”där ute” på nätet. Det gäller innehållet i våra e-brev och namnen på mottagarna, liksom uppgifter om vilka webbsidor vi tittar på – avslöjande allt möjligt från fritidsintressen till politiska åsikter eller sexuella preferenser. Våra möjligheter att kontrollera vad som händer med uppgifterna är försvinnande små.

Denna rapport behandlar problemen med att skydda den personliga integriteten i IT-samhället. Den beskriver riskerna och diskuterar möjligheterna att värna privatlivet med juridiska, tekniska och praktiska metoder.

Rapporten – den fjärde utgåvan i programmet Telematik 2004 från KFB och TELDOK – har skrivits av journalisten och författaren Anders R Olsson (anders.r.olsson@swipnet.se) som länge intresserat sig för frågor om demokrati, personlig integritet och medborgerliga rättigheter.

KFB och TELDOK har tidigare (i programmet Telematik 2001) gett ut debattskriften ”Klarar den svenska offentlighetsprincipen mötet med cyberrymden?” där Anders R Olsson deltar.

KFB & teldok.
KFB-rapport 2000:10 • TELDOK Rapport 133