Efter 11 september 2001:
-Kan Storebror hejdas?

Anders R Olsson

VINNOVA
VERKET FÖR INNOVATIONSSYSTEM
VINNOVA-rapport VR 2003:4
(ISBN 91-89588-89-4)

& teldok.
TELDOK Rapport 149
(ISSN 0281-8574)

TITEL/TITLE
Efter 11 september 2001: – Kan Storebror hejdas?

ISSN
VINNOVA: 1650-3104
ISSN TELDOK: 0281-8574

FÖRFATTARE/AUTHOR
Anders R Olsson

PUBLICERINGSDATUM/DATE PUBLISHED
Februari 2003

SERIE/SERIES
Telematik 2006
VINNOVA Rapport VR 2003:4
TELDOK Rapport 149

UTGIVARE/PUBLISHER
TELDOK och VINNOVA – Verket för Innovationssystem/The Swedish Agency for Innovation Systems, Stockholm

ISBN VINNOVA:
91-89588-89-4

VINNOVAs DNR
341-2002-02064

Formgivning: West studios AB

VINNOVAs uppgift är att främja hållbar tillväxt genom utveckling av effektiva innovationssystem och finansiering av behovsmotiverad forskning

VINNOVA
SE-101 58 Stockholm,
Mäster Samuelsgatan 56
Tel +46 (0)8 473 30 00
Fax +46 (0)8 473 30 05
VINNOVA@VINNOVA.se
www.VINNOVA.se

“In God we trust, all others we monitor.”

Ett motto inom National Security Agency, NSA, från 1970.
(Citerat ur Bamford, 2001.)

Efter 11 september 2001:

– Kan Storebror hejdas?

Anders R Olsson

Telematik 2006

Företal

När måste samhällets behov av skydd mot våldsdåd och annan kriminalitet gå före den enskilde medborgarens behov mot intrång i sitt privata liv?

Frågan är inte ny, vilket decennier av lagstiftningsarbete vittnar om. Redan vad gällt traditionella media och traditionell teknik finns exempel på till synes eviga målkonflikter. Offentlighetsprincipen kan kollidera med Personuppgiftslagen (PUL) så att exempelvis referat från offentliga möten i kommuner och riksdag måste rensas från uppgifter om talarnas partitillhörighet. Samtidigt som Tryckfrihetsförordningen ger obegränsade möjligheter att publicera samma information samt ger uttryckligt skydd åt anonyma uppgiftslämnare till media. Efterhand har dock regelsystem utvecklats för att kunna hantera denna typ av målkonflikter. Ett exempel är att tillstånd för telefonavlyssning prövas av domstol och endast vid grundad misstanke om särskilt allvarliga brott, samt att det finns regler för hur s k överskottsinformation skall avskiljas och förstöras.

Informationstekniken med sin breda spridning över världen har på viktiga punkter ändrat förutsättningarna och flyttat hävdvunna gränser.

Rapporten ”Efter 11 september 2001: – Kan Storebror hejdas?” av Anders R Olsson har tillkommit i ljuset av den internationella utvecklingen efter ödesdigra 11 september. Av väl kända skäl har samhällets behov av skydd mot våld och terror kommit i förgrunden, och frågorna kommit att få räckvidd långt utanför nationella gränser. En tyngdpunktsförskjutning som av döma av samhällsdebatt och media kommit att bli ganska allmänt accepterad som något av en bister nödvändighet. Det är i dagsläget klart svårt att peka på några realistiska alternativ, utan att därmed riskera att eftersätta legitima skyddsbehov.

Rapporten handlar om hur den polisiära övervakningen av medborgarna i västvärlden förändras – vad gäller omfattning, inriktning och teknisk form – i en epok som främst präglas av två skeenden. Det

ena är IT-samhällets framväxt där alltfler människor kommunicerar alltmer information om sig själva, och avsätter spår av sina aktiviteter, i elektroniska nätverk. Det andra är ”kriget mot terrorismen”.

För den som fäster vikt vid integritetsskydd – möjligheten att värna en personlig sfär, att söka information i diskreta former och att sprida kunskaper eller åsikter anonymt – ter sig framtidsutsikterna mörka, enligt Anders R Olsson. Eftersom tekniken och det politiska klimatet idag så medger utökas de polisiära möjligheterna för övervakning. Bevakningen tycks utvidgas av de kategorier människor som anses utgöra potentiella hot och som därför bedöms kräva särskilt strängt övervakning. Idag betonas allt starkare de polisiära organens uppgift att förebygga brott, vilket fordrar ökad tillgång till bred information.

VINNOVA och TELDOK anser att dessa frågor är viktiga att debattera. Genom att publicera rapporten fortsätter vi en utgivning som igångsattes för några år sedan i en den gemensamma serien av Telematik-rapporter.

Hovrättsrådet Krister Thelin skrev i rapporten: ”Klarar den svenska offentlighetsprincipen mötet med Cyber-rymden?” (februari 1998, TELDOK nr 118), och gav underlag för en offentlig debatt med Anders R Olsson som diskussant. De utgick från bl a skilda ideologiska utgångspunkter.

Anders R Olsson skrev därefter en egen rapport med titeln ”Privatliv & Internet – som olja och vatten?” (TELDOK rapport nr 134).

Vi hoppas att Anders R Olssons nya rapport ger god grund för eftertanke.

Bertil Thorngren
Ordförande
Föreningen TELDOK

Karl-Einar Sjödin
Enhetschef
Enheten för Tjänster & IT-användning
VINNOVA

Innehåll

Företal 3

Innehåll 5

Sammanfattning 7

Inledning 8

Kapitel 1. Personlig integritet i Sverige 2003 11

Kapitel 2. Vad rapporten handlar om 17

Kapitel 3. Kan Internet-aktivitet regleras rättsligt? 20
3.1 Bakgrund 20
3.2 Internationellt samarbete – förutsättningar, erfarenheter. .. 22
3.3 Internationellt samarbete – risker, möjligheter 25

Kapitel 4. Övervakandets dystra historia 31
”Dubbla budskap från regeringen” 32
Missbruk av telefonavlyssning 33

Kapitel 5. NSA och Echelon 34

Kapitel 6. USA och reaktionerna på 11 september 40

Kapitel 7. Europa efter terrordåden 51

Kapitel 8. Sverige avvaktar 55

Sammanfattning

Rapporten handlar om hur den polisiära övervakningen av medborgarna i västvärlden förändras – vad gäller omfattning, inriktning och teknisk form – i en epok som främst präglas av två skeenden. Det ena är IT-samhällets framväxt där alltfler människor kommunicerar alltmer information om sig själva, och avsätter spår av sina aktiviteter, i elektroniska nätverk. Det andra är det ”krig mot terrorismen” som USA har förklarat, och som den övriga västvärlden med varierande entusiasm engagerar sig i.

För den som fäster vikt vid integritetsskydd – möjligheten att värna en personlig sfär, att söka information i diskreta former och att sprida kunskaper eller åsikter anonymt – ter sig framtidsutsikterna mörka. Eftersom tekniken och det politiska klimatet så medger utökas de polisiära möjligheterna till övervakning. Det sker mindre genom tydliga politiska beslut om sådan övervakning än genom åtgärder som indirekt får den effekten. Ett exempel är att ”avlyssningsvänliga” tekniska lösningar blir standard för internationella kommunikationssystem. Ett annat är att de kategorier människor som anses utgöra potentiella hot och som därför kan övervakas särskilt strängt utvidgas. Ett tredje är att man allt starkare betonar de polisiära organens uppgift att förebygga brott, vilket fordrar tillgång till information om mycket bredare grupper av människor än de som misstänks för att bryta mot lag.

Sverige kan hittills sägas inta en avvaktande hållning, jämfört med USA och dominerande EU-länder som Tyskland och Storbritannien. Den svenska linjen tycks dock inte innebära något motstånd eller någon konsekvent kritik av utvecklingen som den skisseras ovan. Inom EU, Europarådet och andra internationella organ fattas nu många av de viktiga besluten och därmed tycks det mest vara en tidsfråga innan Sverige, även vad gäller polisiär övervakning, ”harmoniseras” med tongivande stater i västvärlden.

Inledning

Vår användning och vårt beroende av elektronisk kommunikation ökar. Alltfler arbetsuppgifter fordrar nyttjande av mobiltelefon och uppkoppling till Internet. Med piska och morot – fysiska butiker/kontor stängs medan Internet-kunder får rabatt – flyttas människor som köper varor och tjänster över till nätmiljön. Elektroniska kommunikationsnät blir således nödvändiga och självklara i vår vardag, och i dessa nät strömmar alltmer personuppgifter. Vad vi köper, läser och tittar på, vilka vi kommunicerar med, hur vi förflyttar oss geografiskt – allt kan undersökas via elektroniska spår i själva näten.

Entusiasterna talar om dessa nät som en befriande teknologi. Vi kan söka och nå människor över hela världen, vi har fått ofantliga mängder kunskap ”på några knapptryckningars avstånd” och vi kan både kritiskt granska och påverka maktutövning på alla nivåer. Skeptikerna beskriver samma teknologi som disciplinerande eller t o m förtryckande – vi blir alltmer åtkomliga, alltmer påpassade, alltmer genomskinliga, alltmer utlämnade. Åtminstone i teorin öppnar IT-samhället för en enastående effektiv övervakning av varje individ.

Just övervakning och kontroll är temat för denna rapport. I vilken utsträckning kan och får polis- och säkerhetsorgan dra nytta av det faktum att alla människor, praktiskt taget, tvingas kommunicera allt mer uppgifter om sig själva i elektronisk form? Perspektivet är främst rättsligt och rättspolitiskt.

Med givna begränsningar i tid och resurser för undersökningen – rapporten har skrivits på två månader – har avgränsningar i studiens omfattning varit nödvändiga. Uppdragsgivaren Vinnova har förklarat sig främst intresserad av den allra senaste utvecklingen – efter terrordåden i USA den 11 september 2001. Perspektivet bakåt blir därför relativt kort, även om det vore orimligt att börja framställningen vid ett specifikt datum. Kampen mellan de samhällsintressen som verkar för en tilltagande övervakning av medborgarna och de intressen som söker stå emot har pågått länge. Även om terrorat-

tackerna i USA självfallet hade effekter för denna kamp, så att den ena sidans argument under en tid har fått större tyngd och den andra sidans mindre, kan man ännu inte säga – åtminstone inte i Sverige – att vi lever i en ny tid vad integritetsskydd beträffar. I USA och inom EU har man reagerat på 11 september med en rad reformer som medger och underlättar övervakning, och fler sådana förbereds. Det lär dock dröja ytterligare något eller några år innan de rättspolitiska effekterna av terrordåden kan sammanfattas.

Såväl den politiska som den rättsliga aktiviteten är hög. En rad samhälleliga och juridiska förändringsprocesser – direkt eller indirekt motiverade som terroristbekämpning – har alltså inletts men inte avslutats. Nya lagar som medger utvidgad övervakning har stiftats i flera länder men hur de kommer att tillämpas vet vi ännu inte. Andra regelverk föreligger ännu bara som förslag. Ytterligare andra övervakningsprojekt – som det amerikanska försvarets Total Information Awareness, TIA – får sannolikt betecknas som taktiska utspel eller idéskisser snarare än konkreta planer.

I USA är det många som anser (se kapitel 6) att man verkligen lever i en ”ny tid” efter terrordåden. Regeringen Bush hävdar att landet är i krig (låt vara att det är ett retoriskt grepp – inget krig har formellt förklarats, krigstillstånd råder inte) och har i allt väsentligt fått parlamentets stöd för en hårdför politik såväl inrikes som utrikes. Vissa förändringar har påtvingats omvärlden med våld – det militära angreppet på Afghanistan med påföljande regimskifte i landet har varit det hittills mest dramatiska – medan annan påverkan har skett med t ex ekonomiska dekret (frysning av individers eller institutioners tillgångar) eller regeländringar inom flygets område. Det flygbolag som inte förbättrar säkerheten nekas tillstånd att trafikera USA. Flygbolagen accepterar utan diskussion sådana krav. Även här illustreras dock svårigheten att skilja effekter av 11 september-terrorn från drivkrafter av annat slag. Under andra halvåret 2002 flyttades USA-regeringens fokus från Afghanistan till Irak, vars ledare visserligen anklagas för många illgärningar men inte för terrorism i vedertagen mening.

Temat ”övervakning och internationell politik” är svårbehandlat av flera skäl. Även om USA har ambitionen att förmå länder som Sverige att i terroristbekämpningens namn ge polis och säkerhets-

polis bättre tillgång till elektroniska spår, för att sedan dela med sig till amerikanerna av den kunskap som utvinns, är det en politiskt känslig fråga. För påtryckningar mot europeiska länder kan inte samma medel användas som mot mindre länder i tredje världen. Diplomatins kvarnar mal ofta långsamt och politisk prestige står på spel. Skulle Sverige ge efter för amerikanska krav torde reformerna motiveras med att svenskarna behöver dem, inte att de utgör en eftergift till USA. (Vidare om internationellt samarbete, se kapitel 3.)

Därtill kommer den i sig snabba tekniska utvecklingen. Förutsättningarna för övervakning av medborgarna ändras hela tiden, liksom möjligheterna för enskilda att dölja sina handlingar och skydda sitt kommunicerande.

Föreliggande arbete är alltså en lägesrapport. Det enda man med säkerhet kan säga om framtiden är att det snart kommer att behövas en ny, uppdaterad rapport.

Kapitel 1.

Personlig integritet i Sverige 2003

Ända sedan man på 1960-talet började diskutera datortekniken ur ett samhälleligt perspektiv har begreppet ”personlig integritet” framstått som centralt. Dess exakta innebörd var – och är fortfarande – svårfångad. Det handlar dock om människans behov av att i viss mån kontrollera sina livsvillkor och sin interaktion med andra, att upprätthålla en värdighet bl a genom att värna sitt privatliv.

Särskilt på 1960- och 70-talen var det riskerna för en utveckling mot mer auktoritära styrelseskick som stod i centrum för debatten. Begreppet Storebror användes då, efter den allseende diktatorn i Orwells roman ”1984”, som beteckning för en alltmer kontrollbenägen överhet, särskilt en statlig sådan. Denna problematik är mer aktuell än någonsin. (Tydligast illustreras den kanske av det internationella övervakningssystem som kallas Echelon, med USA:s spionorgan National Security Agency, NSA, som spindel i nätet. Se kapitel 5.)

Med tiden började det stå klart att Storebrors-problematik kunde uppstå också när tekniska system togs i bruk för de mest behjärtansvärda ändamål. Trafikövervakning som syftar till lägre hastigheter, bättre framkomlighet och snabbare utryckning vid olyckor visar sig också möjliggöra en exakt övervakning av enskildas geografiska förflyttningar. De övervakningskameror på allmänna platser som blir alltfler får samma dubbla funktion – trygghetsskapande men också potentiellt integritetskränkande.[1]

Det är värt att erinra om att den livliga svenska debatten om integritetshot fick ett närmast abrupt slut med den s k Metropolit-skandalen 1986. Metropolit var ett sociologiskt forskningsprojekt vid Stockholms universitet och byggde på stora mängder personuppgif-

[1] Brin, David. ”The Transparent Society”. Addison-Wesley 1998. Här diskuteras också övervakningskamerornas eventuella uppkoppling mot Internet i framtiden.

ter, insamlade i hemlighet, om 15 000 individer födda i Stockholms län 1953. Efter proteststormen 1986 tvingades man avidentifiera personregistret och i praktiken avsluta projektet. Sedan dess har ingen stor debatt eller journalistisk kampanj förts på integritets-temat. Uppenbarligen har något slags skov inträtt i det allmänna medvetandet som ändrat förutsättningarna för offentlig diskussion i frågan. Ett förslag som 1983 avvisades som en skandal – att ordna en folk- och bostadsräkning genom samkörning av olika myndigheters personregister istället för det omständliga och mycket dyrare utskickandet/insamlandet av pappersblanketter – antogs av riksdagen 1995 utan någon offentlig debatt överhuvudtaget.[2]

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 både skada och spionera på individen B.

Den ”nya ekonomin” drar alltmer kraftfullt människor in på Nätet. Bankerna liksom andra tjänsteproducenter lägger ner sina kostsamma fysiska kontor och ger Internet-kunder förmåner av olika slag. Människors alltmer splittrade mediekonsumtion – det finns inte längre några TV-program som ”alla” tittar på eller tidningar som ”alla” läser – i kombination med att handeln samlar alltmer information om kunderna och att transaktioner i växande utsträckning bedrivs on-line aktualiserar en rad integritetsproblem. En tydlig trend är att företagen får ökande behov av kunskap om såväl etablerade kunder – för att tillmötesgå deras alltmer detaljerade önskemål – som potentiella.[3] Om de förra måste man skaffa alltmer individ-anknuten kunskap för att skräddarsy produkterna. De senare måste man ha detaljerad kunskap om för att kunna sända dem reklambudskap med ökad precision. (För företaget som säljer dykarutrustning är det inte rimligt att satsa stora pengar på en halvsidesannons i Dagens Nyheter. Drömmen för företaget vore istället att få en förteckning över alla i Sverige som har dykarcertifikat, deras ålder, inkomst och uppgift om när de köpte sin utrustning. Då kunde man med direktreklam nå

[2] Prop 1995/96:90. ”Registerbaserad folk- och bostadsräkning år 2000 m.m.”

[3] Samarajiva, Rohan. ”Interactivity As Though Privacy Mattered”. Ur Agre/Rotenberg (edts). Technology and Privacy: The New Landscape. MIT Press 1998.

praktiskt taget alla potentiella kunder med rätt budskap och vid rätt tillfälle.) Såväl e-handelns som den vanliga handelns aktörer får således starka ekonomiska incitament att bedriva närgången kartläggning av konsumenter.

På många håll i den offentliga sektorn arbetar man med att utveckla service och tjänster via Nätet.[4] EU söker bidra till denna utveckling och i ett internationellt perspektiv ligger Sverige långt framme.[5] Enligt en undersökning från hösten 2002 är vi t o m världsledande när det gäller andelen medborgare (57%) som via nätet har tillgång till information och tjänster från myndigheter.[6] Syftet med satsningen är dubbelt, både att erbjuda bättre offentlig service och att göra ekonomiska besparingar. När säker kommunikation blir lätt tillgänglig för alla – så att även gemene man kan framställa elektroniska signaturer och autentisera digitala dokument – kommer svensken att kunna sköta de flesta myndighetskontakter via Nätet. Ska nätbaserad offentlig service leda till besparingar för det allmänna måste den fysiska/personliga servicen successivt trappas ned. Att bygga nya kontor i ”cyberrymden” utan att lägga ned de gamla skulle inte ge sänkta totalkostnader. Mycket talar för att det inom överskådlig tid – en rimlig gissning kan vara 5-10 år – blir rättsligt påbjudet för medborgarna att kommunicera stora mängder personlig information via Nätet.

För att hantera de problem kring integritetsskydd som följer med IT-utvecklingen finns idag ingen organiserad kunskapsuppbyggnad. Inte ens inom avgränsade discipliner – teknik, juridik, sociologi, psykologi m fl – pågår forskning om integritetsskydd med någon högre ambitionsnivå. Bortsett från ett mindre, Vinnova-finansierat projekt vid Swedish Institute of Computer Science, SICS, saknas helt tvärvetenskaplig forskning.[7]

---

[4] Se bl a Statskontorets rapport om 24-timmars-myndigheten: http://www.statskontoret.se/cgi-bin/bokhandel/index.cgi).

[5] Sinter, Therese. ”Svenska 24-timmarsmyndigheter klättrar mot Europatoppen”. Öppna System nr 3/2002. (Statskontorets tidskrift.)

[6] Undersökningen utfördes av Taylor Nelson Sofres och refereras i Computer Sweden 2002-11-12.

[7] Projektets namn är SAITS (Skydd av Användare i IT-Samhället). Se: http://www.sics.se/projects/saits.html.

För den som sedan 1970-talet har följt (och ofta skrivit om) integritetsfrågorna i Sverige är det slående hur det ideologiska klimatet har svängt. Här finns inte anledning att djupare spekulera i orsakerna till klimatförändringen, men åtminstone tre faktorer som bidrar till att människor accepterar övervakning kan urskiljas:

A. Bekvämlighet. Att betala med plastkort, att beställa via Internet, att överallt kunna nås via mobiltelefon, att identifiera sig biometriskt för snabbare service, allt gör att vi sparar tid och möda. Samtidigt lämnar vi alltfler elektroniska spår efter oss i olika kommunikationsnät som visar vad vi köper, vad vi gör och hur vi förflyttar oss.
B. Trygghet är kanske den viktigaste faktorn. Människor accepterar uppenbarligen i starkt ökad utsträckning kontroll – i form av t ex kameraövervakning på allmän och privat plats – i utbyte mot säkerhet, eller åtminstone en känsla av säkerhet. Forskningen kring kameraövervakningens effektivitet som brottsförebyggande teknik tycks inte ge entydiga resultat.[8] Hur denna attitydförändring i sin tur ska förklaras är inte givet. När rädslan för att utsättas för brott ökar avsevärt mer än den faktiska risken kan det tolkas som ett resultat av nyhetsmedias allt hårdare exploatering av de våldsbrott som begås. Våld säljer, och mediekonsumenter som inte ser/förstår nyhetsförmedlingens kommersiella förutsättningar får lätt en snedvriden bild av hur farligt Sverige är att leva i. Ett annat sätt att beskriva samma utveckling kan vara att människors tilltro till staten – att den skyddar, att dess företrädare inte missbrukar sina befogenheter – har ökat.
C. Rättvisekrav. Med sociala skyddsnät som ska träda i funktion vid t ex sjukdom eller arbetslöshet uppstår, oberoende av om de är offentligt eller privat organiserade, risken för fusk. Hårdare kontroll av om den sjuke verkligen är sjuk och om den arbetslöse verkligen avhåller sig från arbete accepteras av det stora flertalet med hänvisning till att fusk oundvikligen drabbar de icke fuskande. Här har också skett en förändring i den allmänna opinio-

[8] Blixt, Madeleine. ”Kamera på rätt plats kan förebygga brott”. BRÅ Apropå nr 5-6/98. Se också: ”Privacy & Human Rights.” Electronic Privacy Information Center, Washington DC, USA, 2002. Sid 54-55.

nen. Samkörning av olika register i kontrollsyfte ansågs så sent som på 1980-talet oacceptabelt, särskilt i politiskt borgerliga kretsar. Vid 2000-talet början kan sådana tongångar sällan spåras på tidningarnas ledarsidor.[9]

[9] Istället låter det allt oftare som hos Göran Skytte, ”Den som fuskar stjäl alltid från folket”, Svenska Dagbladet 021026.

Kapitel 2.
Vad rapporten handlar om

En huvudmotsättning i vår tids politiska filosofi är den mellan människors behov av frihet och deras behov av att ingå i ett fungerande kollektiv som erbjuder materiell trygghet/säkerhet. Den motsättningen är, kan man säga, ovanligt framträdande i frågan om polisiära befogenheter contra medborgerliga fri- och rättigheter.

Här ska främst studeras de polisiära befogenheterna och möjligheterna till övervakning och kontroll i den nya värld där våra personuppgifter är ”överallt”: i USA, inom EU och med ett särskilt avsnitt om Sverige. Perspektivet är således rättsligt och kommer (av tidsskäl) att koncentreras till polis och säkerhetspolis. Brottsbekämpning med inslag av övervakning förekommer också hos militär, tull, skatteväsende och andra myndigheter, men skelettet i ”lagens långa arm” utgörs ändå av polis/åklagare/domare.

En annan viktig konsekvens av att ”alla” finns på nätet är att ”alla” kan begå yttrandefrihetsbrott så mycket enklare. Problemen med sådant som barnpornografi och rasistisk propaganda är hett omdiskuterade och i åtminstone ett par europeiska länder (Tyskland, Frankrike) har domstolar beordrat företag som erbjuder Internet-uppkoppling (s k ISP-företag) att blockera vissa webbplatser så att människor inom domstolarnas jurisdiktion inte kan nå dem. Frågan om huruvida statsmakten ska bestämma om filtrering/styrning av information i kommunikationsnäten är också en Storbrors-problematik, men kan här bara behandlas översiktligt. (Se kapitel 3)

Det måste vidare understrykas att besluten om övervakningslagar – vilka statliga organ som får göra vad, hur och när – s a s skjuter på ett rörligt mål. Den tekniska verklighet i vilken lagarna ska tillämpas förändras kontinuerligt. När åklagaren Kenneth Starr i januari 1998 påbörjade sin utredning om huruvida USA:s president Bill Clinton hade ljugit under ed när han svarat på frågor om utomäktenskapligt sex, ledde det snart till husrannsakan hos Monica Lewinsky, prakti-

kant i Vita Huset. Lewinskys persondator beslagtogs och allt som fanns på hårddisken granskades i detalj. I Starrs slutrapport, som blev offentlig, kunde man sedan läsa inte bara hennes privata anteckningar och de e-brev som Lewinsky hade skickat till Clinton utan också de e-brev som hon skrivit men aldrig sänt iväg. Texter som hon slängt i den virtuella papperskorgen, som hon kanske aldrig hade avsett att visa för någon annan, kunde återvinnas genom en ”dammsugning” av hårddisken. (Det man tar bort genom att ”slänga” texter är ju inte innehållet i en fil eller ett dokument utan adressen, informationen om var på hårddisken uppgifterna ligger.) Den uppseendeväckande kränkningen av Lewinskys integritet blev möjlig därför att tekniker långt tidigare hade gjort ett begripligt men inte nödvändigt val. Att radera/skriva över själva texten i ett dokument framstår ur teknisk synvinkel som en aning opraktiskt – det tar vanligen längre tid än att radera/skriva över datorns interna adress till dokumentet – men den dag efterfrågan uppstår på ett mer effektivt suddnings-kommando kan det lätt ordnas. I en värld där husrannsakan allt oftare tar sikte just på hårddiskars innehåll får frågan allt större betydelse.

Ett annat exempel på viktiga tekniska beslut är utformningen av nästa s k IP-protokoll för Internet, på fackspråk IPv6. Det kommer bl a att innebära en större träffsäkerhet vad gäller möjligheten att geografiskt lokalisera en person som använder nätet.[10]

All utveckling i IT-samhällets tekniska infrastruktur innebär således att val träffas, och den strukturen blir aldrig färdig. Beslut som får stor betydelse för möjligheterna att övervaka medborgare har hittills fattats fortlöpande av människor med tekniskt snarare än juridiskt eller politiskt kunnande och i miljöer där funktionalitet, kostnadspress och säkerhet har stått högt på dagordningen men knappast demokratiska grundfrågor. Politiska aktörer börjar nu tränga in i dessa processer (se främst kapitel 3 nedan). Hur själva näten utveck-

[10] För en genomgång av tekniska och juridiska aspekter på IPv6, se: Alberto Escudero-Pascual. ”Privacy in the next generation Internet. Data protection in the context of European Union Policy.” Kungliga Tekniska Högskolan, Stockholm, december 2002.

Se också utlåtandet från EU:s s k Artikel-29-grupp – bestående av datainspektörer som fokuserar bl a på frågor om integritetsskydd & telekommunikationer – av den 30 maj 2002: ”Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6”. Finns tillgängligt på: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

las ur demokratisk synvinkel – dess standarder, tekniska protokoll m m – vore således värt en egen rapport.

Till sist måste här påpekas att utvecklingen kommer att tvinga fram ställningstaganden i en rad principiellt viktiga frågor. Det gäller sådant som:

- Innebörden av begreppet personlig integritet (”privacy”). Var går egentligen gränserna för jaget och därmed för kränkningar av integriteten? Om ICA med hjälp av stora mängder data om mina livsmedels-inköp gör en ”profil” av mig som konsument – är det integritetskränkande? Beror svaret på frågan – kränkande eller inte kränkande – på i vilket syfte det sker? Är syftet att skicka direktreklam till mig godtagbart medan en samkörning med SÄPO:s uppgifter om kända terroristers livsmedelsinköp – i syfte att utröna om jag oavsiktligt, genom min konsumtion röjer farliga/destruktiva böjelser – inte är det? Flygbolagen (i vart fall i USA) arbetar nu intensivt med att utveckla ”profiler” för att bättre kunna urskilja sådana passagerare som bör granskas särskilt noga innan de släpps ombord. Är det kränkande? Är det i så fall en kränkning som vi måste acceptera?
- Effekter av nya metoder för identifiering av enskilda. I Tyskland har parlamentet beslutat införa ID-kort för medborgarna med s k biometriska data, dvs information om individens fysiskt unika egenskaper. Exakt vilka fysiska egenskaper som ska registreras är ännu inte bestämt. Ett par av alternativen är fingeravtryck och blodkärlens mönster i ögat. Låt säga att man väljer fingeravtryck. När ett allvarligt brott ska utredas hittar man många gånger fingeravtryck från flera personer på brottsplatsen. Har man i framtiden kunskap om alla medborgares fingeravtryck kommer samtliga personer som lämnat avtryck på brottsplatsen att identifieras och kontaktas med krav på en förklaring: -När var ni på brottsplatsen och varför? I tysk debatt diskuteras huruvida detta inte leder till en omvänd bevisbörda – istället för att polis/åklagare ska bevisa att X är skyldig åläggs i praktiken X att bevisa sin oskuld.[11]

[11] Personlig intervju med Dr Alexander Dix, Landesbeauftragter für den Datenschutz und für das Recht auf Akteninsicht, Brandenburg. Kleinmachnow 2002-11-08. Dix är således chef för en delstatsmyndighet som har till uppgift både att värna enskildas personliga integritet och att kontrollera att regler om handlingsoffentlighet följs.

- Etablerade principer och gränser för polisiär övervakning blir svåra att upprätthålla. En i Europa särskilt kontroversiell fråga är huruvida teleoperatörer ska vara skyldiga att spara trafikdata under längre tid för den händelse uppgifter senare skulle behövas i polisens utredningar. (Se kapitel 7) Det gäller således inte innehåll i det som kommunicerats utan uppgifter om kommunikation. Eftersom innehåll av tradition har ansetts så mycket känsligare ur integritetssynpunkt har t ex telefonavlyssning bara medgivits vid utredningar om särskilt grova brott, medan telefonövervakning (uppgifter om den misstänktes telefonsamtal) har ansetts godtagbart i betydligt fler fall. Att överföra denna etablerade princip på e-post är emellertid inte lätt. Visserligen kan den s k headern, som rymmer information bl a om brevets avsändare och mottagare, enkelt skiljas från innehållet, men headern rymmer så mycket mer. Bl a finns där en innehållsrad (subject-line) som oftast avslöjar mycket om innehållet. Alla någorlunda erfarna e-postanvändare har lärt sig att med få ord framföra budskap i innehållsraden, eftersom risk annars finns att meddelandet i mottagarens överfyllda brevlåda slängs eller i vart fall inte uppmärksammas.

Andra gränser av stor betydelse för övervakningen av medborgarna är de mellan 1) inrikes brottsbekämpning (polisens uppgift), 2) vakthållning mot spioneri och annan icke-militär verksamhet som kan undergräva statsskicket eller nationens säkerhet (SÄPO:s uppgift), och 3) informationsinsamling syftande till att klarlägga militära hot mot landet (militär underrättelseverksamhet). I alla tre verksamheterna kan övervakning av Internet-trafik motiveras. Det är inte självklart var/hur terrorism-bekämpning ska bedrivas (som 1, 2 eller 3?) eller i vilken utsträckning ett övervakningsorgan bör få dela med sig av inhämtad kunskap till ett annat. Särskilt i amerikansk politik är dessa frågor omtvistade.

Kapitel 3.

Kan Internet-aktivitet regleras rättsligt?

All övervakning i vår tid handlar förvisso inte om Internet, men uppenbarligen är ”cyberspace” det nya och svåra området. Övervakningen med kameror tilltar på gator och torg, telefoner avlyssnas i ökande utsträckning[12] och papperspost kan fortfarande öppnas med domstols tillstånd, men här har principfrågorna diskuterats under en längre tid. Här finns utredningar, utvärderingar, principuttalanden, lagar och rättsfall.

Internet är något så torrt och artificiellt som en teknisk plattform för kommunikation, men samtidigt en utmaning mot den etablerade ordningen – det står över såväl nationella gränser som mediegränser. Med digitalisering av gamla medier som telefon, radio och TV kan deras innehåll, liksom mycket annat, distribueras via Nätet vart som helst i världen. Vad plattformen möjliggör bestäms inte – hittills, åtminstone – i politiskt kontrollerad ordning. Därmed ställs jurister och lagstiftare inför en rad svårlösta frågor.

3.1 Bakgrund

Av många har problemen med att rättsligt reglera Internet-aktivitet beskrivits som politiskt oöverkomliga, vilket, åtminstone på 1990-talet, fick anarkister och nyliberaler att jubla. Cyberrymden framstod som oåtkomlig för regeringar, poliser, storföretag och annan förtryckande överhet. Därmed kunde yttrande- och informationsfrihet inte kvävas. Anonymitet var möjlig. Den många gånger publicerade skämtteckningen visar Fido vid datorn: ”På Internet vet ingen att du är en hund.”

[12] Enligt uppgifter från Rikspolisstyrelsen och Riksåklagaren, refererade i Dagens Nyheter 2002-09-04, medgav svenska domstolar hemlig teleavlyssning i 398 fall under 2001. Det var en ökning med 25 procent jämfört med 2000 och med 60 procent jämfört med 1999.

Nu mognar dock både tekniken och dess användare och nackdelarna med ett ”oreglerat” Internet börjar framträda. Så länge ingen demokratiskt vald person/församling kan bestämma över nätet blir det närmast omöjligt att hindra polisiära och militära organ från att övervaka och avlyssna trafiken där.

Det blir alltmer uppenbart att tekniken i sig inte upplöser maktstrukturer. Hur fri eller ofri den värld blir som befolkas av människor bestäms av människor. I bästa fall bestäms det demokratiskt. Att så många illusioner föddes med Internet kanske var begripligt, men nu skingras de en efter en.

Då främst amerikanska nördar, dvs datorfrälsta utanför de akademiska och militära etablissemangen, på 1980-talet alltmer började använda telenäten för datorkommunikation blev Vilda Västern-mytologin den självklara referensen. Lagar fanns inte i nybyggarland och just därför var människorna fria. Nu var det cyberrymden som skulle erövras, bebyggas och befolkas av individer, för individer – utan överheter.

Konfrontationer blev oundvikliga. När den amerikanska lagens långa arm vid 90-talets början trevade ute i cyberrymden, ofta klumpigt, ofta på fel ställen, med påståenden om förtal, bedrägerier och upphovsrättsintrång mobiliserades motståndet. John Perry Barlow – sångtextförfattare åt Greatful Dead, farmare och agitator – bildade tillsammans med miljardären Mitch Kapor ”The Electronic Frontier Foundation” (EFF). Uppgiften var att försvara fri- och rättigheter i den ”nya” världen. (Engelskans ”frontier” är just vilda-västern-epokens begrepp – fronten i erövrandet av nytt territorium – men används dubbeltydigt. Det som erövras är samtidigt nya insikter.)

Här började en kamp om cyberrymden som fram till mitten av 90-talet, när nördar och akademiker fortfarande dominerade Nätet, tycktes möjlig att vinna. Deras motståndare, ”de trötta jättarna av kött och stål” för att citera Barlows smått klassiska ”Deklaration om cyberrymdens oberoende” från 1996, förstod inte ens elementa om tekniken. Länder i Nordamerika och Europa lanserade den ena lagen efter det andra för att skapa ordning och samhällelig kontroll över Internet, och regelverken förvandlades ofta till pinsamheter. Sverige fick en ”Lag om elektroniska anslagstavlor” (SFS 1998:112) och därefter Personuppgiftslagen, PUL (SFS 1998:204). USA antog

en ”Communications Decency Act” som i stora delar underkändes av Högsta Domstolen. Lösningen visade sig vid närmare påseende oförenlig med USA:s konstitution.

Nu byggs emellertid det tekniska kunnandet upp i myndigheter och på företag och det blir uppenbart vilka som har både viljan och resurserna att utöva makt i cyberrymden. Förvisso är Internet ett nytt medium som, beroende på hur man vill utnyttja det, fordrar nytänkande och samarbete över vetenskapliga och nationella gränser, men utopisternas tid är förbi.

3.2 Internationellt samarbete – förutsättningar, erfarenheter.

För en nykter och kompetent genomgång av lagstiftandets möjligheter och begränsningar i Internet-eran svarar Stuart Biegel, jurist och lärare vid University of California, Los Angeles. I boken ”Beyond Our Control?” går han igenom rättsfrågorna en i taget och gör när så behövs utflykter från den juridiska sfären för att diskutera hur lagstiftningen hänger samman med politiska, tekniska eller ideologiska problem.[13]

Att Vilda Västern var fri därför att den var laglös är således en föreställning som Biegel finner tvivelaktig. Temat bearbetas f ö i åtskilliga klassiska Västern-filmer – Biegel nämner bl a Shane (med Alan Ladd) och The Man Who Shot Liberty Valance (James Stewart, John Wayne). Där illustreras snarare tesen att frihet uppnås genom kollektivet. Fri var möjligen den geografiskt rörlige, skjutskicklige man som bara hade ansvar för sig själv. All annan frihet måste skyddas kollektivt, med lag och sheriff.

I takt med att såväl politikers, de ekonomiska eliternas som allmänhetens IT-mognad tilltar, blir det allt svårare att försvara ståndpunkten att cyberrymden inte *går* att reglera. För det första beror Nätet av fysiska aktörer – företag och individer – som är i högsta

[13] Stuart Biegel. ”Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace”. MIT Press, 2001.

grad reglerade. De konstruerar, patenterar, bygger, säljer och installerar teknisk utrustning och lyder i varje steg under sina länders lagar. Gårdagens krav på elsäkerhet, barnsäkerhet och konsumentskydd gäller. Frågan är inte *om* utan *vilka* nya krav vi får med IT-samhället. Servrar och ledningar finns inte i någon ”rymd”. Den som kan stänga av strömmen kan stänga av Nätet.

För det andra – och det är viktigare – stiftas lag också genom programmering. Det blir bara lagar av annan natur. Som påpekades i kapitel ovan bestämmer konstruktören av ett IT-system vad som kan och inte kan göras med det. Internet är en rent artificiell konstruktion baserad på standarder, protokoll och outtalade principer. Konstruktionens ”ritning” växte fram för många år sedan bland experter som inte anade att nätet senare skulle användas av alla människor och för alla syften. I tron att användarna var få och tekniskt kvalificerade konstruerades Internet för öppenhet – flertalet servrar använder program vars källkod är fritt tillgänglig, gratis. Censurfientligt blev nätet för att skapa maximal driftsäkerhet. Det föddes ju en gång hos militären, vars kommunikationsnät måste fungera även när flera noder slagits ut.

Egenskaperna är således inte givna. Internet kan i teorin konstrueras hur ”fritt” eller ”övervaknings-vänligt” som helst. Man kan jämföra med telefonnätet. Inget säger att systemets växlar måste registrera, för kontroll i efterhand, vilken abonnent som har ringt en annan, när och hur länge. Men det gör de.

Nu önskar starka samhällsaktörer förändringar i Internets tekniska arkitektur. Dess standarder och protokoll uppdateras fortlöpande allteftersom informationsvolymen sväller och alltmer sofistikerad verksamhet flyttas ut på Nätet. Teknisk och administrativ modernisering sker idag genom arbete i en rad för allmänheten okända grupper som förkortas ISOC, ICANN, AIB, IETF och W3C. De ska, brukar det heta med vackra men oprecisa formuleringar, utveckla ett fritt, maximalt tillgängligt och säkert Internet.

Frågor om hur grupperna ska utses, vilka mandat de ska ha och med vilken öppenhet de ska arbeta diskuteras livligt. Insikten att det inte finns någon ”neutral” eller ”opolitisk” teknisk arkitektur för Internet börjar sprida sig, framförallt sedan den amerikanske juridikprofessorn Lawrence Lessig publicerade boken ”Code and Other

Laws of Cyberspace" 1999.[14] Ännu har inget rimligt förslag till demokratisering av beslutsfattandet kring Internet lanserats. Hur skulle det gå till? Vilka skulle väljarna vara? Hur skapar man en debatt i frågor som är så tekniskt sofistikerade att 95 procent av allmänheten överhuvudtaget inte förstår dem?

Här ser Biegel ingen lösning. (Han är nu jurist, inte statsvetare.) Det är hans diskussion kring förutsättningarna för medborgare och lagstiftare att etablera en fungerande rättsordning som är av intresse här.

Det är inte första gången, påpekar Biegel, som internationaliseringen har ställt krav på nytänkande inom juridiken. Vi har regler om vad som gäller på haven och havsbotten, i luftrummet och rymden, liksom för internationell handel, upphovsrätt och konflikthantering. Här har rättsregler förhandlats eller "värkt" fram och vanligen fått formen av konventioner. Möjligheterna att kontrollera och framtvinga efterlevnad må ofta vara begränsade, men få torde hävda att ansträngningarna har varit betydelselösa. De allra flesta nationer fogar sig hyggligt väl i internationella regelverk.

Biegel tvingas dock konstatera att just USA i många fall har obstruerat mot, eller i vart fall vägrat ansluta sig till, internationella konventioner. (De allra mäktigaste staterna brukar med kraft sätta sina egenintressen främst och vår tid är inget undantag.)

Biegel ägnar bokens avslutande del åt att gå igenom fyra typer av problemskapande Internetanvändning och diskutera förutsättningarna att ingripa mot dem med rättsliga eller andra medel. De fyra kategorierna representerar samtidigt olika grader av farlighet. Biegel föreslår ordningen 1) beteende som uppenbart skapar fara, t ex handel med barnpornografi eller spridande av virus som skadar samhälleligt viktig datordrift, 2) bedrägeri riktat mot företag eller enskilda, 3) olagligt anarkistiskt beteende, varmed åsyftas olaglig kopiering/spridning av upphovsrättsligt skyddat material, spridande av särskilt anstötlig pornografi och förtal av enskilda, samt till sist 4) beteende som är olämpligt eller störande, en kategori med mer oklara gränser men som omfattar "hate-speech" (bl a nazistisk propaganda), trakasserier mot enskilda, och affärsmetoder som kan innebära intrång i enskildas privatliv.

[14] Lessig, Lawrence. "Code and Other Laws of Cyberspace". Basic Books 1999.

Hans slutsats blir – med de reservationer som är självklara, han talar ju om framtiden – att man för de flesta typer av problemskapande Internetanvändning har möjligheter att nå resultat. För en läsare som engagerat sig i yttrandefrihets- och integritetsfrågor inställer sig dock några kritiska funderingar. Vetenskapsmannen Biegel väljer, kan man säga, ett perspektiv på Internet som gör det svårt för medborgaren Biegel att komma till tals.

Han diskuterar främst problemet att kontrollera aktiviteter på Internet, inte problemet att säkra yttrandefrihet eller rätten till anonymitet. Kontrollmöjligheter som vilar på att t ex webb-sidor märks eller kategoriseras – ett fullt realistiskt resultat av internationella förhandlingar om hur Internet ska bli ”säkert” för barnen, fritt från rasism eller något annat lika ädelt mål – kan sedan utnyttjas också för andra syften. EU-kommissionens Safer Internet Action Plan har en budget på 25 miljoner euro som bl a används till att stödja innehållsmärkning av webbplatser och utvecklandet av effektivare filteringstekniker.[15] Ju mer utbredd och standardiserad märkningen blir, desto bättre förutsättningar för att automatiskt filtrera www vid jurisdiktions-gränser. Flera internationella experter, bl a Lawrence Lessig och tysken Herbert Burkert, ordförande för EU-kommissionens Legal Advisory Board, förutspår just en sådan ”geografins återkomst” på nätet.[16]

3.3 Internationellt samarbete – risker, möjligheter

Risken för att små länder som Sverige kommer i kläm i Biegels scenarier är uppenbar. Det blir redan allt vanligare att riksdagen måste ta ställning till lagförslag med effekter för yttrandefriheten eller integritetsskyddet – de kan avse t ex upphovsrätt, terrorist- eller brottsbekämpning – som antingen direkt har initierats genom internationella överenskommelser eller som diskuteras i termer av ”anpassning” till omvärldens krav. Turerna kring EU-direktivet om skydd

[15] Se: http:// europa.eu.int/information_society/programmes/iap/index_en.htm

[16] Olsson, Anders R ”Internet för alla – Alla för Internet?” Expressen 020103.

för persondata, som resulterat i den svenska Personuppgiftslagen är kanske det mest uppmärksammade exemplet.

”*Det är självklart att europeiseringen och internationaliseringen innebär problem*” påpekade häromåret Justitiedepartementets rättschef Göran Lambertz. Politikens inflytande minskar, vilket innebär ”*att vi i Sverige inte längre kan göra som vi vill utan måste anpassa oss till och ibland böja oss för andra staters vilja. Ibland blir vi överkörda i förhandlingar och måste införa regler i svensk rätt som vi helst hade varit utan*.”[17]

För ett land med en radikal yttrandefrihetstradition och de mest långtgående offentlighetsreglerna i världen ger kraven på ”harmonisering” och ”anpassning” till omvärlden uppenbarligen anledning till oro. Föreställningar om vad människor har rätt att säga och om öppenhet i gemensamma angelägenheter – ytterst om relationen mellan medborgare och valda ledare – är djupt förankrade i vår demokratiska kultur. Den byter man inte som man byter skjorta.

Därtill kommer att ett land som har den politiska ambitionen att vara världsledande vad gäller samhälleligt utnyttjande av IT, vilket gäller för Sverige, inte alltid kan avvakta de lösningar som sakta ”värker fram” i omvärlden. Snarare måste Sverige agitera för sina lösningar och demonstrera, genom att skapa egna, fungerande regelverk i samklang med nya tekniska system, att de fungerar. Regler om informationsfrihet och integritetsskydd har inte bara effekter för demokratin utan också industripolitiska och ekonomiska konsekvenser. De strider om upphovsrätten i digitala miljöer som rasar i USA och Europa illustrerar detta. Vilken grad av kontroll en upphovsman i framtiden ska kunna ha över sina verks spridning bestämmer i hög grad utformningen av de tekniska system genom vilka verken förmedlas. Huruvida det ska finnas något så (för en svensk) demokratiskt viktigt som folkbibliotek i cyberrymden beror på hur upphovsrätten formas framöver.

Att det råder starka internationella motsättningar på områden som yttrandefrihet och integritetsskydd utgör kanske ett slags tröst för den som anser svensk tradition värd att bygga vidare på. Biegel, för att återgå till honom, konstaterar att USA är ett av ytterst få länder

[17] SVJT 2000, sid 244.

som – med stark förankring i första tillägget till konstitutionen – vägrar förbjuda rasistisk eller fascistisk propaganda. (Ingen annanstans skulle nazipropaganda placeras i den fjärde, minst farliga kategorin problemskapande Internet-beteende, se ovan.) Hundratals tyska nazister har flyttat sina webb-platser till amerikanska servrar, där deras i Tyskland illegala innehåll är tillgängligt – låt vara att tyska ISP-företag kan försvåra åtkomsten – för hemlandets webbsurfare men utom räckhåll för tyska myndigheter.

Kritiken går också åt andra hållet över Atlanten. På Internet finns hårdporr från t ex Sverige, Holland och Danmark som är olaglig i många amerikanska delstater.

I en rad länder, och inte bara sådana med utpräglat auktoritära regimer som Kina och Saudiarabien, hävdas uppfattningen att nationella (i praktiken juridiska) gränser bör återskapas i cyberrymden. EU-kommissionen säger det inte öppet, men med dess ansträngningar att utveckla effektivare innehållsmärknings- och filtreringsteknologier läggs grunden för en sådan utveckling. Efterfrågan på filtreringslösningar är stark. I en rad beslut har både tyska och franska domstolar krävt att Internet-företag under lokal jurisdiktion ska blockera särskilt anstötliga webplatser baserade i utlandet därför att innehållet bedöms vara obscent, rasistiskt eller uppviglande.[18]

Den amerikanska konstitutionen har hittills utgjort ett robust skydd för yttrandefriheten, vilket p g a den amerikanska dominansen på Internet har fått spridningseffekter. För flertalet auktoritära regimer i världen är Internet något mycket problematiskt. Ett USA i ”krig mot terrorismen” tycks dock berett att rucka på åtskilliga medborgarrättsliga principer. Det finns ingen anledning att utesluta en framtida kohandel mellan stora politiska aktörer, t ex mellan USA och EU. Det är naturligtvis ren spekulation att säga att Bush-administrationen kan komma att vidta åtgärder mot nazistisk propaganda från USA riktad mot Europa i utbyte mot t ex bättre övervaknings-data från EU:s medlemsstater, men det vore egendomligt om dessa aktörer inte sökte hitta överenskommelser som tillfredsställer bådas intressen.

Internationellt samarbete på övervakningsområdet är inget nytt.

[18] Biegel, sid 44 och 373.

Med början 1993 arrangerade amerikanska FBI en rad internationella möten i Quantico, Virginia, med titeln ”International Law Enforcement Telecommunications Seminar”, förkortat ILETS. Deltagarna kom, förutom från USA, från Canada, Hong Kong, Australien och EU. Vid dessa möten utarbetades tekniska standarder för övervakning av telekommunikationer – dvs krav på hur de tekniska systemen ska vara utformade i vissa avseenden – baserade på den i USA nyligen antagna Communications Assistance for Law Enforcement Act, CALEA. I januari 1995 antog EU:s ministerråd en (då) hemlig resolution om anslutning till ILETS standarder. En rad medlemsländer anslöt sig via nationell lagstiftning till dessa standarder. EU och USA skrev ett s k MOU (Memorandum of Understanding) i vilket fler länder inbjöds att ansluta sig till ILETS, och bl a Canada och Australien gjorde det.[19]

ILETS-gruppen har sedan fortsatt sina möten för att utveckla avlyssningsstandarder anpassade för att täcka alla typer av tele- och datakommunikationer, via fasta som mobila enheter. Inom EU har detta arbete avsatt dokument benämnda ENFOPOL. Ministerrådet antog i juni 2001 en resolution (9194/01) ”om rättsväsendets operationella behov med avseende på offentliga telekommunikationer och teletjänster”. EU:s medlemsländer uppmanas där att försäkra sig om att all utveckling av telekommunikationssystem sker med beaktande av de polisiära behoven av övervakning och avlyssning.[20] I september 2002 sammanfattade svenska Rikspolisstyrelsen läget i en skrivelse till regeringen:

Det finns idag sju stora leverantörer av den teknik som teleoperatörer använder (Ericsson, Nokia, Siemens, Motorola, Cisco, Alcatel och Northel). Det pågår ett internationellt standardiseringsarbete inom ramen för ETSI (European Telecommunications Standards Institute) i syfte att fastställa en gemensam standard för de tekniska lösningar som används vid verkställighet av hemlig teleavlyssning och hemlig teleövervakning. För närvarande innehåller dock varje operatörs telesystem unika tekniska lösningar som omöjliggör en enhetlig teknik för ett fullt ut fungerande system för verk-

[19] Privacy & Human Rights. Electronic Privacy Information Center, Washington DC, USA, 2002. Sid 35-36.

[20] Resolutionen finns på: www.statewatch.org/news/2001/sep/9194.pdf

ställighet av hemliga tvångsmedel. Idag finns uppskattningsvis närmare 200 olika aktörer i Sverige som bedriver verksamhet där beslut om hemlig teleavlyssning eller hemlig teleövervakning kan komma att verkställas.[21]

Att incitamenten för internationellt samarbete och koordinering av insatser mot internationell brottslighet är starka står klart. Det är värt att påminna om att flera av terroristerna som slog till den 11 september bodde en längre tid, och sannolikt när de planerade dåden, i Hamburg. I ett brev till EU-kommissionens president Romano Prodi skriver George Bush den 16 oktober 2001 att man, när beslut fattas i dataskyddsfrågor måste beakta att effektivitet i polisiärt arbete och kampen mot terrorism är något absolut nödvändigt (to view ”data protection issues in the context of law enforcement and counter-terrorism imperatives”). Bush begär att förslag till dataskyddsdirektiv som innebär obligatorisk radering av viktiga persondata ändras så att de tillåter sparande av sådana data under rimligt lång tid (”to permit the retention of critical data for a reasonable period”). Här handlar det i första hand om ISP- och teleföretags uppgifter om den trafik man förmedlar. Det kan noteras att Bush begär av Europa att lagregler ska införas som man saknar – som inte ens har föreslagits – i USA.

Brevet till Prodi rymmer också en lång rad önskemål om hur informationsutbyte mellan brottsbekämpande organ i USA och EU ska underlättas. Det handlar då om kamp mot både terrorism och vanlig brottslighet.[22] Även den s k G8-gruppen har tagit ställning för att trafikdata ska sparas.[23]

Såväl diplomatiska förhandlingar som praktiska åtgärder för brottsbekämpning omges vanligen av stort hemlighetsmakeri, och vad som egentligen händer inom området ”internationellt samarbete kring övervakning och kontroll” är ytterligt svårt att få reda på.

Förutom uppgörelser mellan USA och EU kan sådana, hypotetiskt, tänkas mellan USA och strategiskt viktiga länder som t ex de

[21] Skrivelse 2002-09-30. ”Tillgång till telekommunikation för Polisens brottsutredande verksamhet.” Rikspolisstyrelsens diarienummer: RÄS-002-3668/02.

[22] http://www.statewatch.org/news/2001/nov/06uslet.htm

[23] Privacy & Human Rights. Electronic Privacy Information Center, Washington DC, USA, 2002. Sid 48-49.

oljerika i arabvärlden. De senare vill ha ett Internet som ger bättre möjligheter att blockera oönskat innehåll (från pornografi till hädelse mot islam) och USA:s regering skulle sannolikt vara frestad att använda sitt betydande inflytande för att vrida utvecklingen i sådan riktning om den i utbyte kunde få en effektivare övervakning av individer och politiska skeenden i arabländerna.

Här finns ingen anledning att spekulera vidare på detta tema. Avsikten har bara varit att tydliggöra hur viktiga tekniska val och framtida politiska uppgörelser – särskilt om de kombineras – blir för möjligheterna att framöver realisera medborgerliga fri- och rättigheter via nätet.

Till internationellt samarbete kring utformandet av tekniska system måste också läggas en rättslig samordning.

Kunde vi betrakta IT-miljön som något rent nationellt så kunde vi möjligen någon tid hålla oss kvar i den illusionen. Men det är inte av klåfingrighet det inom EU skapats över 30 olika lagstiftnings- och normgivningsprocedurer avseende IT-samhällets rättsliga utmaningar och det var ganska tidigt (1985, min anm) *som Europarådet enades om att datorrelaterad brottslighet var ett område som skulle gagnas av internationell reglering.*

Det skriver Erik Wennerström, ämnesråd vid Justitiedepartementet i Europarättslig Tidskrift nr 4/2001. Han går i artikeln bl a igenom den konvention om ”brott i cyberrymden” som Europarådet antog den 8 november 2001. Den handlar om allt från s k hacking till barnpornografi och rasism. Konventionen är ett försök att definiera inte bara vad som är ett ”IT-brott” utan vad medlemmarna i rådet måste göra för att en rättslig process – från upptäckten av misstänkt brottslighet till utredning, åtal och dom – ska fungera i praktiken.

Kapitel 4.
Övervakandets dystra historia

Frågor om övervakning contra medborgerliga fri- och rättigheter är och har alltid varit politiskt känsliga. Det tycks gälla för alla länder i västvärlden att polis- och säkerhetsorgan ertappas, mer eller mindre ofta, mer eller mindre flagrant, med att ha agerat på otillåtet sätt. Det kan sedan ha skett med eller utan stöd från ledande politiska kretsar. Just Sverige förde under decennierna efter andra världskriget en slags dubbel utrikespolitik där neutralitet och alliansfrihet var den officiella linjen medan landets politiska och militära ledning i själva verket bedrev samarbete med NATO-sidan. Dubbelheten präglade också frågorna om säkerhetsorganens uppgifter och befogenheter. Klas Åmark, professor i historia, sammanfattar:

"Övervakningen av kommunisterna går tillbaka till mellankrigstiden. Under andra världskriget blev den Allmänna säkerhetstjänstens verksamhet oerhört omfattande, med personkontroll och en enorm censur av post-, telefon- och telegramtrafik. Vid krigsslutet stoppade den ansvarige ministern, Tage Erlander, övervakningen av kommunisterna. Den sattes igång igen efter Pragkuppen 1948, när kommunisterna tog över makten i Tjeckoslovakien. Fast militären hade tjuvstartat tidigare, vilket fick Erlander att i sin dagbok förfasa sig över militärens 'monumentala omdömeslöshet' och beklaga att han inte gjort sig av med den alltför svage försvarsministern Allan Vougt. Sedan växte övervakningen stadigt fram till 1960-talet. År 1955 fanns det cirka 200 000 svenskar i Säpos register – det är första gången vi får en exakt uppgift om antalet före 1970."[24]

Kontroverserna har varit många. Med IB-affären i början av 1970-talet avslöjades en i viktiga delar olaglig militär spion- och övervakningsverksamhet riktad mot svenska medborgare och svenska organisationer. Också den s k personalkontroll som SÄPO har skött under lång tid har utsatts för hård kritik, både för att vara alltför omfat-

[24] Åmark, Klas. "Ideologiska fördomar slog ut kalla fakta." Dagens Forskning 23-24 sept 2002.

tande och för att drabba fel personer. Under slutet av 1990-talet blossade debatten åter upp:

"För fyra, fem år sedan gick debattens vågor höga kring den statliga övervakningen av kommunister och andra påstådda säkerhetsrisker. Situationen blev besvärande för regeringen, som anslog 20 miljoner kronor till ett forskningsprogram om den militära säkerhetstjänsten för att bli av med frågan. När det kom till kritan svek regeringen sitt löfte att öppna arkiven för forskarna på ett uppseendeväckande sätt och debatten tog ny fart. Då utsåg Göran Persson en säkerhetstjänstkommission , som gavs fria händer att gå igenom alla arkiv, men vars rätt att publicera resultaten vi ännu inte vet något om."[25]

Just när sista handen läggs vid denna rapport, den 17 december 2002, presenterar denna säkerhetstjänstkommission sitt stora (3 200 sidor) betänkande. Erik Ridderstolpe och Jan Mosander, journalister på Ekoredaktionen, rapporterar samma dag att olaglig åsiktsregistrering och dito telefonavlyssning har pågått även in på 1990-talet:

Säkerhetspolisen, Säpo, har åsiktsregistrerat enskilda individer på ett sätt som enligt lag är förbjudet, och det är något som ansvariga politiker och polis tidigare intensivt förnekat. Den militära underrättelsetjänsten har också under 70-talet sysslat med förbjuden åsiktsregistrering. Det finns ett förbud mot åsiktsregistrering från 1967.

– Regeringen har gett vissa allmänna direktiv för detta, och de har gett direktiv som är offentliga och de har gett direktiv som är hemliga, och det är där vi talar om i viss mån dubbla budskap, säger Anders Knutsson som är före detta ordförande i Högsta domstolen, HD, och med i utredningen.

"Dubbla budskap från regeringen"

Den förbjudna registreringen har kunnat förekomma, säger kommissionen, för att regeringens föreskrifter har präglats av dubbla budskap. Regeringen har alltså försökt tillfredsställa den opinion som protesterat samtidigt som man ändå har gett Säpo och militären rätt att registrera.

Kommissionen säger också att man uttrycker betänkligheter mot

[25] Åmark, a a.

den sammanblandning av stats- och socialdemokratiska partiintressen som har förekommit under alla de här övervakningsoperationerna.

Missbruk av telefonavlyssning

Något av det allvarligaste som kommissionen berättar om handlar om missbruket av telefonavlyssning. Inte bara polisen, utan också åklagare och domstolar har missbrukat bestämmelserna om när man får och när man inte får telefonavlyssna, och inte bara det: Justitieombudsmannen, JO, och Justitiekanslern, JK, som ska övervaka att allt går rätt till och se till att det inte förekommer övergrepp mot enskilda människor har sett igenom fingrarna med missbruket.

Det finns fall där telefonavlyssning har pågått i tio år utan att misstankarna som ledde till avlyssningen har lett till åtal, och utan att någon har reagerat. Dessutom har man använt telefonavlyssning mot människor som inte har haft något att göra med det som man egentligen har försökt undersöka. Det har skett i tusentals fall utan att det har funnits något som helst stöd i lagen för det.

(Hämtat från Ekoredaktionens webbplats: http://www.sr.se/cgi-bin/ekot/artikel.asp?artikel=160939)

Problematiken är alltså inte specifikt svensk. Tendensen att låta övervakning av spioner och kriminella vidgas, i hemlighet och utan formella politiska beslut, till övervakning av politiskt oppositionella känns igen från många västländer. Redan i den gamla ”analoga” världen, där övervakning i huvudsak var en nationell angelägenhet, dyr och praktiskt tungrodd, var det således besvärligt – för att uttrycka det milt – att få genomslag för demokratiska beslut och principer. När den säkerhetspolisiära verksamheten alltmer formas i internationella organ – och när övervakningen med stigande effektivitet kan utövas via elektroniska kommunikationsnät – kan svårigheterna te sig oöverstigliga.

Kapitel 5.
NSA och Echelon[26]

Även om det är svårt att få fram exakta siffror råder ingen tvekan om att USA:s National Security Agency, NSA, är världens största och dyraste spionorganisation. Uppgifterna om antalet anställda brukar anges till mellan 35 000 och 38 000, och budgeten (före 11 september 2001) till omkring 40 miljarder svenska kronor. I dessa siffror räknas dock inte in all personal vid – eller alla kostnaderna för – ett stort antal avlyssningsstationer runt om i världen.

Spindeln i ett mäktigt avlyssningsnät är NSA:s huvudkontor i Fort Meade, Maryland, nära Washington DC. Det är i själva verket en egen, väl inhägnad och väl bevakad stad – ”crypto city” som journalisten James Bamford kallar den i sin tegelstenstjocka bok *The Body of Secrets*, *Anatomy of the Ultra-Secret National Security Agency*.

NSA:s huvuduppgift är att avlyssna och analysera kommunicerade meddelanden. Det kan gälla allt från interna telefonsamtal i det kinesiska kommunistpartiets högkvarter till gigantiska flöden av e-post mellan Europa och USA. Här ska dock bara diskuteras vad som är känt om övervakningen av vanliga medborgares kommunicerande. Fokus kommer att ligga på det s k Echelon-systemet, inte därför att all NSA-övervakning av internationell tele- och datatrafik sker inom ramen för Echelon utan därför att just detta system är känt åtminstone i sina huvuddrag. Av lätt insedda skäl är praktiskt taget all NSA-verksamhet hemlig. Bamford har skrivit en tjock och informa-

[26] Uppgifterna om NSA och Echelon har hämtats från den amerikanske journalisten James Bamfords bok ”The Body of Secrets, Anatomy of the Ultra-Secret National Security Agency”, (Doubleday, USA, 2001), från ett anförande som Bamford höll vid konferensen Computers, Freedom and Privacy i San Francisco den 17 april 2002, en intervju i Washington DC 2002-11-22 med James X Dempsey, chef för Center for Democracy and Technology, samt från en hearing med NSA:s chef, generallöjtnant Michael V Hayden inför två utskott i USA:s kongress den 17 oktober 2002 (The Select Committé on Intelligence, The House Permanent Select Committé on Intelligence), tillgänglig på: http://intelligence.senate.gov/0210hrg/021017/hayden.pdf

tionsrik, om än rörig bok om organisationen. Han kan berätta 1) vad som är tekniskt möjligt i avlyssningsväg, 2) vad som är tillåtet juridiskt och 3) mängder av fakta om vad NSA sysslade med fram t o m 1980-talet, inklusive en del olagligheter, men ju närmare han kommer nutid desto färre blir detaljerna. Dock har debatterna kring Echelon och kritiken mot NSA för att fram till 2001-09-11 ha misslyckats i övervakningen av terrorister lockat/tvingat fram en hel del färsk information.

Strax efter andra världskrigets slut träffade Storbritannien (UK) och USA ett hemligt avtal om samarbete inom området ”signal intelligence”, ett partnerskap som praktiskt nog fick namnet UKUSA. Avtalet gick i korthet ut på att det ena landet, när dess avlyssningsverksamhet genererade information av värde för det andra, skulle dela med sig. Småningom anslöt sig ytterligare tre engelsktalande länder till UKUSA-gruppen: Australien, Nya Zeeland och Canada.

Allteftersom tele- och datatrafiken växte i omfattning blev uppgiften att urskilja och förstå de få verkligt viktiga/intressanta meddelandena allt svårare. De höstackar i vilka man behövde hitta små nålar blev allt större. Åtminstone vad datatrafiken beträffar måste man övergå till automatisk filtrering av informationen, dvs dataströmmarna måste köras genom snabbt arbetande datorer som programmerats att reagera på/spara meddelanden med vissa egenskaper – i första hand när de innehåller vissa namn eller begrepp.

För att effektivisera samarbetet mellan UKUSA-parterna infördes ett gemensamt informationssystem vars programvara fick kodnamnet Echelon. Systemet fungerar i praktiken som en larmlista där t ex Storbritannien lägger in namnen på de irländska terrorister man tror kan vara farliga så att övriga UKUSA-parter kan fånga upp meddelanden där namnen förekommer och vidarebefordra materialet till britterna.

Hur effektivt detta system är kan en utomstående inte bedöma. Å ena sidan sker en häpnadsväckande snabb teknisk utveckling vad gäller datorernas arbetskapacitet och möjligheterna att lagra/återsöka information. I vilken utsträckning dessa kapaciteter verkligen kommer till effektiv användning bestäms av kvaliteten på datorprogrammen: är de tillräckligt sofistikerade för att filtrera fram ”rätt” material? Förre NSA-chefen (1988-1992) William Studeman berättar för Bamford att ett

enda av organisationens system kan behandla en miljon kommunicerade meddelanden under loppet av en halv timme. Rent statistiskt händer sedan detta: datorprogram filtrerar bort alla utom 6 500. Av dessa bedöms 1 000 värda att vidarebefordra till experter för närmare granskning. 10 meddelanden kategoriseras av analytikerna som särkilt intressanta och en enda rapport sammanställs.

När NSA:s chef, generalen Michael V. Hayden, vid en hearing i den amerikanska kongressen den 17 oktober 2002 fick frågan vad hans myndighet visste före 11 september om planerade terrorattacker svarade han:

”*Dessvärre, NSA hade ingen information som tydde på att al-Qaída siktade in sig på mål i New York eller Washington DC, eller att man överhuvudtaget planerade attacker i USA. Före 11 september hade NSA inte ens uppgifter om att dessa terrorister befann sig i USA.*”

Informationsvolymerna är enorma, påpekade Hayden vid samma hearing:

”*Vi gräver ur ett djupt hål. Under 1990-talet skars antalet anställda vid NSA ned med en tredjedel och budgeten med lika mycket. Under detta 1990-tal har det ”paketbaserade” elektroniska kommunicerandet i kvantitet gått förbi det traditionella. Under detta decennium har antalet mobiltelefoner i världen ökat från 16 till 741 miljoner, en nästan 50-faldig ökning. Antalet Internet-användare växte från 4 miljoner till 361 miljoner, en mer än 90-faldig ökning. Av all kommunikationskabel som hade lagts ned i marken fram till år 2000 hade en tredjedel lagts ned under de senaste sex åren. Under 90-talet steg mängden utrikes telefonsamtal från 38 miljarder minuter till 100 miljarder minuter. I år är siffran uppe i 180 miljarder minuter.*”

Bamford räknar upp fyra faktorer som gör NSA:s uppgift särskilt svår idag. Den första är just den snabba ökningen av datamängder som kommuniceras. De övriga är:

1. En växande andel av den kommunicerade informationen går via fiberoptiska kablar istället för satellit, vilket gör den svårare att komma åt.
2. Det blir allt lättare för gemene man, och därmed också för brottslingar, att komma åt datorprogram för stark kryptering. Det ger ”fienden” ett starkt skydd mot avlyssning.

3. Kriget mot terrorismen fordrar tillgång till experter på avsevärt fler språk än det kalla kriget mot Sovjetunionen gjorde. Vid mitten av 1990-talet fann sig NSA ha alldeles för många översättare från ryska och alldeles för få översättare från de många väst- och sydasiatiska språken. Hos NSA finns otaliga fall där viktig information har samlats in men sedan inte har blivit läst/översatt i tid för att komma till användning.

Samtidigt, påpekar Bamford, skickas stora mängder känslig information faktiskt okrypterad via Internet eller andra kommunikationsnät. Uppgifter som skulle krypteras om de skickades inom ett lands administration måste ofta kommuniceras okrypterade mellan länder eftersom de inte har kompatibla system. Det gäller också kommunikation om sådant som vapenaffärer. Även terrorister tvingas ibland, visar det sig, kommunicera i klartext därför att de rent praktiskt inte klarar att utbyta krypteringsnycklar.

Huruvida NSA:s avlyssning i allmänhet eller Echelons i synnerhet bedrivs på ett rättsligt och/eller etiskt försvarbart sätt är en annan fråga som den utomstående knappast kan besvara. Det finns anledning att vara misstänksam. Under många år fick NSA under hand, men i strid med amerikansk lag, kopior av praktiskt taget alla utrikes telegram från telegrambyråerna.

När EU-parlamentet fick rapporter om Echelon och reagerade på dessa med kraftfulla protester var det frågan om företagsspioneri som stod i centrum. Misstanken att NSA bistod amerikanska företag med information om europeiska konkurrenter låg nära till hands, möjligen därför att nationella underrättelsetjänster i Europa har ertappats med sådan ”hjälpsamhet” tidigare. NSA nekade självfallet till alla sådana anklagelser, och Bamford har inte kunnat få belägg för oegentligheter av det slaget. (Han erkänner dock att han inte kunnat göra mer än fråga sina källor inom organisationen.) I den lätt infekterade debatten gjorde förre CIA-chefen R James Woolsey småningom detta inlägg:

”*Det är sant att vi använder datorer för att med hjälp av nyckelord söka igenom data. (...) Det stämmer, mina kontinentala vänner, att vi har spionerat på er. Det beror på att ni mutar. Era företags produkter är ofta dyrare eller mindre tekniskt avancerade, eller båda delarna, jämfört med*

era amerikanska konkurrenters. Därför mutar ni. Så delaktiga i detta är era regeringar att mutor i flera europeiska länder fortfarande kan dras av i företagens skattedeklarationer.

För er kännedom kan vi berätta att när vi ertappar er med att muta, berättar vi det inte för de USA-företag som deltar i budgivningen. Istället kontaktar vi den regering som ni är i färd med att muta och berättar hur illa vi tycker om korruption. Dess reaktion blir ofta att ge hela eller delar av ordern till det företag (ibland ett amerikanskt, ibland inte) som har lagt det mest förmånliga budet. Detta upprör er, och ger ibland upphov till beskyllningar och gräl mellan de hos er som mutar och det andra landets mottagare av mutor. Ibland blir det offentlig skandal. Vi älskar det."

(egen översättning från: Body of Secrets, sid 425)

Med teleavlyssnandets internationalisering byter man alltså, utan att det fattas några politiska beslut om saken, från domstols-kontrollerad avlyssning av brottsmisstänkta individer och företag till generell avlyssning av samtliga medborgare. Echelon förefaller att ännu vara ett nät med stora maskor, men från principiella utgångspunkter är systemet uppseendeväckande.

Bamford litar således på NSA vad gäller företagsspioneri, men, fortsätter han – och observera att detta skrevs före 11 september 2001:

"Det finns en betydligt viktigare fråga: den är huruvida Echelon i praktiken undanröjer skyddet för personlig integritet – som är en grundläggande mänsklig rättighet. Några uppgifter ur en konversation som plockas fram från etern, kanske ryckta ur sitt sammanhang, kan feltolkas av en analytiker som sedan i hemlighet vidarebefordrar dem till spion- och polisorgan världen runt.

Den missvisande informationen placeras sedan i NSA:s närmast bottenlösa datalagringssystem (…) Till skillnad från uppgifter om USA-medborgare, som inte får sparas mer än ett år, kan uppgifter om utlänningar sparas hur länge som helst. Outplånlig kan informationen häfta vid individen så länge han lever. Han får aldrig veta hur han hamnade på tullens svarta lista, vem som placerade honom där, varför han aldrig fick det där kontraktet – eller också kan något än värre hända.

Några uppgifter från NSA eller CIA handlade om en egyptisk invandrare, Nasser Ahmed, som sökte asyl i USA. Den hemliga informationen

ledde till att han häktades; utan möjlighet att bli fri mot borgen hölls han fängslad i ensamcell i över tre år i väntan på deportation. Trots att hans advokat Abdeen Jabara, själv en gång föremål för olaglig NSA-övervakning, kämpade i flera år fick han aldrig veta vilka ´hemliga bevis´ man hade mot honom eller hur USA hade kommit över dem. I denna Kafkaliknande värld kunde han inte försvara sig mot anklagelserna eftersom han inte fick veta vad de bestod i: de var hemliga. Först sedan arab-amerikanska grupper lyckats mobilisera ett tillräckligt politiskt tryck mot Justitiedepartementet släppte man där ifrån sig en del av uppgifterna. Ahmed kunde då bemöta påståendena och till slut återfå friheten.

(…)

Fungerande utan politisk och rättslig kontroll kan UKUSA:s världsomspännande avlyssningsnät bli en slags hemlig cyber-polis, utan domstolar, juryer eller någon rätt för individen att försvara sig."

(Body of Secrets, sid 425-426)

Denna debatt, liksom praktiskt taget all debatt om Echelon, dog ut med 11 september-attackerna. De risker som växer fram med övervakningen av internationell tele- och datatrafik, och som hör samman med att den är just internationell, dvs bedrivs av spionorganisationer som inte underställs någon effektiv rättslig eller politisk kontroll, är kanske lika stora som riskerna med att polisiära intressen får stort genomslag i lagstiftning på nationell nivå. Att det under flera år blir politiskt "omöjligt" att ifrågasätta en framväxande internationell avlyssningsverksamhet – rättsligt oreglerad och okontrollerad – kan vara lika skadande ur demokratisk synpunkt som att riva ned etablerade murar till skydd för yttrandefrihet och personlig integritet.

Det kan jämföras med en ishockeymatch där domaren p g a publiktrycket inte vågar blåsa av hemmalagets spelare för regelbrott – det leder närmast oundvikligen till en brutalisering av spelet. Allt blir tillåtet.

Kapitel 6.

USA och reaktionerna på 11 september[27]

Efter terrorattackerna den 11 september tog regeringen Bush snabbt initiativ till en rad lagändringar som, när de inledningsvis förstummade medborgarrätts-organisationerna åter fick mål i mun, har blivit hårt kritiserade. I centrum för intresset har stått en lag antagen den 26 oktober 2001 med namnet ”Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, förkortat USA PATRIOT Act.[28] Det är en närmast oöverskådligt stor samling bestämmelser som innebär reformer inom många olika områden, från immigrationskontroll till penningtvätt. Den trumfades igenom på rekordtid, utan sådana ”hearings” i kongressens utskott som normalt föregår beslut om kontroversiella lagförslag. Trots namnet syftar lagen inte bara till ökad effektivitet i terroristbekämpningen utan i all brottsbekämpning. Det är uppenbart att lagtexten i stora delar bygger på

[27] Denna översikt bygger på nedanstående litteratur och intervjuer i Washington DC i november 2002. Litteratur:

- Cole, David/Dempsey, James X: Terrorism and the Constitution. (The New Press, 2002.)

- Electronic Privacy Informations Center (EPIC) and Privacy International: Privacy and Human Rights – An International Survey of Privacy Laws and Developments. (EPIC 2002).

- Etzioni, Amitai: Implications of New Technologies for Individual Rights and Public Safety. (Harvard Journal of Law and Technology, Volume 15, Number 2. Spring 2002.)

- Falk, Richard: The Great Terror War. Olive Branch Press 2003.

- Gertz, Bill: Breakdown – How America´s Intelligence Failures Led to September 11.” (Regnery Publishing Inc. 2002.)

- Goldberg, Danny/Goldberg, Victor/Greenwald, Robert (edts): It´s a Free Country – Personal Freedom in America after September 11. (RDV Books/Akashic Books 2002.)

Intervjuer: James X Dempsey, chef för Center for Democracy and Technology, Washington DC, 2002-11-22. Professor Orin Kerr, George Washington University Law School, 2002-11-26.

[28] Lagtexten finns på http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162

sådana förslag som polis- och säkerhetsorgan har framfört (eller åtminstone utarbetat) redan före 11 september och som, i ett dramatiskt hårdnat samhällsklimat efter terrordåden, framstod som angelägna. Vissa bestämmelser är dock av s k solnedgångs-karaktär, dvs om de inte förnyas om några år upphör de att gälla.

Mycket av kritiken mot PATRIOT-lagen var i själva verket upprepningar av argument i en diskussion som pågått i mer än 50 år och som handlar om dels vad USA:s konstitution egentligen garanterar, dels vilken skillnad man ska göra mellan USA-medborgare och icke-USA-medborgare. Patriot-lagen innehåller få regler som konkret handlar om teknisk övervakning, men genom att vidga kretsen människor som anses utgöra hot, och genom att ge de polisiära organen större frihet att själva avgöra hur hot ska förebyggas kan lagens effekter ändå bli långtgående.

1952 antogs den s k McCarran-Walter-lagen, som innebar att en person som inte var medborgare och som tillhörde en kommunistisk eller anarkistisk organisation normalt skulle nekas inresa eller, om vederbörande redan befann sig i landet, utvisas. (Och USA-medborgare som i FBI:s ögon tillhörde den politiska vänstern övervakades så långt möjligt.) På 1950-talet var det få som ville eller vågade kritisera denna lag. Den byggde uppenbarligen på idén om ”guilt by association”. Människor bedömdes utifrån sina politiska uppfattningar och sitt umgänge, inte utifrån sina handlingar. Listan över kända personer som med hänvisning till McCarran-Walter-lagen vägrades inresa till USA blev småningom lång – den rymde bl a Gabriel Garcia Marques, Graham Greene, Carlos Fuentes, Czeslaw Milosz, Yves Montand och Charlie Chaplin – och blev i ljuset av en utbredd politisk radikalisering under 1960- och 70-talen alltmer kontroversiell. Det dröjde dock till 1990 innan Kongressen formellt avskaffade – i allt väsentligt – möjligheten att avvisa och deportera personer på enbart ideologisk grund.

Den ”liberaliseringen” blev nu inte långvarig. 1993 detonerade en kraftig bomb i garaget under en av World Trade Center-skyskraporna på Manhattan – som emellertid höll för påfrestningen denna gång. Ansvarig för dådet var en terrorgrupp vars medlemmar hade sina rötter i mellanöstern. 1995 sprängde Timothy McVeigh, en amerikansk f d soldat som förklarat krig mot staten, en federal byggnad i

Oklahoma City och dödade 168 personer. Som en reaktion på dessa händelser antogs 1996 års Anti-Terrorist-lag, som i princip återinförde guilt-by-association-principen men ersatte ”kommunistisk organisation” med ”terroristorganisation”. Vilken organisation som är ”terroristisk” bestäms formellt av utrikesdepartementet. Departementet uppdaterar löpande en lista över sammanslutningar som ska anses terroristiska. Personer som är medlemmar i en sådan organisation eller stöder den (t ex ekonomiskt) ska hindras inresa. Om de redan finns i landet ska de utvisas. Om de är USA-medborgare och medlemmar i organisationen får de övervakas. Att skänka pengar till en terroristorganisation är ett brott.

Själva begreppet terroristorganisation har vållat kontroverser. Hur skiljer man terroristorganisationer från gerilla-grupper eller befrielseorganisationer av andra slag? Sydafrikanska ANC fanns med på terrorist-listan praktiskt taget fram till dess organisationen genom demokratiska val kom till makten i sitt eget land. Hade Anti-Terroristlagen varit kraft på 1980-talet skulle det således ha varit brottsligt att skänka pengar till Nelson Mandela när han reste runt i USA och agiterade mot apardheid. (Han kanske inte ens hade släppts in i landet.) Därtill kommer frågan hur sådana organisationer skulle behandlas som verkligen utförde terrordåd men samtidigt bedrev annan, laglig verksamhet. Särskilt Israel/Palestina-konflikten aktualiserar detta problem. (USA-regeringen tenderar att karaktärisera alla rörelser på den palestinska sidan som använder våld terroristiska, medan stora delar av omvärlden betraktar dem som politiska rörelser i kamp mot en ockupationsmakt.) Palestinska Hamas t ex, har tagit på sig ansvar för attacker mot civila israeler, men huvuddelen av organisationens verksamhet är av social och humanitär natur. Enligt 1996 års amerikanska Anti-Terroristlag skulle det vara ett brott att skänka filtar eller skolböcker till projekt som Hamas driver. Lagens kritiker hävdar att det strider mot grundläggande konstitutionella principer att kriminalisera sådana handlingar.

Före 11/9 kritiserades regeringen för att den i kampen mot terrorism fokuserade på människor som inte var inblandade i brottslig verksamhet eller i planeringen av våldsamheter utan bara sympatiserade med radikala grupper, t ex palestinska som PLO, PFLP eller Hamas. Regeringen satsade stora resurser på att övervaka politiskt

och religiöst aktiva, hävdade kritikerna, när de borde koncentrera sig på de kriminellt aktiva.

Med terrordåden 11/9 fick kritikerna på sätt och vis rätt. Ingen av flygplanskaparna var, medan de levde i USA, inblandade i politisk aktivitet. De gick inte till moskéer, deltog inte i manifestationer, höll inga offentliga tal. De låg lågt, och medan polis och terroristbekämpare bevakade muslimers samlingsplatser, demonstrationer och politiska möten på jakt efter människor med ”farliga” åsikter kunde terroristerna sköta sin planering och sina förberedelser på ställen och via kanaler där rättsväsendet aldrig letade. Hoten mot USA kommer inte, hävdar kritikerna, från PLO eller Hamas utan från organisationer eller nätverk av Al Qaidas typ. De har inte kopplingar till någon politisk eller humanitär rörelse.

Inget brottsbekämpnings- eller underrättelseorgan i USA hade, visade det sig 2001, särskilt mycket kunskap om terroristnätverk som Al Qaida. Kraven på kraftfulla åtgärder och rädslan för att det fanns fler ”sovande” terrorister som väntade på att slå till fick regeringen Bush att byta strategi från ”guilt by association” till något som närmast liknar ”guilt by ethnicity”. Man visste inte var man skulle leta, och valde att utgå från det som flygkaparna hade gemensamt: att de var män, araber, muslimer och i åldrarna 20-40.

- Man tog snabbt och på tämligen lösa grunder fram en lista på 5 000 muslimska immigranter som man ville ”tala med”. I mars 2002 utökades listan med ytterligare flera tusen personer. Av dessa var det bara en liten bråkdel som ens hade några informationer av intresse för polisutredarna, men åtminstone delar av listan kom ut till offentligheten. Bl a publicerades många av namnen på en sydamerikansk webbsida som ”misstänkta terrorister”. Ett stort antal människor har därmed ställts inför den närmast omöjliga uppgiften att bevisa att de inte är potentiella massmördare.
- Av de 6-8 miljoner invandrare som vistas illegalt i USA satsades betydande resurser på att hitta alla som var araber eller muslimer och utvisa dem. Flera tusen personer deporterades. (Att polis- och immigrationsmyndigheter normalt inte anstränger sig med att få tag på människor som tagit sig över gränsen i hemlighet eller vars visa har gått ut beror på att de fyller en viktig funktion för ekonomin, främst som lågbetald säsongsarbetskraft i vissa branscher.)

Tilläggas kan att de allra flesta av 11/9-terroristerna formellt hade rätt att vistas i landet när dåden genomfördes. De skulle alltså att klarat sig undan en rensning av denna typ.

- I juni 2002 beslöt justitieminister John Ashcroft dels att alla personer som reser in i USA från länder i mellanöstern ska fotograferas och lämna fingeravtryck, dels att ungefär 100 000 invandrare från dessa länder som redan vistas lagligt i USA ska registreras på samma sätt.

Alltmer kontroversiell är också USA:s fängslande av människor runt om i världen som, anser man, kan misstänkas för terrorism eller har kunskaper om sådan. Här finns bl a fångarna på Guantanamo-basen på Cuba. Där är antalet fångar känt (ca 600) liksom deras identitet i flertalet fall. En av dem – Mhedi Ghezali – är svensk. Internationella Röda Korset har kontakt med dem, men de står utanför rättssamhället. (Dvs de betraktas inte som vanliga kriminella, med rätt till advokat, till att få veta vad de anklagas för mm, eller som krigsfångar – som också har rättigheter.) En annan kategori är de personer som hålls fångna på andra ställen runt om i världen, bl a ombord på fartyg och i militära anläggningar – de flesta sannolikt i Afghanistan och Pakistan. Inte heller de tillerkänns juridiska rättigheter. Antalet sådana fångar är okänt liksom deras identiteter. En tredje kategori är de människor som är fängslade i USA enligt den s k Material Witness Law, en tidigare sällan utnyttjad lag som tillåter staten att låsa in människor som man antar har information om brott och som man misstänker kommer att fly/resa iväg om de får chansen. Lagen kom till 1984 och var avsedd att tillämpas främst vid utredningar om narkotikasmuggling. Washington Post kunde den 24 november 2002 publicera en lista på 44 personer som hållits fängslade med stöd av lagen och där avsikten var att förhöra dem om dåden 11/9. Huruvida dessa 44 var samtliga eller bara liten del av de som fängslats på sådan grund hade tidningen inte kunnat utröna. Varken polis, åklagare eller justitiedepartement svarade på frågor i ämnet.

Mycken information om detta fängslande av människor i jakten på terrorister är således hemlig. Tom Ridge, nyutnämnd chef för det ”superdepartement” som ska börja fungera 2003 och få övergripande ansvar för ”homeland security” (säkerheten inom USA:s gränser),

hävdade dock i november 2002 att sammanlagt 2 700 misstänkta terrorister dittills hade fängslats.[29]

Att informationsflödena mellan olika myndigheter måste utökas och effektiviteten i vissa kontroller effektiviseras är det knappast någon i USA som bestrider. Två av terroristerna, Muhamed Atta och Marwan al-Shehhi, antogs år 2000 som studerande vid Huffman Aviation International, en flygskola i Florida. Skolan skickade i augusti 2000 en ansökan till immigrationsmyndigheten INS om att de båda männens visa skulle ändras från kategorin ”besökare” till ”studerande”. INS beviljade denna ansökan den 17 juli 2001 (för Atta) respektive 9 augusti (för al-Shehhi). Den 6 mars – ett halvår efter terrordåden – meddelade INS formellt flygskolan att viseringarna hade ändrats.[30]

Vad gäller statens möjligheter att avlyssna och övervaka telefon- och datatrafik innebär PATRIOT-lagen att polisens och underrättelseorganens befogenheter i vissa fall vidgas. Det råder dock delade meningar om hur stor skillnad som PATRIOT-lagen egentligen har gjort, och uppgifter om i vilken utsträckning regeringen verkligen har utnyttjat sina nya befogenheter är i stor utsträckning hemligstämplade.

Flera olika regelverk i amerikansk lag bestämmer möjligheterna till avlyssning och övervakning. Ett är FISA (Foreign Intelligence Surveillance Act) som ger regeringen rätt att utföra både avlyssning av kommunikation och fysiska undersökningar – som husrannsakan, genomsökning av bagage och liknande – i hemlighet. FISA fordrar dock att målet/individen som undersöks på goda grunder kan antas vara agent för främmande makt eller medlem av en internationell terroristorganisation. Den som utsätts för hemlig undersökning enligt FISA behöver aldrig underrättas om vad som skett. PATRIOT-lagen sänker här ribban för att domstol ska godkänna avlyssning. Tidigare skulle ”det enda eller huvudsakliga syftet” vara att inhämta underrättelser om spionerі eller internationell terrorism, i fortsättningen kan avlyssning/husrannsakan med stöd av FISA beviljas om ”ett av syftena” är få sådana underrättelser. Detta vidgar väsentligt

[29] Washington Post 2002-11-23.

[30] Gertz, sid 141-142.

möjligheterna att åberopa FISA, hävdar civil-liberties-grupperna. Andra, som juridikprofessorn vid George Washington Law School, Orin Kerr, menar att den faktiska skillnaden sannolikt blir liten. (Kerr har själv ett förflutet som tjänsteman på Justitiedepartementet.)

En annan förändring som följt av PATRIOT-lagen är att även CIA, inte bara polisiära myndigheter i kamp mot vanlig brottslighet, kan utnyttja den s k Grand Jury-institutionen – en slags förberedande rättslig process ledd av en domare. Som ett moment i den pågående förundersökningen kan åklagaren kalla till vittnesförhör, som hålls under sanningsförsäkran, och begära fram informationer och material av alla slag från myndigheter, företag eller privatpersoner. Det kan gälla praktiskt taget vad som helst: bankkontouppgifter, kreditkortsdata, flygbolags uppgifter om resor eller uppgifter om bibliotekslån. Den som åläggs att lämna ut uppgifter kan uttryckligen förbjudas att avslöja något för utomstående om saken.

Civil-liberties-aktivister misstänker, mot bakgrund av hur människor med ”fel” åsikter eller religion har behandlats tidigare, att Grand Jury-institutionen nu kommer att bli ännu ett redskap för kartläggning av personer och grupper som är politiskt kontroversiella men som inte kan beslås med någon brottslig aktivitet. Biblioteksorganisationerna, som anser sig ha ett särskilt ansvar för yttrande- och informationsfriheten, har protesterat. ALA (American Library Association) har gått ut till landets bibliotek med frågor om hur många order om utlämnande av information till Grand Juries som de har fått. Biblioteken får inte avslöja något om ett enskilt fall av utlämnande, men kan kanske svara på frågor om antalet fall. (Huruvida de skulle tillåtas svara var i skrivande stund, november 2002, fortfarande oklart.)

EPIC (Electronic Privacy Information Center)är den organisation som mest aktivt arbetar för medborgerliga fri- och rättigheter i cyberrymden. I flera omgångar har EPIC stämt regeringen när den vägrat lämna ut uppgifter om i vilken utsträckning polis och underrättelsetjänst avlyssnar Internet-trafik i hemlighet och gör ”virtuell husrannsakan” i enskildas datorer. (EPIC stöder sig på the Freedom of Information Act, lagen som rymmer USA:s regler om handlingsoffentlighet hos federala myndigheter.)

Vad gäller avlyssning inom ramen för vanliga brottsutredningar

är det ”Safe Streets and Crime Control Act” från 1968 och ”The Electronic Communications Privacy Act” från 1986 som sätter gränser. För att få tillgång till innehåll i meddelanden (t ex avlyssna telefonsamtal eller läsa e-post) fordras domstols godkännande. Det ska beviljas under vissa omständigheter, som att det brott som utreds är grovt och av sådan natur att t ex telefonavlyssning kan resultera i ny bevisning. För att få tillgång till uppgifter om tele- eller datatrafik (motsvarande hemlig teleövervakning i svensk rätt) är kraven lägre. Även här fordras domstols tillstånd, men det räcker med att en åklagare intygar för domaren att den information som ska samlas in är relevant för en pågående förundersökning.

Här innebär PATRIOT-lagen ökade möjligheter för polisen att utföra s k sneak-and-peak-undersökningar. Vid en vanlig husrannsakan i ett bostadshus har den boende rätt att närvara då polisen genomför undersökningen. Han/hon har rätt att läsa domstolens beslut om husrannsakan och kan kontrollera att det följs. Ska poliserna leta efter t ex en stulen bil får de inte gå in i sovrummet, söker de ett parti stulna TV-apparater får de inte gå igenom bokhyllan. Tar polisen med sig föremålen x, y och z från huset får den boende med sin namnteckning bekräfta att polisen beslagtagit x, y och z, men inget annat. Domstolen får en kopia av listan. Vid sneak-and-peak-undersökningar (”smyga-in-och-kika”) kan den utsatta personen inte kontrollera någonting. Polisen går in när vederbörande inte är hemma och kan följaktligen genomsöka vad den vill inklusive datorers hårddiskar och andra medier för datalagring. Den kan installera dolda mikrofoner – buggning är vid misstanke om allvarligare brott tillåten i USA – eller ett s k Key Logger System, KLS, i datorn. Avsikten med KLS är att i smyg registrera den misstänktes lösenord till krypterad information – som man annars inte kommer åt ens genom att beslagta datorn.

Nästa tekniska steg, som redan prövats i utredningar om brott som begåtts av utländska medborgare, är att använda Internet för sneak-and-peak-undersökningar av datorer. Det kan ske genom vanlig s k hacking eller genom att polisen skickar en ”trojan” till den misstänktes dator – ett datorprogram som laddas ner när han/hon öppnar en bilaga till ett e-brev eller laddar hem något från www. Programmet registrerar och sparar sådan information som polisen

vill ha, t ex lösenord, så att den blir åtkomlig vid en vanlig husrannsakan eller via Internet.

Att en sneak-and-peak-undersökning har genomförts behöver polisen inte informera om förrän upp till 3-4 månader senare. Om förundersökningen inte leder till åtal ska den utsatta personen dock informeras om att en undersökning har genomförts, vilket gäller även vid hemlig avlyssning av telefon- eller Internet-trafik. PATRIOT-reformen ger således polisen ökade möjligheter att i smyg undersöka misstänkta personer. Även här finns dock skilda uppfattningar om hur stort steg som egentligen har tagits. Professor Orin Kerr påpekar att domstolarna redan före PATRIOT-lagen beviljade sneak-and-peak-undersökningar – där man tilläts skjuta upp underrättelsen till den misstänkte – när det fanns starka skäl. Enligt Kerr´s uppfattning handlar detta, liksom flera andra till synes ”polis-vänliga” lagändringar efter 11/9, om att anpassa lagens bokstav till en ny teknisk verklighet som domstolarna genom praxis redan hade accepterat.

De senaste årens mest omdiskuterade fråga vad gäller Internet-avlyssning i USA – politiskt ”het” redan före terrordåden – har handlat om Carnivore, ett system som FBI skapat för att kunna samla upp precis den Internet-trafik hos en ISP som man har fått domstols tillstånd att kontrollera. (Namnet, på svenska ”köttätare”, var sällsynt illa valt. Det skulle understryka avsikten att sortera fram ”köttet” i stora informationsflöden – det FBI skulle titta på och inget annat. Motståndarna associerade snarare till ett statligt rovdjur på jakt i medborgarnas privata sfär.) Enligt FBI var det alltför många ISP-företag som inte klarade att leverera just den information som polisen skulle ha – de levererade för lite, för mycket eller för sent – varför Carnivore utvecklades för att kunna installeras hos ISP:n.

Civil-liberties-agitatorerna protesterade mot en sådan lösning eftersom de ansåg att man helt enkelt inte kunde lita på FBI. Med Carnivore tog polisen s a s kontroll över alla dataflöden hos ISP:n. Man kunde titta på vad som helst och möjligheterna för utomstående att avslöja sådant missbruk av systemet var försvinnande små.[31]

[31] Organisationen EPIC har dock på sin hemsida dokument som visar att polisen i åtminstone ett fall har använt Carnivore för att ”tappa av” mer information än man hade tillstånd till: http://www.epic.org

FBI gick inte med på att beskriva i detalj hur Carnivore fungerade – man var inte beredd att offentliggöra programmens källkod. Om systemet överhuvudtaget skulle användas, hävdade bl a James Dempsey, borde Carnivore vid varje tillfälle överlämnas till ISP:n som sedan gjorde de inställningar i programmen som erfordrades.

Om Carnivore är ett polisiärt projekt som realiserats enligt planerna så har debatterna i USA också handlat om djärvare – ur demokratisk synpunkt obehagligare – planer. Ett program fick arbetsnamnet TIPS (Terrorism Information and Prevention System) och syftade till att vissa yrkesgrupper skulle utbildas i terrorism-kunskap för att sedan fungera som informatörer till staten. Långtradarchaufförer, brevbärare, parkeringsvakter och andra som dagligen rör sig ute i samhället skulle lära sig känna igen tecken på att allt inte står rätt till: t ex att människor gömmer sig, att de visar anmärkningsvärt stort intresse för samhällets vattenförsörjning eller för sprängmedel. När dessa idéer lanserades blev motreaktionen kraftig. Parallellen med östtyska STASI och dess nät av informatörer låg nära till hands. I skrivande stund (början av december 2002) tycks projektet vara politiskt avsomnat.

I centrum för en annan radikal satsning står John Poindexter, amiral med ett förflutet som huvudperson (tillsammans med Oliver North) i Iran-Contras-skandalen på 1980-talet. (Den handlade om att ordna USA:s finansiering av gerillakriget mot den demokratiskt tillsatta regimen i Nicaragua – utan att det togs några politiska beslut om saken och utan att det syntes i statens budget. Poindexter dömdes i första instans för flera brott men friades sedan i en högre.) Han utsågs i februari 2002 till chef för en ny försvarsmyndighet med namnet Office of Information Awareness, och lanserade på hösten samma år TIA (Total Information Awareness) som nytt redskap i kampen mot terrorism.

TIA innebär att man samlar eller tillgängliggör (hur det skulle realiseras tekniskt och praktiskt verkar inte alldeles klart) så gott som all personinformation som finns i elektronisk form, även den mest integritetskänsliga, i offentlig och privat sektor. Ur dessa ofantliga datamängder skulle det, hävdar TIA-förespråkarna, vara möjligt att vaska fram kritisk information. Personer vars egenskaper och beteenden – hur de reser, hur de handskas med pengar etc – stämmer

överens med kända terroristers skulle upptäckas och kontrolleras närmare.

För den som har följt debatten om personlig integritet i västvärlden är det häpnadsväckande idéer. TIA är, enkelt uttryckt, Storebrors våta dröm. Debatten har också spretat åt olika håll beroende på att vissa deltagare (både anhängare och motståndare) har tagit idéerna på blodigt allvar medan andra, bl a Orin Kerr, uppfattar projektet som ”ett tankeexperiment”. Kerr påpekar att Poindexters myndighet skulle, om TIA realiserades i den form det beskrivits i nyhetsmedia, bryta mot åtminstone ett dussin lagar till skydd för medborgarnas personliga integritet. Intressantast är TIA kanske inte som polisiär praxis utan som illustration av tidsandan. I USA, där ”privacy” är något heligt, kan ett så extremt projekt lanseras av en federal myndighet och diskuteras seriöst. Det hade inte kunnat ske före 11 september 2001.

Kapitel 7.
Europa efter terrordåden

”Kriget mot terrorismen” har förvandlats till en fortlöpande ”krig mot frihet och demokrati” där nya normer etableras – normer som innebär att politiskt ansvar, kritisk genomlysning och garantier för mänskliga rättigheter är lyxföreteelser som vi kan bortse från när vi försvarar ”demokratin”.

Det skriver 2002 Tony Bunyan, redaktör för Statewatch, en organisation som bevakar demokratiska fri- och rättigheter i Europa.[32] Hans kritik handlar mindre om konkreta beslut om skärpt övervakning (bara vad gäller ”data retention” blir den frågan aktuell, se nedan) och mer om juridiska definitioner och nya organisatoriska lösningar. Här kan övervakning dock bli den indirekta följden.

EU fattade på hösten 2001 två snabba s k rambeslut, ett om kampen mot terrorism och ett annat om en europeisk arresteringsorder. Bunyans (och många andras) kritik mot rambeslutet om terrorism riktas främst mot definitionen av vem som är terrorist och vad som utgör terroristiska handlingar. Med en definition som inkluderar t ex vissa typer av icke våldsamma demonstrationer (när deltagarna genom att sätta sig ned blockerar en väg eller när de kedjar fast sig på en plats) riskerar stora grupper av politiskt oppositionella att bli föremål för säkerhetspolisens intresse. Mönstret känns igen från USA. Personer som fyller kriterierna för ”spion” eller ”terrorist” kan, även enligt lagregler som gällde före 11 september, övervakas och fängslas på lösare grunder än vad som gäller för andra brottsmisstänkta och har då ytterligt små möjligheter att ta tillvara sina rättigheter. En till synes liten språklig förändring i definitionen av terrorism kan således flytta stora grupper av medborgare in under ett strängare regelverk där deras integritetsskydd i det närmaste upphävs.

Den gemensamma arresteringsordern innebär att ett vissa rätts-

[32] Bunyans text är ”Statewatch analysis no 13” och finns, liksom många andra artiklar och politiska dokument kring övervakning, på organisationens webbplats: http://www.statewatch.org

säkerhetskontroller i samband med utlämnande, mellan länder, av misstänkta brottslingar avskaffas.

Bunyan kritiserar också tillkomsten, efter 11 september, av informella samarbetsorgan där viktiga beslut fattas. Ett exempel är ”The Police Chiefs Operational Task Force” (PCOTF). Dess konstitutionella status har aldrig klargjorts. Polischefs-gruppen skulle när den bildades vid ett EU-toppmöte i Tammerfos 1999 koncentrera sig på tre eller fyra viktiga problem kring organiserad brottslighet men gavs, skriver Bunyan, efter den 11 september

”*en rad operationella uppgifter: underrättelseverksamhet och informationutbyte, samarbete mellan nationella anti-terrorist-styrkor, flygplatssäkerhet, planering av gränskontroller och operationer och samordning av para-militära polisenheter i samband med EU-toppmöten och internationella möten.*

När Statewatch begärde att få ta del av gruppens möteshandlingar fick vi svaret att PCOTF inte lydde under ministerrådet och att några dokument därför inte kunde lämnas ut.”

Mest kontroversiell inom EU har dock varit frågan om att spara trafikdata hos tele- och datakommunikationsföretag, ”data retention”. Enligt ett EU-direktiv från 1997 om skydd för den personliga integriteten vid utnyttjande av telekommunikationer var det uttryckligen förbjudet för kommunikationsföretag att spara uppgifter om kundernas kommunicerande längre än vad som fordrades för att säkra korrekt debitering. Som nämnts ovan begärde USA:s regering att EU skulle ändra denna regel för att öka möjligheterna för poliser och säkerhetsorgan att undersöka vem som gjort vad i tele- och datakommunikationsnät. Ministerrådet ställde sig bakom kravet och EU-kommissionen, som tidigare motsatt sig en sådan försvagning i integritetsskyddet, gjorde detsamma. Ändringen förutsatte dock även EU-parlamentets godkännande, och där hade förslag om ”data retention” tidigare röstats ned vid flera tillfällen. Att parlamentet i en omröstning den 30 maj 2002, efter att ledamöterna hade utsatts för intensiv lobbying från såväl anhängare som motståndare till förslaget, accepterade ett direktiv som medgav ”data retention” sågs av Statewatch och liknande organisationer som ett svek och ett allvarligt bakslag för medborgerliga fri- och rättigheter.

Den 12 juli fattade ministerrådet beslutet om ett nytt direktiv

(2002/58/EG). Det tillåter EU:s medlemsländer att med lagstiftning tvinga kommunikationsföretag att spara trafikdata, men kräver det inte. Beslutet fattades i den första pelaren, dvs det handlade om den gemensamma marknaden. Tämligen omgående togs frågan upp inom den tredje pelaren, där bl a frågorna om brottsbekämpning hanteras. Ett förslag till rambeslut som tvingar kommunikationsföretagen i Europa att spara trafikdata diskuteras[33], men förhandlingarna sköts under sträng sekretess. Här ska påpekas att ett beslut fordrar enighet. Det räcker att något land, t ex Sverige, röstar nej för att blockera reformen.

Det är lätt att allmänt instämma i Bunyans farhågor, men det ska också sägas att helhetsbilden vad gäller medborgar-övervakning i Europa fortfarande är splittrad och full av oklarheter. Många europeiska regeringar och parlament reagerade förvisso på terrorattackerna den 11 september. Det övergripande temat för många nya lagregler och andra insatser tycks, precis som i USA, bli ökade befogenheter och resurser för övervakning, men variationerna är stora. Någon kartläggning av olika länders åtgärder har inte varit möjlig inom ramen för denna rapport, men av nyhetsrapportering och inlägg på relevanta diskussionslistor framgår att vissa lagstiftare har koncentrerat sig på obligatoriska ID-kort, andra på effektivare gränskontroll, ytterligare andra har ställt krav på ISP-företag att övervaka sina dataflöden och spara trafikuppgifter. Några länder, framförallt Tyskland, reagerade oerhört snabbt – alltför snabbt, enligt kritikerna.[34]

I en del fall tycks besluten och de vidtagna åtgärderna mest ha skapat oklarhet. I Storbritannien t ex, diskuterades frågan om ”data retention” intensivt, regeringen drev linjen att trafikdata borde sparas i sju (!) år för att finnas tillgängliga i polisutredningar, men parlamentet nöjde sig med en ”rekommendation” till tele- och datakommunikationsföretagen att spara trafikuppgifterna. Enligt landets Privacy Commissioner (motsvarande Sveriges Datainspektion) for-

[33] Hansson, Tom. ”EU-tvång att lagra e-post nytt vapen mot brottslighet.” Dagens Forskning 23-24/9 2002.

[34] Personlig intervju med Dr Alexander Dix, Landesbeauftragter für den Datenschutz und für das Recht auf Akteninsicht, Brandenburg. Kleinmachnow 2002-11-08. T o m den tyske inrikesministern, som lade fram lagförslaget, har medgivit att parlamentsledamöterna inte hade tid läsa ”det finstilta” eller att ordentligt sätta sig in i de nya reglernas effekter.

dras dock en lagändring eftersom ett lagrande av trafikdata strider mot The Data Protection Act från 1998. Parlamentet kan inte ”rekommendera” landets företag att bryta mot lagen – det måste ändra lagen.

Kapitel 8.

Sverige avvaktar[35]

Sverige hör till de länder som inte har fattat beslut om utvidgad övervakning. Betraktar man däremot reglerna om hur polisen ska arbeta och vilka personuppgifter den förväntas registrera i framtiden, märks en förändrad hållning.

Frågan om s k förspaningsregister, register med uppgifter om personer som inte misstänks för brott, har diskuterats i decennier. I en utredning i regeringskansliet från 1992 (Ds 1992:32) hävdas fortfarande åsikten att sådana register inte kan accepteras. Nio år senare – i en utredning som visserligen publicerades efter 11 september men som sannolikt till större delen skrevs före – betonas att polisen måste arbeta mer förebyggande, varmed frågan om förspaningsregister får ett annat svar.

”*Uppgifter om en skild person som det inte finns någon misstanke om brott mot bör få behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer*.” (SOU 2001:92, sid 19)

De relevanta reglerna om teleavlyssning och teleövervakning finns f n i Telelagen, Rättegångsbalken och en speciallag från 1952. Regelverken tycks inte helt samordnade.

– Av TELELAGENS §§ 45 och 47 följer att teleoperatörer har tystnadsplikt vad gäller uppgifter om teleabonnemang, innehåll i telemeddelanden och uppgifter om teletrafiken. (Här avses t ex uppgifter om vilka nummer som abonnent X har ringt under en viss tidsrymd, information som på polissvenska kallas ”telefonlistor”. Det kan också handla om s k mastinformation – uppgifter om var, geografiskt, en mobiltelefon har befunnit sig vid ett visst tillfälle.)

Vad gäller uppgifter om teleabonnemang kan tystnadsplikten brytas, dvs teleoperatören ska svara på polisens frågor om brottet

[35] Redogörelsen för övervakning inom ramen för kriminalpolisens verksamhet bygger i stora delar på en intervju med Anders Ahlqvist vid Rikskriminalpolisens IT-brottsrotel.

som utreds kan ge fängelse – vilket gäller för de flesta brott – och polisen i det aktuella fallet bedömer att påföljden blir någon annan än böter. (Det räcker således med samhällstjänst.) Operatören ska här lämna ut uppgifter om IP-adresser och hemliga telefonnummer.

För att operatören ska bryta tystnadsplikten vad gäller trafikdata, dvs lämna ut ”telefonlistor”, krävs att det aktuella brottet ger minst två års fängelse – vilket gäller endast ett fåtal mycket grova brott.

För innehållet i samtal eller telemeddelanden medger telelagen överhuvudtaget inget undantag från tystnadsplikten.

Medan Telelagen bestämmer tystnadsplikt för historiska uppgifter (sådant som redan har hänt) har RÄTTEGÅNGSBALKEN, kapitel 23, regler om teleövervakning och teleavlyssning som tar sikte på framtiden. Teleoperatören kan beordras att fr o m ett visst datum lämna ut ”telefonlistor” och ”mastinformation” för ett visst abonnemang om det brott som utreds ger fängelse i minst 6 månader. Teleavlyssning (vilket täcker inte bara vanliga telefonsamtal utan även e-post och annan Internet-användning) kan medges om brottet ger minst två års fängelse.

Speciallagen från 1952 (SFS 1952:98) är av s k solnedgångs-karaktär, dvs dess giltighetstid måste hela tiden förlängas. (Det skedde senast 2002, och lagen gäller nu till 2005-01-01.) Den gäller vid förundersökning om 1) vissa allmänfarliga brott som mordbrand och sabotage, 2) vissa högmålsbrott som uppror och olovlig kårverksamhet och 3) vissa brott mot rikets säkerhet, t ex spioneri. Lagen gäller också försök, förberedelse och stämpling till dessa brott. Den ger polisen utvidgade möjligheter att använda tvångsmedel: häktning, beslag, hemlig postöppning, hemlig teleavlyssning och hemlig teleövervakning. Varför denna specialreglering av utredningar om vissa brott inte kan infogas i rättegångsbalken – om de polisiära befogenheterna verkligen behövs – är oklart. (Av allt att döma är det främst säkerhetspolisen som åberopar sig på den i sitt arbete.)

Det enda lagförslag med direkt relevans för den polisiära övervakningen som har presenterats i Sverige sedan 11 september 2001 skulle faktiskt – om det realiserades – snarare försvåra än underlätta övervakning. I ett delbetänkande från den s k e-komutredningen (SOU 2002:60) föreslås den nu gällande Telelagen bli ersatt med en

ny ”Lag om elektronisk kommunikation”. Där stadgas bl a att teleoperatörer ska radera trafikinformation så fort den inte längre behövs för en korrekt fakturering av abonnenten. För Internet-abonnemang med fast avgift (t ex ADSL-uppkopplingar) torde det innebära att trafikinformation ska förstöras genast.

Telelagen är f n inte särskild tydlig på denna punkt. I vart fall kan operatörerna behålla trafikdata så länge materialet kan behövas av tekniska skäl, en tämligen elastisk tidsgräns.

I en skrivelse till regeringen på hösten 2002 begärde Rikspolisstyrelsen att större hänsyn tas till polisens behov av trafikdata. ”*Polisens möjlighet att få tillgång till uppgifterna bör säkerställas genom särskild lagstiftning som ålägger teleoperatörer att spara uppgifter i minst 12 månader*.” Vidare begär RPS att polisen bör få tillgång till historiska trafikdata i samma utsträckning som man idag kan få framtida trafikdata enligt Rättegångsbalken, dvs teleoperatörens tystnadsplikt borde brytas vid förundersökning om brott som ger minst sex månaders fängelse.[36]

Tilläggas kan att Europarådets konvention om ”brott i cyberrymden” (se kapitel 3.3) kräver effektiva rutiner för att trafikdata i telekommunikationsnät ska kunna sparas.

Konventionens bestämmelser föreskriver bl a att myndigheter snabbt skall kunna säkra data (”snabbfrysning”), för att ge de brottsutredande myndigheterna rådrum till att gå vidare med beslag eller edition. Det ska därför vara möjligt för behörig myndighet att förelägga eller på annat sätt se till att skyndsamt bevara trafikdata oberoende av om en eller flera operatörer varit involverade i sändningen.

Trafikdata skall kunna röjas för de brottsutredande myndigheterna i syfte att kunna identifiera operatörerna och den väg informationen gått. Det skall också vara möjligt att förelägga den som har kontroll över lagrad data att lämna ut denna och att förelägga en operatör att lämna ut information om sina abonnenter.[37]

[36] Skrivelse 2002-09-30. ”Tillgång till telekommunikation för Polisens brottsutredande verksamhet.” Rikspolisstyrelsens diarienummer: RÄS-002-3668/02.

[37] Wennersten, Erik. ”Europeiskt arbete mot IT-brottslighet.” Europarättslig Tidskrift nr 4/2001, sid 481.

Sverige har undertecknat konventionen och även om de flesta länder ännu (i nov/dec 2002) dröjer med att ratificera den tycks alla experter eniga om att den kommer att godtas av Europarådets medlemsländer och, åtminstone i stora delar, få genomslag. Därmed skulle Sverige just vad gäller polisens tillgång till historiska trafikdata åta sig att ändra lagreglerna i ”övervakningsvänlig” riktning. Att reformer är på gång står klart. Jan Stålhandske på Näringsdepartementet berättar att en lagsrådsremiss om en ”Lag om elektronisk kommunikation” förväntas i januari 2003, med sikte på en proposition två månader senare. Den som frågar om innehållet vad gäller polisens tillgång till historiska trafikdata får dock inget besked.

Den som med hänvisning till historisk erfarenhet (se kapitel 4) misstänker att polis och säkerhetspolis överträder sina befogenheter även i IT-samhället kan naturligtvis spekulera i detta. Möjligheterna för en tekniskt kunnig kriminalpolis att med hjälp av en ”trojan” – ett datorprogram som via t ex e-post översänds till den misstänktes dator – komma över information eller lösenord är i princip goda. Det vore emellertid brottsligt (dataintrång enligt brottsbalken 4 kap 9c §) och problemet för polismannen ifråga blir att, sedan han/hon väl kommit över den intressanta informationen, förklara för åklagaren varifrån den kommer. Flera personer inom rättsväsendet måste således vara delaktiga i – eller åtminstone införstådda med – lagbrottet.

I princip torde resonemanget även gälla för säkerhetspolisen. Möjligen är lockelsen att använda otillåtna metoder större eftersom hela verksamheten är omgärdad av så stark sekretess. Risken för upptäckt kan te sig mindre. Å andra sidan sysslar säkerhetspolisen ofta med så allvarlig brottslighet (hot mot rikets säkerhet) att de mest integritetskränkande tvångsmedlen, t ex teleavlyssning, ändå får användas. Kring just säkerhetspolisens verksamhet finns dock (se kapitel 4) särskilda trovärdighetsproblem.

Telematik 2006 genomförs i samarbete mellan VINNOVA 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 2006 kan skönjas och granskas i verkliga livet och i demonstrationsmiljöer flera år före år 2006. Inom ramen Telematik 2006 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 2006.

Utgivna publikationer inom programmet Telematik 2006:

Anders R Olsson Efter 11 september 2001: – Kan Storebror hejdas?

Efter 11 september 2001:
- Kan Storebror hejdas?

Informationsteknikens utveckling och spridning samverkar med dagsläget i världspolitiken till att den polisiära övervakningen kan utökas av medborgarna i västvärlden. Medborgarnas kommunikation har länge blivit alltmer elektronisk och därmed möjlig att övervaka och spåra; och efter den elfte september 2001 har USA förklarat ”krig mot terrorismen”.

Nu kan ”avlyssningsvänliga” tekniska lösningar bli standard för internationella kommunikationssystem. De kategorier människor som anses behöva övervakning utvidgas. Myndigheterna understryker polisens uppgift att förebygga brott, vilket fordrar tillgång till information om stora grupper medborgare, inte bara om dem som är skäligen brottsmisstänkta.

”För den som fäster vikt vid integritetsskydd – möjligheten att värna en personlig sfär, att söka information i diskreta former och att sprida kunskaper eller åsikter anonymt – ter sig framtidsutsikterna mörka”, skriver frilansjournalisten *Anders R Olsson*, som författat rapporten *Efter 11 september 2001: - Kan Storebror hejdas?* Här visar han hur.

Rapporten utges av VINNOVA och TELDOK i programmet *Telematik 2006*. Utgångspunkten för programmet är de förändringar som sker i samband med förverkligandet av kunskaps- och informationssamhället och vad detta betyder för Sverige. Rapporterna skall beskriva hållbara tillämpningar och uthållig användning, med fokus på hur IT används, med framåtblick mot 2006.

VINNOVA
VERKET FÖR INNOVATIONSSYSTEM
& teldok.
VINNOVA-rapport 2003:4 • TELDOK Rapport 149