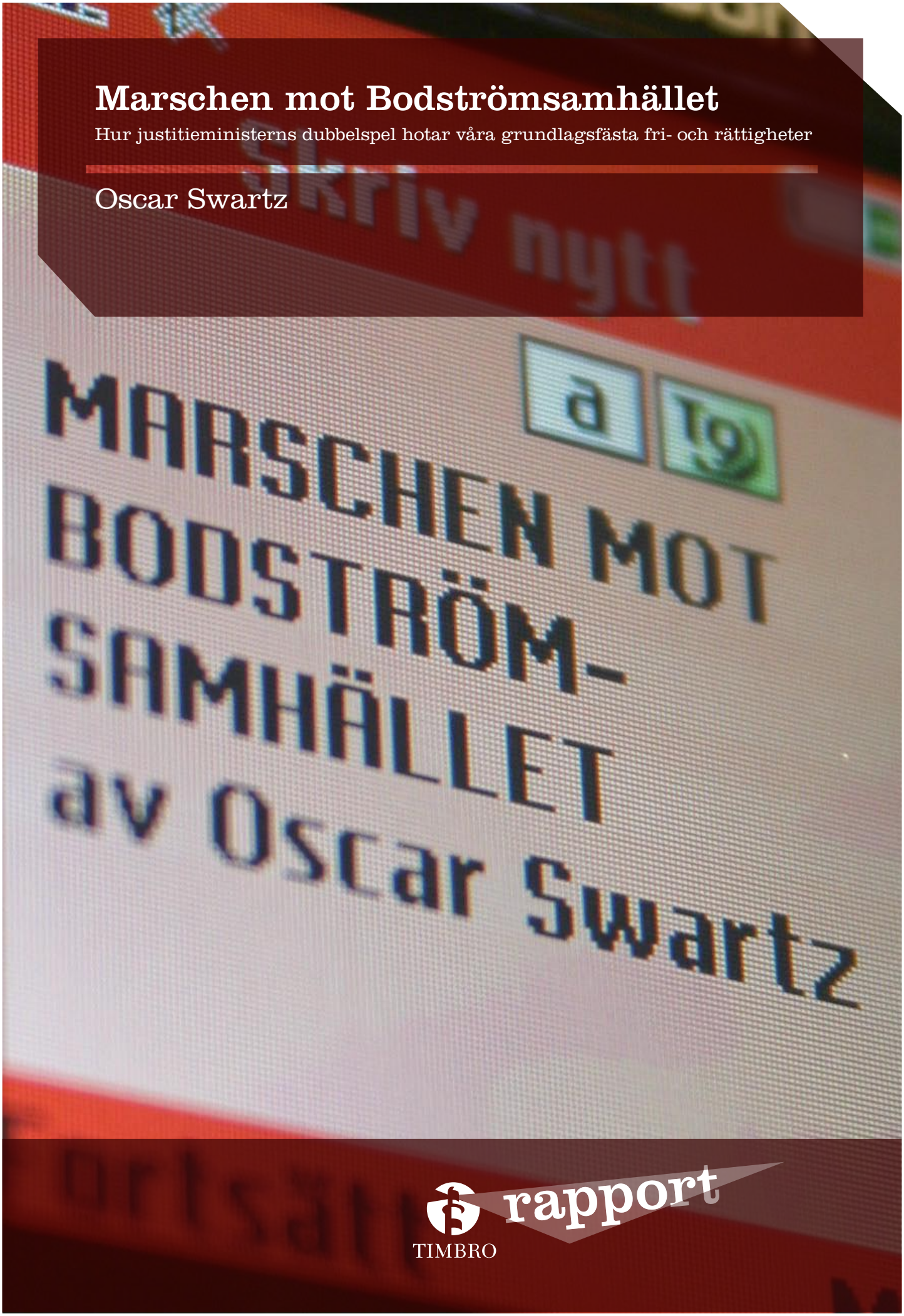
Marschen mot Bodströmsamhället

Hur justitieministerns dubbelspel hotar våra grundlagsfästa fri- och rättigheter

Oscar Swartz



rapport
TIMBRO

Marschen mot Bodströmsamhället

Hur justitieministerns dubbelspel hotar våra grundlagsfästa fri- och rättigheter

Oscar Swartz

Oscar Swartz är skribent med ekonomutbildning på forskarnivå från Handelshögskolan i Stockholm och Columbia University i New York. Han startade 1994 ett av Sveriges första internetföretag och var entreprenör i tio års tid. Nu skriver han och bloggar på http://swartz.typepad.com/texplorer.

TIMBRO

Timbro, Juni 2006
ISBN 10: 91-7566-622-7
ISBN 13: 978-91-7566-622-8
Timbro, Box 5234, 102 45 Stockholm
tel 08-587 898 00, fax 08-587 898 55
info@timbro.se, www.timbro.se

Förord

De senaste åren har ett antal lagförslag som ger staten nya och stora befogenheter vad gäller avlyssning av såväl tele- som Internetkommunikation presenterats. Vissa lagar har redan trätt i kraft medan andra fortfarande befinner sig på utrednings- eller diskussionsstadiet.

Det råder ingen tvekan om tangentens riktning. Regeringen med justitieminister Thomas Bodström i spetsen håller på att skapa ett samhälle som i sin extrema form får framtidsdystopin i 1984 att blekna. Trots detta har debatten inte riktigt tagit fart. Bodström har skickligt presenterat sina förslag som ett hot enbart mot grovt kriminella personer. Journalisten och internetpionjären Oscar Swartz visar i den här rapporten att den bilden är felaktig. Thomas Bodströms idéer hotar inte bara ett litet fåtals, utan alla medborgares, integritet.

Oscar Swartz har tagit ett helhetsgrepp på det han kallar för Bodströmsamhället. Han går systematiskt igenom och analyserar samtliga förslag som hittills har diskuterats. Förhoppningsvis kan rapporten ge fler människor inblick i den utveckling som pågår. Bodströmsamhället berör inte bara tekniknördar och terrorister. Det berör oss alla.

Stockholm i juni 2006

Maria Rankka,
Biträdande Timbrochef

Innehåll

Inledning

Den 24 maj 2005 överlämnade generaldirektören för Kammarkollegium Anders Eriksson utredningen *Tillgång till elektronisk kommunikation i brottsutredningar m m* (SOU 2005:38) till sin uppdragsgivare, justitieminister Thomas Bodström. Ett av Bodströms första beslut som justitieminister efter valet år 2000 var att utse Anders Eriksson att leda BRU, Beredningen för Rättsväsendets Utveckling, i vilken den framlagda utredningen var det sjunde betänkandet. Anders Eriksson var tidigare generaldirektör för Säkerhetspolisen. Det brukar justitiedepartementet inte nämna.

I den här rapporten kommer jag att visa hur den grundlagsstadgade rätten till privatliv och korrespondens stegvis trängs tillbaka och nu på ett häpnadsväckande sätt hotas när man analyserar den sammanlagda effekten av ett antal initiativ från Bodström. De lagförslag som på allvar kan förändra internetkommunikationen för vanliga användare är dock att vänta under 2007, förutsatt att socialdemokraterna sitter i regeringsställning. Det finns alltså all anledning att informera, debattera och agera nu.

Eftersom utvecklingen har varit smygande förekom knappt någon kritik förrän hösten 2005, när Bodström lyckades baxa sitt datalagringsdirektiv genom EU. I december 2005 gick även remisstiden för SOU 2005:38 ut, och det började gå upp för övriga samhället vad som höll på att ske. I mars 2006 lades två propositioner om övervakning och avlyssning fram, som inte hade något med datalagringen eller SOU 2005:38 att göra men som accentuerade lappkastet i svensk lagstiftning.

Förre Säpochefens SOU 2005:38 är skrämmande läsning för en vanlig medborgare. Den välvillige skulle kunna säga att detta ju än så länge bara är en utredning, inte ett regeringsförslag. Det är dock att göra det bekvämt för sig. Att justitieminister Bodström har en annan syn på förhållandet mellan brottsbekämpande myndigheter och medborgarna än vi varit vana vid indikeras kanske av att han den 4 maj utsåg samme förre Säpochef Anders Eriksson till generaldirektör i justitiedepartementet samt till ordförande i Registernämnden. Registernämnden ansvarar bl a för att granska Säpos (alltså de forna kollegernas) efterlevnad av de lagar som förbjuder åsiktsregistrering.

Det har uppstått en debatt kring SOU 2005:38 samt de andra Bodströmförslag som tycks markera ett skifte i svensk rättstradition. Dagens Nyheter ägnade en huvudledare med rubriken *”En justitieminister utan principer”* åt bl a den utredningen.[1] En krönika på samma ämne i Aftonbladet av Jan Guillou sammanfattades av rubriksättaren som *”Bodströms nya lag – farligare än bin-Ladin”*.[2] Bodström har inte kritiserat ett enda av de förslag som förre Säpochefen har levererat i utredningen. Tvärtom går justitieministern till motattack på ett mycket aggressivt och arrogant vis mot kritikerna och hävdar att kritikerna inget förstått. Han gör detta genom att servera rena lögner. Inte små lögner, utan lögner som tycks kallblodigt kalkylerade att lura väljare och allmänhet.

Ett exempel är när han levererar en attack mot integritetsexperten och författaren Per Ström. Artikeln har titeln ”Bara misstänkta övervakas”.[3] Bodström skriver om EU-direktivet om datalagring, vilket kommer att tvinga operatörer att lagra information om vår kommunikation via telefon och Internet. Om Per Ström har han följande att säga:

> *”När hans fantasi får fritt spelrum går ingen människa säker. Ström blandar ihop begrepp och metoder, rykten och fördomar.”*

Sedan lägger Bodström saker tillrätta:

> *”Information från bland annat telefontrafik har visat sig ha avgörande betydelse för att bekämpa mord, terrorism och annan organiserad brottslighet. Vi har på senare tid även sett att de varit viktiga för att avvärja och lösa grova värdetransportrån. Jag vill understyrka att informationen inte omfattar innehållet i samtalen, utan bara när man ringt och till vem. Och detta gäller bara dem som är misstänkta för allvarliga brott. Ingen annan behöver vara det minsta orolig.”*

Thomas Bodström målar ständigt upp denna bild av att han skapar lagar för att komma åt några få väldigt grova brottslingar: terrorister och förhärdade ligor.

Så här ligger det till

EU-direktivet om datalagring kommer att tvinga tele- och internetoperatörer att lagra information om kundernas kommunikation, exempelvis vem som ringer vem vid vilken tidpunkt och vem som skickar e-post till vem vid vilken tidpunkt.

En av de mest omdebatterade punkterna i EU-direktivet om datalagring gällde just för vilka brott myndigheterna skulle kunna begära ut den lagrade datan från operatörerna. *Man motiverade* förslaget med behovet att kunna utreda terrorism och organiserad grov brottslighet. EU-parlamentet började ha synpunkter och man diskuterade i olika omgångar att lagen bara skulle få användas för grova brott med minimistraff på 4 års fängelse. En del förordade 2 år. Till slut enades man om att lämna beslutet om användningen av lagrad data *helt och hållet till de enskilda länderna*, en eftergift till Ministerrådet, där Bodström ursprungligen varit initiativtagare till frågan. För Sveriges del behöver vi inte fundera på vilka brott som kan komma att omfattas. I Sverige har vi redan lagstiftning som bestämmer när den lagrade data som EU-direktivet avser kan bli åtkomlig för myndigheterna. ”Hemlig teleövervakning” kallas denna åtkomst och den regleras i Rättegångsbalken (= RB) 7 kap 19 § samt Lag (2003:389) om elektronisk kommunikation (= LEK) 6 kap 22 §.

I Sverige kan alltså brottsutredande myndigheter få tillgång till de uppgifter Bodström talar om vid utredning av *samtliga brott som har ett minimistraff på 6 månader* eller mer,

vissa *andra specificerade brott med lägre minimistraff* samt dessutom *försöks- förberedelse- och stämplingsbrott till alla dessa, oavsett straffsatser*. En central del av de uppgifter som enligt EU skall datalagras – nämligen IP-nummer för Internetkommunikation – är en av de viktigaste bitarna för att exempelvis jaga fildelare. Och dessa uppgifter är redan i dag åtkomliga så fort en åklagare bedömer att något annat straff än böter kan komma ifråga. I utredningen SOU 2005:38 föreslås dessutom att polisen *utan brottsmisstanke* skall ha *rutinmässig och ständig tillgång* till dessa uppgifter. Datalagring gäller alltså inte ”mord, terrorism och organiserad brottslighet”. Tvärtom är det ju så att den stora del av svenska folket som anser att fildelning av musik och film för personligt bruk borde vara tillåten, och därför ägnar sig åt sådan, *behöver* vara orolig! Att det skulle röra terrorism och grov brottslighet, som Bodström hävdar gentemot Per Ström är alltså en lögn, vilket även bekräftas av Regeringskansliet.[4]

I samma debattserie i Svenska Dagbladet fortsatte Bodströms försök att tysta kritikerna genom rena personangrepp:

> *”Man förväntar sig att en professor har kunskap om eller åtminstone tar reda på grundläggande fakta, innan han eller hon ger sig ut i debatten. Det är minst sagt förvånande att Janne Flyghed, professor i kriminologi, inte vet att uppgifter som lagras från telefonsamtal är av fundamental betydelse för brottsutredningsverksamheten och ofta helt avgörande för att lösa grova brott. Detta hävdar inte bara polis och åklagare utan också den statliga utredningen Tillgång till elektronisk kommunikation i brottsutredningar m m (SOU 2005:38).”*[5]

Varför detta utfall? Jo, Janne Flyghed, professor vid Stockholms universitet, hade vågat försvara Per Ström och bad Thomas Bodström ”att presentera det faktaunderlag han har för att införa buggning samt allmän kontroll av data- och teletrafik. Så vitt vi vet finns inga belägg för att sådana åtgärder är verksamma mot terrorister och grov organiserad brottslighet.” Sedan undrade Flyghed en smula insinuerande: ”Och det är väl mot de grupperna åtgärderna är riktade? ... Thomas Bodström upprepar i sin artikel att det bara är misstänkta för allvarlig brottslighet som skall övervakas. Men stämmer det?” Som jag visade ovan stämmer det inte alls, vilket Bodström givetvis vet och därför måste han undvika sakfrågorna.

Justitieministern vet vad han säger och det kan bara tolkas som att han försöker föra allmänhet och väljare bakom ljuset. Så sent som 1 oktober 2004 reviderades ju Rättegångsbalken 7 kap 19 § på ett sätt som bereder väg för att all information som sparas genom datalagring hos operatörerna enkelt skall kunna fås ut av myndigheterna. Bodström drev ju själv igenom lagen, så den kan inte vara okänd för honom. Man förberedde där för datalagring genom att göra det möjligt att enligt Rättegångsbalken *utföra hemlig teleövervakning på historisk information*, vilket på vanlig svenska innebär att polis och åklagare kan få del av information som tele- och internetoperatörer lagrat om människors kommunikation.

Bodström saknade dock en pusselbit. Trots att Sverige har en paternalistisk stat kan vi med rätta vara stolta över vår tradition av starkt skyddad yttrandefrihet, en offentlighetsprincip som gör att vi kan granska myndigheters agerande samt en starkt värnad privat sfär där förtrolig kommunikation anses viktig att skydda. I Sverige är kommunikationsoperatörer i dag *förbjudna* att lagra data om sina kunders kommunikation – med några få undantag. De kan bli bötfällda om de ändå gör det. Dessutom är de underkastade stark tystnadsplikt om sin kunders kommunikation och kan bli dömda enligt Brottsbalken om de bryter den.

Hur skulle Bodström – i ett land med denna tradition – kunna få en majoritet i riksdagen att kovända? I stället för att *förbjuda* operatörerna att lagra information om kundernas kommunikation ville han alltså *tvinga* dem att göra det. Detta är ingen marginell justering. I dag straffar Sverige en operatör som lagrar data. I morgon vill Bodström straffa – och förmodligen stänga – en operatör som *inte* gör det. Det var sannerligen en politisk uppförsbacke att få en uppgörelse om detta i riksdagen.

Strategin blev att i stället få med sig Ministerrådet i EU, i detta fall bestående av alla ländernas justitieministrar. Genom att fatta ett s k rambeslut skulle Sverige vara tvunget att foga sig. Det föreföll enklare att propagera för detta bland justitieministrar än i den svenska riksdagen. Och vad var då bättre än att appellera till terrorismbekämpning? Sveriges justitieminister blev känd som en av hökarna och drev frågan hårdast – trots att Sverige för en utrikespolitik som inte utsätter oss för terroristhot.

Bodströms förslag till rambeslut var något i hästväg. George Orwell och Big Brother – släng er i väggen! Sändare och mottagare av varje enskild kommunikation via Internet skulle registreras och lagras för att sedan vara åtkomliga för myndigheterna. Varje sökning folk gjorde på Google skulle lagras, varje chattsession, varje hemsida man besökte, varje forum man gick in på – och varje protokoll, som det heter på internetspråk – allt allt allt! Operatörer gick ut och förklarade att detta ju i stort sett innebar att all trafik på nätet måste lagras eftersom kommunikationen går till så att all information bryts ned i små paket som vart och ett har en sändare och en mottagare, och att det oavsett integritetsaspekter inte vore möjligt att spara så mycket material. Men även om Bodström kanske var teknisk och ekonomisk idiot när han lade fram förslaget visar det ju någonting om viljan: Att samla på sig heltäckande informationsmängder om oss alla och låta myndigheterna gå igenom informationen vid behov.

EU är dock oförutsägbart ibland, och det hela blev en uppvisning i EU-politisk dragkamp. EU-kommissionen hävdade att frågan inte kunde beslutas av den slutna kretsen i Ministerrådet utan måste ta vägen via Europaparlamentet. Kommissionen lade fram sitt eget förslag till direktiv om datalagring. Bodström och handläggarna på svenska justitiedepartementet blev rasande och framhärdade i att ministrarna helt enkelt skulle fatta ett beslut i alla fall och tvinga igenom datalagring. Kommissionen och Europaparlamentet svarade med att de i så fall skulle dra det hela inför EU-domstolen, som med stor sannolikhet skulle riva upp beslutet.

Det hela slutade med en förhandlingslösning. Ett kompromissförslag godkändes av parlamentet. Man bör här notera att samtliga svenska EU-parlamentariker röstade nej till datalagringsdirektivet – utom socialdemokraterna. Moderaterna, folkpartiet, vänstern, centern, kristdemokraterna, miljöpartiet, junilistan – samtliga ledamöter sa nej.

Men mer är alltså på väg. En kontroversiell del av SOU 2005:38 gäller det nya tvångsmedlet *hemlig dataavläsning*: Polisen kommer i hemlighet att kunna bryta sig in i folks hem, installera dold programvara som via nätet rapporterar allt de gör på sina datorer; som registrerar varje tangenttryckning och skickar en kopia av allt som finns på hårddiskarna och kopior på alla mejl folk skickar; som sänder information om varje webb som besökes. Visst finns restriktioner runt användningen. Men förslaget handlar absolut inte om att begränsa den hemliga dataavläsningen till kampen mot den omtalade grövsta brottsligheten.

Datainspektionens informationschef Leif Stenström ägnade ett par arbetsdagar åt att lista de lagförslag från de två senaste åren som genomförts, befinner sig under utarbetande eller har lagts fram och som rör kontroll och övervakning om enskilda. Det hela resulterade i artikeln ”Vem gnager på integriteten?”[6] Stenström fick ihop en lista på 22 förslag, men garderade med att det kan finnas fler. Datainspektionen påpekade också att många av förslagen bygger på s k Departementspromemorior (Ds-serien), snarare än utredningar (SOU). Skillnaden är att Ds-serien utarbetas av enskilda tjänstemän på departementet (i detta fall nästan enbart justitiedepartementet). Dess tjänstemän representerar rättsväsendet och har ingen bredare samhällsförankring, vilket SOU:er brukar ha, även om vi i fallet SOU 2005:38 snarast har att göra med en önskelista från Säkerhetspolisen. Som kriminologiprofessorn Janne Flyghed uttryckte saken i sin kritik av detta faktum: ”Är det ensidiga partsintressen som skall styra tvångsmedelsutvecklingen?”[7]

Datalagringen är bara en del av den stora apparat för kontroll och övervakning av oss alla som Bodström nu bygger. Jag kommer att visa det få har förstått, nämligen hur långtgående förslag som är på väg att ta form i justitiedepartementet, vilka konsekvenser Bodströmsamhället får för vår kommunikation och dessutom att förslagen på intet sätt är begränsade till de grova brott, som gärna framhålls. Jag redovisar också det dubbelspel Thomas Bodström ägnar sig åt. Hans offentliga retorik överensstämmer inte med det han faktiskt gör. Och i fallet med datalagringen redovisar jag fakta om hur han agerade. Fakta som bör undersökas av Konstitutionsutskottet för att utröna om han har bedragit riksdagen om vilken Sveriges linje i EU verkligen var.

Kritiken kommer från alla håll. Som vänsterledaren och stödpartisten Lars Ohly sa till Aktuellt:

> *”Jag tror aldrig vi har sett maken till mängd av förslag och snabbheten i förändringen av Sveriges lagstiftning i repressiv riktning som vi har sett under Thomas Bodströms tid som justitieminister. Det är ett rekord för Sverige.”*[8]

Förtrolig kommunikation: Om post- och telesekretess

Det känns fullkomligt naturligt att kunna gå in på ett café och tala med en bekant – utan att caféägaren begär ID och registrerar namn, adress och tidpunkt när vi kommer och går och sedan, på begäran av myndigheter, plockar fram sina besöksjournaler från de senaste åren. Det känns också naturligt att kunna gå till en brevlåda och posta ett brev – utan att visa ID-kort för en postmästare som noggrant för in vårt namn i en liggare och noterar till vem brevet skickas.

Ja, denna princip har ansetts så viktig för västerländska demokratiska samhällen att Europakonventionen om de mänskliga rättigheterna i Artikel 8, punkt 1, slår fast att:

> *”Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.”*

I Sverige fastslår grundlagen att Europakonventionen gäller och dessutom finns separata skrivelser om samma fråga i Regeringsformen 2 kap, 6 §:

> *”Varje medborgare ... är skyddad mot ... undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande.”*

Dessa rättigheter är naturligtvis inte absoluta. Men i princip är det detta som gäller och staten måste noggrant motivera om man vill inskränka dessa rättigheter, vilket bara är tillåtet med hänvisning till vissa specifika skäl. Åtgärder måste också stå i rimlig proportion till det syfte som skal tillgodoses genom ingreppet. Jag återkommer till detta senare, men låt oss hålla i bakhuvudet att grundlagar inte är tillkomna i en hast och att de inte ändras i en hast. De är sprungna ur historiska processer för att *skydda oss mot oss själva*. De skall förhindra oss och våra folkvalda från att fatta förhastade beslut som riskerar att underminera demokratin.

Caféprincipen – att kunna samtala med någon utan obligatorisk registrering av vem man samtalar med och utan att samtalet spelas in – gäller i dag när vi pratar i telefon eller skickar post elektroniskt. ”Lag (2003:389) om elektronisk kommunikation”, där 6 kapitlet har titeln *Integritet*, förbjuder tele- och internetoperatörer att avlyssna eller lagra kundernas trafik. Inte heller får de lagra information om vem som kommunicerar med vem. Dessa trafikuppgifter måste utplånas eller avidentifieras så fort de inte längre behövs för att överföra ett elektroniskt meddelande. Ett undantag finns: Operatörerna får lagra uppgifter för att kunna sköta sin fakturering. De måste dock förstöra dem så snart fakturan är betald eller tvistetiden har gått ut. De får inte ens lämna ut

uppgifter om vem som har ett visst abonnemang såvida inte kunden har medgivit det. ”Hemligt nummer” och ingen datalagring är alltså den lagstadgade grunden, både för telefoni och Internet.

Tystnadsplikten om de (eventuellt) lagrade uppgifterna är lagstadgad och stark. Den som röjer uppgifterna kan dömas till brott enligt brottsbalken: ”Brott mot tystnadsplikt” eller ”brytande av post- eller telehemlighet”. För brott som inte finns listade i brottsbalken (att exempelvis lagra trafikuppgifter trots att man inte får det) kan man dömas till böter enligt LEK, 7 kap. 15 §.

Tystnadsplikten får bara brytas i några få sammanhang. De intressanta här är:

1. Abonnentuppgifter, och ibland trafikdata, får lämnas ut i vissa sammanhang som bedöms vara av värde för abonnenten själv. SOS Alarm har exempelvis tillgång till uppgifter om ”hemliga” telefonnummer.

2. Abonnentuppgift skall lämnas ut om polis eller åklagare begär det, och de i sin tur får endast gör det om de undersöker brott som bedöms leda till annan påföljd än böter (fängelse eller villkorligt med eller utan skyddstillsyn).

3. Vissa andra myndigheter kan få ut abonnentuppgifter i vissa sammanhang, t ex Skatteverket och Kronofogdemyndigheten.

4. Andra uppgifter, t ex vilket abonnemang som ringde vilket abonnemang vid en viss tidpunkt, får bara begäras ut vid utredning av brott som har minimistraff på 2 års fängelse. (Men vi får inte glömma bort att egentligen får ju inte operatörerna lagra några data såvida de inte måste för sin egen fakturering. Det är alltså inte säkert att det finns något att begära ut.)

Här kommer Rättegångsbalken in. Den reglerar bl a tvångsmedel, alltså vad polis och åklagare får ta sig till mot den enskilde mot dennes vilja. I en ”polisstat” bestämmer polismakten själv vad den vill göra, och enskilda kan inte värja sig mot övergrepp och godtycke. Demokratiska rättsstater är medvetna om riskerna med att ge fria händer till den eller de myndigheter som innehar våldsmonopolet i samhället. Varje agerande måste därför strikt följa lagen och dessutom måste man bygga in balanser där olika institutioner kontrollerar varandra. En polispatrull har ingen rätt att plötsligt komma och söka igenom ditt hus. För husrannsakan krävs att en domstol ger dem denna rätt efter att en åklagare under en brottsutredning begärt detta samt visat att förutsättningar för åtgärden föreligger. I enklare fall får åklagaren besluta själv, men under tjänsteansvar.

Man skulle kunna tänka sig att polisen helt enkelt gör husrannsakan hos en operatör för att plocka med sig servrar eller tvinga fram den specifika information de är ute efter. Den starka synen på kommunikationens sekretess och integritet kommer dock fram i det faktum att de inte kan använda sådana ”generella tvångsmedel” *mot operatörer.*[9]

I Rättegångsbalken finns i stället ett antal hemliga tvångsmedel reglerade som myndigheterna i stället är tvungna att ta till om de vill ha uppgifter som rör vår kommunikation. Åklagare kan av domstol begära att få använda *hemlig teleavlyssning*[10] (ta del av innehållet i meddelanden) och *hemlig teleövervakning* (få del av annan information som angår meddelanden) för en brottsutredning, förutsatt att det gäller en skäligen misstänkt person och åtgärden är av synnerlig vikt för utredningen. Fram till 1 oktober 2004 innebar det att domstol kunde besluta att avlyssning måste initieras av operatören, vilket alltså innebar att polisen kunde sätta igång och avlyssna trafikinnehållet på ett visst telefonnummer (eller internetabonnemang). På samma sätt kunde teleövervakning initieras, vilket innebär att operatören börjar spara trafikdata, d v s uppgifter om trafiken (exempelvis när och till vem en abonnent skickar e-mejl). *Man kan säga att domstolsbeslutet om tvångsmedel innebar att datalagring påbörjades för en viss abonnent. Datalagring var alltså något som bara drabbade skäligen misstänkta personer och endast abonnemang som de själva innehade eller kunde förväntas komma att använda.*

Caféprinicpen för konversation – alltså att vi faktiskt tillåts sätta oss på ett café och snacka utan att ägaren registrerar oss – är i Sverige på väg bort om vi kommunicerar elektroniskt. Ja, snart är den helt avskaffad. Vi kan dock fortfarande vara med och påverka politikerna och stävja de värsta övertrampen. Vill man tolka skeenden på ett cyniskt sätt var följande lagändringar några små steg på vägen mot en större vision av kontroll över medborgarnas kommunikation, en tillvänjningsfas med successiv förändring eftersom folkopinionen inte skulle svälja hela den beska medicinen i ett svep.

”En mer ändamålsenlig reglering”

(= *mer övervakning och avlyssning på Bodströmska*, [övers anm])

Ett första steg på vägen mot Bodströmsamhället togs den 22 maj 2003 då regeringen lade fram en proposition med den föga uppseendeväckande titeln: *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering.* Vem kan ha något emot en sådan? Offentliga ombud låter fint, vad det än är. Ändamålsenlighet är ju alltid bra och lär inte ifrågasättas av någon. Kanske var det därför man tog bort ändamålsenligheten från rubriken på pressmeddelande från justitiedepartementet samma dag: *Offentliga ombud införs i ärenden om hemlig teleavlyssning.* Många ord i meddelandet används till att beskriva hur ett system med offentliga ombud skall öka rättssäkerheten. Sedan nämner man i kortast möjliga ordalag fyra viktiga ändringar i regleringen av hemliga tvångsmedel (inklusive hemlig kameröövervakning) som i samtliga fall rejält ökar myndigheternas möjlighet att avlyssna och övervaka, alltså göra dem mer ”ändamålsenliga”. En femte ändring – som jag nog skulle säga är den mest principiellt omvälvande – nämns inte ens. Den kan se oskyldig och teknisk ut på ytan, men visar sig ha stora konsekvenser och kan vara den som definitivt sätter stopp för caféprincipen i svensk kommunikationshistoria. De nya lagarna började gälla 1 oktober 2004.

Låt oss gå igenom utvidgningen av tvångsmedlen eftersom de visar principen för det som är på gång. Man utvidgar möjligheterna i flera dimensioner

1. **Åtkomlig information utvidgas.** Exakt vilken information myndigheterna kan komma åt genom tvångsmedlen är givetvis viktigt. Här lägger man till en kategori, vilket kan sägas utgöra en ny princip.

2. **Brottskatalogen utökas.** Det brukar heta att starkt integritetskränkande tvångsmedel – som att i hemlighet få all sin kommunikation avlyssnad eller få en spionkamera inmonterad i lägenheten – måste finnas för att utreda riktigt grov brottslighet. Här kryper man dock rejält nedåt bland brotten och kommer att kunna inkludera en rad nya.

3. **Vem som kan bli utsatt för övervakning och avlyssning utökas.** Det är inte längre bara misstänkta brottslingar utan i princip alla deras vänner och kontakter.

1. Mer information blir tillgänglig:

Före propositionen *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering* var alltså regeln att hemlig teleavlyssning och hemlig teleövervakning gällde *framåt i tiden*, från det att domstolen beslutade om åtgärden. Då kunde

man börja avlyssna och övervaka. Detta ändrades i lagförslaget. *Avlyssning och övervakning fick nu ske även retroaktivt och gälla historiska data*. Det låter kanske ologiskt med normalt språkbruk. Att avlyssna och övervaka indikerar ju närmast någon typ av kontinuerlig aktivitet som sker i realtid. I Rättegångsbalken innebär dock ”avlyssna” helt enkelt att få del av innehållet i ett telemeddelande. Låt säga att detta telemeddelande finns lagrat hos en operatör. Då kan det ”avlyssnas” trots att kommunikationen kanske ägde rum för länge sedan. Samma sak med övervakningen. Att ”övervaka” innebär helt enkelt att få tillgång till uppgifter *om* telemeddelanden. Om sådana uppgifter finns lagrade kan man alltså övervaka kommunikation som redan skett.

Ändringen i sig kan synas oviktig eftersom historiska data hos operatörerna ju egentligen inte borde finnas alls. Som nämnts förbjuder LEK operatörerna att lagra innehållet i kommunikationen eller uppgifter om kommunikationen. Det finns dock undantag. Vi såg undantaget för uppgifter som har med fakturering att göra, vilket innebär att telefonbolagen ofta lagrar information om vem som ringde vem och hur länge samtalet pågick. De behöver detta för att kunna skicka ut räkningar och kontrollera räkningar vid tvister. Abonnenter kan också *ge operatören tillstånd* att lagra information. Och de gör det ofta genom de tjänster de väljer att använda. Hos en internetleverantör kan man till exempel välja att använda deras webbmejltjänst, vilket kan innebära att man ackumulerar stora arkiv av e-post på operatörens servrar för att kunna komma åt sin e-post från vilken dator som helst via en vanlig webbläsare. Utvidgningen till att göra historisk information åtkomlig är alltså inte så tandlös.

Vi har tidigare sett att polisen redan kan använda LEK för att få ut historisk information. Nu kan de alltså *även* komma åt den genom att använda Rättegångsbalkens bestämmelser om tvångsmedel. Så vilken extra information kunde man få ut som ett resultat av de lagar som föreslogs i propositionen och röstades igenom i riksdagen? Jo, enligt LEK kan myndigheterna *aldrig*, inte ens med husrannsakan, få tillgång till *innehållet* i historiska meddelanden, så möjligheten att *avlyssna* historisk kommunikation är genuint ny. Inte ens med husrannsakan kunde man tidigare göra det. Enligt LEK kan man få ut uppgifter ”som angår ett särskilt elektroniskt meddelande”, inklusive lagrade historiska uppgifter. Det är alltså samma uppgifter som avses i Rättegångsbalkens bestämmelser om hemlig teleövervakning, men begränsningen att uppgifterna skall röra ett ”särskilt” meddelande är borta och torde innebära att en utvidgning har skett även här vad gäller informationsmängden. Nu ges ju automatisk rätt att plocka ut all information som lagrats om kommunikationen på ett helt abonnemang.

Att man adderade möjligheten att i hemlighet teleövervaka historisk information är av stor principiell betydelse eftersom detta banar vägen för ett snabbt implementerande av det omdiskuterade EU-direktivet för datalagring, som efter ett par års procedurer slutgiltigt fastställdes den 15 mars 2006. Redskapet finns

alltså sedan den 1 oktober 2004. Nu väntar man bara på att få mer data att applicera det på, vilket EU-direktivet tar hand om.

2. Brottskatalogen utökas

Före propositionen fick hemlig *teleavlyssning* och *kameraövervakning* ske endast vid utredning av brott för vilka *minimistraff* på 2 års fängelse var föreskrivet, alltså hyfsat grov kriminalitet. Nu införde man s k straffvärdesventiler som säger att alla brott omfattas ”om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i 2 år”. Det gäller nu alltså att bedöma om det brott man undersöker kommer att ge 2 års fängelsestraff eller mer i det enskilda fallet. Åklagaren kan alltså gå till domstol och begära användning av tvångsmedlen för en rad brott som aldrig tidigare hade kommit ifråga. Lagrådet är generellt kritiskt till sådana ventiler:

”Nackdelen med straffvärdesregeln är att ett brotts straffvärde skall prövas med hänsyn till en rad faktorer (se 29 kap. 1–3 §§ brottsbalken) varav bara en del torde vara kända för de instanser som skall bedöma dem i tvångsmedelsärendet. Det finns stor risk att bara för den misstänkte negativa faktorer tas med i bedömningen och att straffvärdet för det enskilda brottet senare visar sig vara betydligt mindre än vad som antagits först.”[11]

Före propositionen fick hemlig *teleövervakning* ske endast vid utredning av brott för vilka *minimistraff* på 6 månaders fängelse var föreskrivet. Regeringen ville införa en straffvärdesventil även här. Lagrådet var dock mycket kritiskt och avstyrkte ”eftersom den innebär att hemlig teleövervakning kan användas som tvångsmedel vid många brott som kan leda till en icke frihetsberövande påföljd”.[12] I den slutliga propositionen var förslaget borttaget, men man indikerade att man inte var nöjd utan varnade: ”Regeringen avser dock att noga följa utvecklingen och kommer om det behövs att återkomma till frågan i ett annat sammanhang.”[13] Man utökade dock brottskatalogen genom att lägga till ett par specifika brott för vilka hemlig teleövervakning skall få användas trots att de inte har 6 månaders fängelse som minimistraff: dataintrång och barnpornografibrott. (Man kan här notera att brottet ”grovt barnpornografibrott” har 6 månader som minimistraff så detta var redan inkluderat. Man lade till paragrafen för att kunna teleövervaka även vid misstanke om ”normalt” barnpornografibrott (Brottsbalken 16 kap 10 § a). Dessutom utökade man de försöks-, förberedelse- och stämplingsbrott som kan komma ifråga för hemlig teleövervakning.)

3. Fler får övervakas och avlyssnas

Före propositionen var principen att den avlyssnade/övervakade måste vara skäligen misstänkt för ett brott. Denna princip avskaffas genom att myndigheterna nu ges rätt att i hemlighet teleavlyssna och teleövervaka abonnemang tillhörande personer som inte alls är misstänkta för brott. Om polisen har synnerlig

anledning att anta att den misstänkte har kontaktat, eller kommer att kontakta, en annan person kan även dennes abonnemang avlyssnas och övervakas.

Principen var också den att man måste ha en skäligen misstänkt person för att få använda hemliga kameror. Observera att detta tvångsmedel inte har något att göra med s k ”allmän kameraövervakning” i exempelvis butiker eller tunnelbanan. Här är det alltså fråga om att i hemlighet montera upp en dold spionkamera i en lägenhet eller ett kontor för att smygfilma en viss person i samband med brottsutredning. Nu infördes i lagen att man även får montera upp sådana hemliga kameror utan att ha någon skäligen misstänkt person. Man får sedan den 1 oktober 2004 övervaka en plats där ett brott har begåtts eller en plats i dess nära omgivning, om syftet är att försöka utröna vem som kan *bli* skäligen misstänkt.

Vad innebär nu detta med ”en mer ändamålsenlig reglering” i praktiken? Jo, låt säga att polisen tror att en person som är skäligen misstänkt för ett brott som de *bedömer att de kan övertyga rätten om att det kan ge* två års fängelse, brukar ha mejlkontakt med dig och kan ha nämnt eller kommer att nämna något som kan hjälpa dem i utredningen. Då kan polisen begära av domstol att få använda hemlig teleavlyssning *mot dig* och läsa all din e-post *som finns lagrad* hos operatören samt givetvis alla mejl du skickar och tar emot framöver. Vi skall inte underskatta skillnaden mot tidigare då en person som var skäligen misstänkt för ett brott med två års *minimistraff* kunde få sin *egen* telefon eller e-post avlyssnad framåt i tiden från domstolsbeslut.

Det finns givetvis generella rekvisit som åklagaren måste visa domstolen att han uppfyller när han begär att få använda hemliga tvångsmedel. Exempelvis skall åtgärden vara av ”synnerlig vikt för utredningen”. Man kan notera att rätten under 2004 avslog begäran om hemlig teleavlyssning i endast 1 fall av 715.[14] Man kan tolka det på samma sätt som Riksåklagaren och Rikspolisstyrelsen, nämligen att deras underlag är så goda och välgrundade. Det skulle också tolkas som att en domare inte kan göra mycket mer än godkänna begäran eftersom han endast har en sida att gå på. Och det är här ombuden kommer in.

Offentliga ombud

Det är tingsrätten som ger tillstånd att använda hemliga tvångsmedel i en brottsutredning. Åklagaren lägger fram sitt fall och rätten avgör. Prövningen i domstol om åklagarens begäran uppfyller de krav som lagen ställer anses utgöra en garanti för rättssäkerheten. Eftersom de hemliga tvångsmedlen är speciellt integritetskränkande har tankar funnits på att ge den enskilde någon form av representation mot åklagaren. Eftersom tvångsmedlen är hemliga kan den enskilde ju inte underrättas om vad som håller på att ske. Offentliga ombud infördes tillsammans med de redan nämnda lagändringarna.

Ombudet företräder dock inte den misstänkte. Ombudet ”företräder enskildas rätt och integritetsintressen i allmänhet” men får inte inhämta någon egen information om ärendet utan måste acceptera det som serveras av åklagaren. Regeringen har flera gånger tidigare avvisat tankar på offentliga ombud i andra sammanhang.[15] Exempelvis har man tidigare avvisat förslag eftersom: *”det var tveksamt om det offentliga ombudet kunde fylla någon reell funktion eftersom ombudet inte kunde hämta in upplysningar från den misstänkte eller från något annat håll än åklagarens”*.[16]

Lagrådet kommenterade att ett offentligt ombud egentligen inte fyller någon annan funktion än exempelvis ytterligare en domare i rätten skulle ha. Dessutom kritiserar man att regeringen själv utser ombuden, eftersom ombuden ju skall representera ett intresse som går emot statens i dessa fall – där ju staten är parten som vill tillgripa hemliga tvångsmedel mot en enskild. Lagrådet menar att misstankar kan uppstå om att bekväma och ”pålitliga” personer förordnas till offentliga ombud av regeringen.

Sedan den 1 oktober 2004 gäller den föreslagna ordningen och offentliga ombud finns numera vid ansökan om hemlig teleavlyssning och kameraövervakning, dock inte vid ansökan om hemlig teleövervakning. Om de tjänar något annat syfte än att bli rubrikmaterial när justitiedepartementet börjar bygga ut övervakning och kontroll vet vi inte.

Datalagringen: Hur Sverige fick EU att massregistrera medborgarnas kommunikation

Den 11 mars 2004 smällde bomberna på pendeltågen i Madrid. EU snabbinkallade justitieministrarna till ett rådsmöte den 19 mars för att diskutera åtgärder mot terrorismen. Riksdagen i sin tur lyckas blixtinkalla EU-nämnden dagen innan för att förbereda. EU-nämnden fungerar som ett utskott i riksdagen och har 17 ledamöter från alla partierna. Sverige representeras av sina statsråd i Europeiska Unionens Råd, det högsta beslutande organet i EU. Men ministrarna skall ju driva Sveriges linje i EU, inte sitt partis. Regeringen rådgör i EU-nämnden och förväntas följa majoritetens ställningstagande.

På mötet den 18 mars nämner justitieminister Thomas Bodström en fråga han tror kommer att diskuteras i EU nästa dag, på terrormötet:

> *”En sak som jag vill understryka är frågan om lagring av trafikdata, alltså mobiltelefonsamtal och liknande, hos teleoperatörerna. Detta är vi angelägna att diskutera. Bomberna i Madrid utlöstes ju med hjälp av just mobiltelefoner, och uppgifter om mobilsamtal är oerhört viktiga i många brottsutredningar.”*[17]

Idén visar sig vara väckt av Bodström själv.[18]

Bodströms EU-nämndsmöte den 23 april var bara en halvtimme långt och en rad frågor drogs igenom i rasande fart. Bodström nämnde att man vid toppmötet i mars, i deklarationen mot terrorism uttalade att lagring av trafikdata skulle prioriteras samt att Sverige nu skulle lägga ett förslag till rambeslut i EU tillsammans med Frankrike, Storbritannien och Irland. Han läste upp följande:

> *”Rambeslutets huvudsakliga syfte är att underlätta det straffrättsliga samarbetet mellan medlemsstaterna genom att säkerställa att data från allmänna elektroniska kommunikationsnät finns tillgängliga när det behövs för att förebygga, utreda, upptäcka eller åtala brott inklusive terrorism. Teleoperatörer och Internetoperatörer ska enligt förslaget åläggas att lagra vissa data under viss tid, nämligen 12–36 månader.”*[19]

Ingen reagerar. Ännu. Ledamöterna är överrumplade och Madridchockade. Och EU-nämnden diskuterar under samma sittning allt från ”AVS-ländernas position rörande Cotonouavtalet” till ”krav på ljudskrämmare på fisknät för att förhindra oavsiktlig fångst av små valar”. Så utan diskussion får justitieministern klartecken att lägga fram det där antiterrorförslaget.

Men vänta nu, vad står det egentligen? Jo, det gäller ”brott” i allmänhet, där terrorism nog nämns specifikt av ett enda skäl: Att dra uppmärksamheten från det egentliga syftet. Och en helt ny princip skall tydligen införas. Hittills har, som vi sett, myndigheterna kunnat få ut uppgifter om vår kommunikation vid förundersökning av misstänkt brott, via reglerna i RB och LEK. Men här gäller det inte bara utredning av brott. Det gäller att *förebygga* och *upptäcka*, vilket väl innebär att man vill kunna använda den lagrade datan till att spionera? Se vad folk har för sig för att kanske upptäcka något misstänkt. Och hallå, det talades ju om mobiltelefoner nyss! Men nu har internetoperatörer stoppats in trots att dessa tidigare knappast har lagrat någon data alls om sina kunders surfande. Ja, som vi såg har de varit *förbjudna* att göra det förutom av faktureringsmässiga skäl. Förslaget handlar alltså inte egentligen om terrorism, vilket framgår om man noggrant studerar vad justitieministern faktiskt meddelade då, den 23 april 2004, på EU-nämndens möte i Stockholm.

Fem dagar senare lägger Konungariket Sverige fram ett förslag till rambeslut tillsammans med Republikerna Frankrike, Irland och Storbritannien.[20] Bodströms handläggare har inte varit blyga. Man kan nog säga att de tagit i från fotknölarna. Förutom uppgifter om telefoni, SMS, MMS och liknande tjänster vill de att följande trafikdata för Internet lagras:

> *”uppgifter som genereras av tjänster inom ... följande protokoll: ... Internetprotokoll, inklusive e-post, protokoll för rösttjänster över Internet, webben, protokoll för filöverföring, protokoll för nätöverföring, protokoll för överföring av hypertext, rösttjänster för bredband och undersekvenser av Internetprotokollnummer – nätadressöversättningsuppgifter.”*[21]

Med reservation för både imprecis och delvis udda terminologi kan man säga att det där fångar precis all kommunikation på nätet. Man skall inte lagra innehållet i kommunikationen men många andra uppgifter *om* den: vem som sände (innehavare av abonnemang med namn och adress), vem som mottog, tidpunkt, fysisk plats det sändes från, vilken typ av kommunikation det rörde.[22]

För att förslaget till rambeslut verkligen skall bli ett beslut – som alltså blir bindande för alla medlemsstater i EU – krävs förhandlingar mellan ländernas justitieministrar. I en del frågor krävs kvalificerad majoritet enligt ett ganska komplicerat system där t ex olika länders ministrar har olika många röster. I många frågor krävs enhällighet, och det är ändå vad man ofta strävar efter. I den processen skall regeringen alltså rådgöra med EU-nämnden i Sveriges riksdag. Man är inte rättsligt bunden att exakt följa EU-nämndens ståndpunkt, även om man måste ”rådgöra”. Konstitutionsutskottet har dock flera gånger uttalat att regeringen förutsätts avstå från att agera i strid med nämndens position och även aktivt följa dess ståndpunkt. Sveriges position i EU-förhandlingar skall alltså, enligt KU, reflektera en parlamentarisk majoritet – inte en ministers, ett departements eller ett partis ståndpunkt.

Jag har gått igenom samtliga protokoll (”EU-mämndens stenografiska uppteckningar”) från justitieminister Thomas Bodströms möten med EU-nämnden i riksdagen, där lagringen av trafikdata tas upp. Jag har jämfört hans diskussioner och uttalanden och svar på frågor från ledamöter där med grundfakta om hur Sverige faktiskt har drivit processen framåt i EU:s ministerråd. Detta kan man åtminstone delvis följa genom EU-dokument. Jag sammanfattar ett och ett halvt års möten i EU-nämnden helt kort nedan, och delar upp materialet i två huvudfrågor som ledamöterna hela tiden återkommer till.

Jag finner ett flagrant dubbelspel. Bodström säger en sak till våra folkvalda riksdagsledamöter men gör något annat. Bodström mörkar medvetet om hur han, som representant för Sverige, agerar i Ministerrådet. Flera partier och riksdagsledamöter i EU-nämnden blir under processen oroliga för vad Sverige egentligen håller på med och börjar motsätta sig datalagringsinitiativet. De ställer oerhört berättigade frågor till Bodström. På vissa punkter förefaller han ljuga konsekvent – eller om man är välvillig – förtiga de sanningar han inser skulle kunna få de ledamöterna att försvåra för honom.

Vad skall lagras?

Kanske har saker legat och grott över sommaren 2004, för på hösten tar oron fart. En fråga som återkommer gång på gång gäller vad som egentligen är tänkt att lagras om vår internettrafik. Ledamöterna tycker att detta är oklart och dessutom av största vikt att veta för att bedöma om de skall kunna stödja Sveriges agerande. Den 26 november samlas EU-nämnden för ”Information och samråd inför ministerrådsmöte den 2 och 3 december 2004”[23]:

> Beatrice Ask (m) har problem med lagring av data om folks beteende på Internet, speciellt information om vilka webbar de besöker, och ser en stor skillnad mot att få veta vilket telefonnummer som har ringt vilket nummer, som i telefonifallet.
>
> *”Men vad som nu kommer med tekniken är att man på det här sättet också lagrar vad folk har läst, tittat på och eventuellt kommunicerat, och det är inte lika självklart. Det är de här invändningarna som kan komma.”*. Hon förklarar också att moderaterna är mot att lagra mer än man gör i Sverige redan.
>
> Karin Granbom (fp) är också obekväm:
>
> *”Det här är en beslutspunkt i dag. Bland annat ska vi ta ställning till vilka uppgifter det är som ska lagras. Det handlar om att vi ska lagra uppgifter från telekommunikation och Internettrafik. De flesta vet väl vad telekommunikation är, vad ett telefonsamtal är. Men vad är Internettrafik egentligen? Är det bara e-mail? Nuförtiden kan man till exempel ringa via Internet, och tekniken utvecklas hela tiden. Jag kan ju själv säga att jag inte är*

någon expert på Internettrafik, och jag tycker att det är svårt att veta vad som kommer att lagras."

Bodströms avfärdar farhågorna och berättar vad regeringens avsikt med Sveriges initiativ om datalagring i EU är:

"Det som jag har efterlyst när det gäller de här sakerna är framför allt att man ska kunna spåra varifrån personer har ringt. Sedan kan jag inte nu vare sig för min egen eller för regeringens räkning binda om det här ska vara tillräckligt, men det är i alla fall det som har varit avsikten."

Här skulle man förstås kunna ställa frågan: Om det nu är detta som är regeringens avsikt, varför har då Sverige lagt ett förslag till rambeslut som inkluderar lagring av information om all internettrafik, inklusive vilka webbar folk besöker? Just sådant som Beatrice Ask frågar om. Hon nöjer sig inte heller utan pressar vidare:

"Jag tyckte inte att jag fick riktigt klart för mig vilka uppgifter som statsrådet kommer att driva att det är man ska lagra."

Det börjar brännas så Bodström svarar inte på frågan utan duckar i stället och förklarar att man nu på ministerrådsmötet bara skall besluta *om* man skall ha tvingande minimiregler för vilka data som skall lagras, men inte vilka data det skall gälla. Bodström har ju i ett formalistiskt beslutsperspektiv rätt. Just då vid detta ministerrådsmöte var det just det där beslutet som skulle tas.

Både Karin Granbom (fp) och Carl B Hamilton (fp) verkar dock fortsatt misstänksamma och vill ha till protokollet att det endast är det där principbeslutet man säger ja till.

Ordföranden konstaterar:

"Ja, det är noterat. Jag konstaterar då att det finns ett stöd för regeringens upplägg inför de fortsatta förhandlingarna."

Men hur är egentligen gången när ett rambeslut bereds, förhandlas och beslutas i Ministerrådet? Jo, ministrarna bekräftar lösningar som är framförhandlade av tjänstemän, givetvis i enlighet med instruktioner och målsättningar från de enskilda regeringarna.[24] Någon enstaka gång, när man på tjänstemannanivå inte kan uppnå enighet under förhandlingarna, tvingas man hänskjuta en fråga upp till ministrarna för formellt beslut. Här fanns nu två linjer som man inte kunde nå enighet om: Skulle man tvinga operatörerna att under längre tid bevara den data de redan i dag (tillfälligt) sparar av operationella skäl. Eller skulle man sätta en miniminivå för vilken information sparas, alltså skulle man kunna tvinga operatörerna att bevarar även data som de i dag inte själva sparar? Länderna hade olika uppfattning och ordförandelandet såg sig tvingat att efterfråga formellt ministerbeslut i rådet.[25]

Men faktum kvarstår: Vid denna tidpunkt ligger Sveriges datalagringsförslag på bordet. Sverige har föreslagit att information om all internettrafik skall lagras och det är alltså – tvingas man förmoda – Sveriges position. Att ministrarna måste kallas in för att lösa en knut på vägen är en detalj och det vet givetvis Bodström. Men han väljer att mörka för EU-nämnden och kör – som vi skall se – oförtrutet vidare med sina maximalistiska krav.

Inför ett ministerrådsmöte den 2–3 juni 2005 skall EU-nämnden ”besluta” om man skall gå vidare med ett utkast till rambeslut, som delats ut till ledamöterna.[26] Frågan om vad som skall lagras är mycket allmänt hållen. På mötet den 25 maj 2005 är det nästan upprorsstämning i EU-nämnden när datalagringsfrågan kommer upp.

> Beatrice Ask (m) viftar med en kritisk rapport från EU-parlamentet och vill lägga ned hela frågan:
>
> *”Här är ett stort utropstecken, måste jag säga. Vi moderater är mycket tveksamma till att gå vidare med ärendet som det ser ut just nu.”*
>
> Hon får medhåll av (v) och (mp). Ingvar Svensson (kd) kräver att artikel 2.2, där det skall slås fast vilken data som måste lagras, blir mycket strikt så att det hela inte blir integritetskränkande.
>
> Och Karin Granbom (fp) upprepar återigen den eviga frågan:
>
> *”Vad är det som ska sparas egentligen? Är det saker som ska sparas som inte sparas i dag? Om det handlar om att man bara ska vissgöra sig om att vissa uppgifter som sparas redan i dag sparas i sex månader, i så fall är det en viktig uppgift. Men är det nya saker som ska sparas? Ska varje hemsida som man har besökt på Internet sparas? Jag skulle vilja få lite mer information innan jag säger vare sig ja eller nej till förslaget.”*
>
> Bodströms svar kan närmast betecknas som en spottloska i ansiktet på Granbom när vi senare skall se vad som pågick från regeringens sida parallellt med hans framträdande i EU-nämnden. Han jämför med vad som gäller i Sverige i dag och säger:
>
> *”...vår principiella inställning är att vi inte ska utvidga något område över huvud taget…”.*

På fråga den 31 augusti 2005 om hur läget i rådet ligger angående lagringskrav svarar Bodströms ämnesråd Erik Wennerström att det pågår förhandlingar om lagringskravets omfattning men att det i dagsläget gäller *” … såväl telefoniuppgifter som Internetbaserade uppgifter såsom e-mail-trafik och URL-adresser, det vill säga adresser till hemsidor”*.[27] Dessvärre kräver ingen att få veta vilken linje Sverige driver i förhandlingarna.

På EU-nämndens möte den 7 oktober 2005[28] finns ett kompromissförslag från ordförandelandet till rambeslut om lagring av trafikdata. Bodström konstaterar att leda-

möterna inte fått ut den rätta varianten eftersom det nyligen har uppdaterats. Han meddelar att kravet på lagring av chattdata inte längre finns med. V, mp, c och m säger att de inte stöder förslaget om datalagring. Fp säger att det är helt avgörande att chatt- och hemsidor nu tagits bort och kd konstaterar att man som väl är har tagit bort surfningen. Vem är då denne ”man” som har tagit bort surfningen? Uppenbarligen inte Sverige. Bodström säger nämligen plötsligt, nu när saken är klar, att han gärna hade sett att chatt och surfning på hemsidor hade inkluderats.

Ordföranden meddelar:

”Jag konstaterar sammanfattningsvis att det finns en majoritet för regeringens ståndpunkt.”

Beatrice Ask (m):

”Det är kanske oartigt att fråga, men hur ser den majoriteten ut?”

Ordföranden:

”Både kristdemokraterna och folkpartiet har gett stöd åt regeringens position.”

I det dokument som ledamöterna inte hade fått ut den 7 oktober fanns en not angående lagring av trafikdata för internetkommunikation. Där kan vi läsa: ”Several delegations [DELETED] could accept or supported the Presidency proposal. Others wanted to go further and include logs of web browsing, Internet chat and peer-to-peer communications [DELETED]. However [DELETED] could not accept the inclusion of Internet chat or other Internet data types”.

I de offentliga dokumenten tycks EU regelmässigt censurera bort de olika ländernas specifika positioner i förhandlingarna. Med tanke på att fyra länder tillsammans presenterade det ursprungliga maximalistiska kravet på lagring av internetdata skulle man kanske vänta sig att det var de som fortfarande krävde lagring av t ex vilka webbar unionsmedborgare besöker. Fast knappast Sverige förstås med tanke på de svar Bodström givit under alla dessa möten i EU-nämnden, där bara några få citat redovisats. Hans budskap har varit att det är telefonin han är intresserad av och att han inte egentligen vill utvidga lagring jämfört med vad som görs i Sverige i dag.

Som tur är har jag lyckats komma över ocensurerade versioner av dokumentet. De visar att det mycket riktigt var fyra länder som in i det sista krävde att inte bara webbsurfning och chattande skulle registreras utan också all peer-to-peer-trafik. Detta inkluderar all fildelning.

Länderna? Belgien, Danmark, Litauen – och Sverige.

För vilka brott?

Vi kan konstatera att ledamöterna i EU-nämnden även oroar sig för hur myndigheterna skall få tillgång till all den lagrade datan. Thomas Bodström upprepar samma svar hela fem gånger på fem olika EU-nämndsmöten: Det gäller *bara* vid *grova* brott, sådana som *har minimistraff på 2 års fängelse*. Han säger att detta redan är reglerat och hänvisar till Lag om elektronisk kommunikation.

Men detta är ju bara en tredjedelssanning. IP-nummer är en viktig del av det lagringstvång rambeslutet handlar om. Detta är en uppgift som operatörerna i dag inte har skyldighet att bevara. IP-nummer och deras koppling till en abonnent kräver – som vi tidigare sett i rapporten – misstanke om brott som i det specifika fallet förväntas ge något annat än böter som påföljd, till exempel villkorlig dom. Dessutom vet givetvis Bodström att riksdagen våren 2003 röstade igenom propositionen *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering m m* där lagrade data blev åtkomliga via Rättegångsbalken från 1 oktober 2004 för brott som har lägsta straff på 6 månaders fängelse samt för vissa andra brott med lägre straffvärden samt dessutom försöksbrott som kan ge mycket lägre straff. Sedan åtminstone maj 2005 vet han också att hans egen utredare föreslagit att *polisen skall få regelmässig tillgång till IP-nummeruppgifter utan någon misstanke om brott*, vilket jag återkommer till senare.

Precis som i medierna skjuter justitieministern alltså kritiken i sank genom att hävda – mot bättre vetande givetvis – att inget egentligen kommer att ändras och att hans små detaljjusteringar bara gäller de allra grövsta brottslingarna. Med en dåres envishet upprepar han samma sak om och om igen. I SvD skriver Thomas Bodström att det finns missuppfattningar kring förslaget och förklarar vad den lagrade datan skall användas till. Detta sker några dagar efter att slutförslaget har blivit accepterat i EU:

> *”Vid misstanke om allvarlig brottslighet, såsom terrorism, människohandel och mord, skall polisen få tillgång till dessa uppgifter bara för att spåra om två människor haft kontakt med varandra.”*[29]

Detta är – som jag hoppas alla förstått vid det här laget – en frisering av sanningen som är så omfattande att det bara kan kallas lögn. Jovisst, vid de misstankarna skall polisen ha tillgång till de lagrade data som Bodström talar om. Men varför inte berätta om alla de andra fallen när polisen också skall få tillgång till dessa data, och att hans departement vid tillfället höll på att bereda ett förslag där man avskaffar alla brottsmisstankar som krav för åtkomst av en viktig del (IP-nummer kopplade till person) av den data som skall lagras?[30] Obligatorisk IP-nummerlagring är ju en viktig del av det EU-direktiv som blev slutresultatet av Bodströms initiativ. Man kan notera den kraftiga lobbying som in i det sista pågick i Bryssel från CMBA (Creative and Media Business Alliance) med globala underhållningsjättar som EMI, Disney och Time Warner bakom sig. Man kontaktade exempelvis samtliga EU-parlamentariker och bad om deras hjälp att få ett nytt och ”effektivt instrument i kampen mot piratkopiering.”[31]

Bodström anser möjligen att intrång i upphovsrätten via fildelning ingår i hans uttryck ”allvarlig brottslighet”. Den miljon svenskar som ägnar sig åt att dela med sig av innehållet på sina hårddiskar lär dock ha en annan uppfattning och skulle anse att hans skrivning är en förfalskning av verkligheten. Just IP-nummeråtkomsten är mycket viktig i jakten på fildelare, som vi strax skall se.

Det står klart att Bodström, även vad gäller myndigheternas åtkomst av data har misslett EU-nämnden och senare försökt missleda allmänheten.

Bodströms agerande bör prövas av KU

Man borde kunna begära att Sveriges justitieminister, som enligt konstitutionsutskottet i riksdagen bör följa viljan hos en parlamentarisk majoritet när han förhandlar i EU, på ett objektivt sätt informerar EU-nämnden så att de andra partierna vet vad de beslutar om. Läsning av stenografianteckningarna visar att justitieministern drivit sin egen agenda. Han tycks ha haft ett mål för vad han vill få EU att anta, och sedan har han ransonerat informationen i Sverige på ett sätt som stöder detta. Vad hade hänt om Bodström på riksdagsmännens frågor hade svarat så här i stället: *”Svenska regeringens linje är att lagra data om i stort sett all internettrafik och speciellt information om vilka webbar folk besöker, information om deras chattande samt data om varje paket med information som de utbyter via fildelning. Och jag vill göra ledamöterna av EU-nämnden uppmärksamma på att den här informationen som skall lagras blir tillgänglig vid undersökning av brott med 6 månaders fängelsestraff och ibland lägre. Dessutom kommer svenska polisen snart att få regelmässig tillgång till vissa av uppgifterna, nämligen de som visar vilken person som innehade ett visst IP-nummer vid ett visst tillfälle – ja, utan brottsmisstankar alltså.”*

Det här gäller frågor som kan vara tveksamma ur grundlagsperspektiv: masslagrade uppgifter om folks kommunikation. Att missleda svenska riksdagen samtidigt som man i EU driver en fråga som kan tvinga Sverige att införa lagar som kan bryta mot både den svenska grundlagen och Europakonventionen är ingen liten fråga. Det är möjligt att det handlar om en ny politisk strategi? Om man inte kan få igenom förslag i riksdagen kan man i stället försöka i en krets av justitieministrar samtidigt som man vilseleder riksdagen.

Mot bakgrund av min redogörelse och mitt material anser jag att KU bör granska justitieminister Thomas Bodströms agerande i samband med Sveriges förslag till rambeslut om lagring av trafikdata i EU.

Effekter av datalagringen och rekommendationer till riksdagen

Egentligen blev det aldrig något *rambeslut* i EU angående lagring av trafikdata. Rambeslut tas av Ministerrådet, d v s direkt av justitieministrarna, medan Europaparlamentet endast får yttra sig om saken. Man röstade ned förslaget två gånger, vilket alltså inte har någon formell betydelse alls. Utan att gå in i detaljer kan man säga att en maktkamp i EU uppstod där EU-kommissionen tillsammans med Europaparlamentet hävdade att frågan var deras och ändå måste passera genom parlamentet. Parterna talade om att stämma varandra inför EG-domstolen och riva upp eventuella lagar som stiftades av den andra sidan. En förhandlingslösning mellan rådet, kommissionen och parlamentet syddes till slut ihop och den hade formen av ett *EU-direktiv*, inte ett rambeslut. Formellt blev direktivet godkänt den 15 mars 2006[32].

Telefoni- och internetoperatörer kommer att vara tvungna att lagra data som visar:

a) sändaren av kommunikationen (telefonnummer/IP-nummer samt riktigt namn och adress på abonnenten);

b) mottagaren av kommunikationen (telefonnummer/IP-nummer samt riktigt namn och adress på abonnenten);

c) start och sluttidpunkt för kommunikationen;

d) data som identifierar vilken typ av kommunikation (telefoni, mobiltelefoni, IP-telefoni samt e-post);

e) data som identifierar användarnas kommunikationsutrustning (bl a IMSI- och IMEI-koder på mobiltelefoner samt för anonyma kontantkort platsen för dess ursprungliga aktivering[33], uppringande telefonnummer vid internetaccess, identifiering av DSL-linje eller annan förbindelse vid fast bredband);

f) lokalisering av mobil utrustning (cell-ID samt cellens fysiska geografiska position under hela kommunikationen).

Ett EU-direktiv skall implementeras i nationell lagstiftning. Bodström har åtskilliga gånger påpekat att det här ett direktiv om minimikrav och att den enskilda nationen kan ha hårdare krav. Med tanke på vad han önskade att EU skulle lagstifta om är det ett hyfsat säkert tips att han vid förnyat mandat kommer att driva en höklinje vid implementering av direktivet i Sverige. Den 18 maj utsågs generaldirektören för Ekobrottsmyndigheten, Gudrun Antemar, till särskild utredare för att föreslå hur direktivet skall implementeras i svensk lag. Hon skall vara färdig den 1 april 2007. Möjligen indikerar

valet av utredare att Charlotte Cederschiöld, Europaparlamentariker (m), var på rätt spår när hon i en bloggintervju hävdade att Bodströms verkliga syfte med datalagring snarare kunde vara att komma åt skattesmitare och fildelare.[34]

Det finns en mängd frågor där man kan göra olika tolkningar, både minimalistiska och maximalistiska. Detta bör parlamentariker och allmänhet ha i tankarna. Om vi väljer internetföretagarperspektivet skulle mina rekommendationer för svensk lag, som ändå skulle uppfylla EU-direktivet, vara:

Gör en snäv definition av vilka operatörer och leverantörer som måste lagra trafikdata. Vilka behöver egentligen lagra? Jo, ”leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät”. För att veta vad detta betyder måste man gå till ett par andra EU-direktiv (2002/21/EC samt 94/48/EC). Gränsdragningen kan synas klar, men när man går ned på detaljnivå är den inte det. Tjänsterna det gäller handlar om att transmittera signaler på elektroniska nätverk men exkluderar tjänster som har med innehåll att göra. En internetleverantörs webbhotell omfattas till exempel inte av direktivet, medan deras accesstjänster och e-post gör det.

Gör en så snäv definition av e-post som möjligt. Frågan är om en tjänsteleverantör som bara erbjuder webbmejl – alltså e-post läsbar via webbinterface – omfattas. Måste denna lagra uppgifter om vem som skickar mejl till vem? Hur är det med webbaserade gemenskaper och forum där man får möjlighet att skicka meddelanden (e-post?), kanske både internt och externt?

Kräv identifikation endast om detta ingår i leverantörens normala sätt att erbjuda sina tjänster. Måste leverantören alltid kräva in verkligt namn och adress av alla sina ”abonnenter”, eller blir anonyma tjänster förbjudna? Om leverantören måste lagra namn och adress för varje kommunikation, ja då innebär det kanske att man inte kan teckna sig för ett webbmejlkonto utan att uppge verkligt namn och adress. Samma sak skulle kunna gälla för att ansluta sig till en ”community”, en webbaserad gemenskap. Eller måste man visa identitetshandling så fort man vill koppla upp sig på ett trådlöst nät på ett café? Eller om man skall surfa på ett bibliotek? Anonymitet på nätet är av stort värde – inte främst ett hot.

Det är fullt möjligt att mer extremistiska tolkningar av dessa viktiga frågor skulle kunna vara grundlagsstridiga. Hela direktivet bör tas till Europadomstolen så småningom. Två mycket tunga EU-instanser som har att yttra sig om lagstiftningen anser att direktivet kan bryta mot Europakonventionen. Artikel 29-gruppen, som består av alla ländernas mostvarighet till Datainspektionen, ansåg att Bodströms första förslag solklart bröt mot Europakonventionen. Vad gäller slutresultatet har man tonat ned detta lite, men om lagen nu måste genomdrivas förser man lagstiftarna med en lista på 20 punkter som måste uppfyllas för att den skall närma sig det respektabla ur mänsklig rättighetssynvinkel och den listan bör studeras av lagstiftarna.[35]

Även *Europeiska ekonomiska och sociala kommittén* (EESK) har att yttra sig om EU-lagar. Den består av representanter för det civila samhället från alla medlemsstaterna. Sverige har 14 ledamöter som främst kommer från stora organisationer: SACO, Transport, TCO, LO, Svenskt Näringsliv, LRF, Kooperationen, Sveriges Konsumentråd, Svensk Handel, Handikapprörelsen m fl. Första meningen i deras yttrande lyder:

> *”Kommittén ser med förvåning och oro på detta lagförslag eftersom det är oproportionerligt och inkräktar på de grundläggande rättigheterna.”*

Deras slutsats? Om man skall ha den där lagen måste den omarbetas helt för att uppfylla grundläggande rättigheter.[36]

Bodström och fildelningen

Ett hinder om man vill skapa ett totalt kontrollsamhälle är förstås det där med IP-numren. I och för sig lyckades Bodström via sin EU-manöver göra lagring av IP-nummer obligatorisk för operatörer. Men vi har ju sett hur Lagen om Elektronisk kommunikation har lagstadgad sekretess runt abonnentuppgifter. För allvarliga brott utgör detta inte något problem för myndigheterna. Enda kravet för att kräva ut uppgiften om vilken abonnent som innehade ett visst IP-nummer vid en viss tidpunkt är att polis eller åklagare vid en förundersökning väntar sig att straffet för det undersökta brottet blir mer än böter om misstankarna bekräftas.

I två domar mot fildelare har tingsrätter nu utdömt straff på 20 dagsböter för brottet ”intrång i upphovsrätt”. Båda har blivit dömda för att utan upphovsmannens tillåtelse ha tillgängliggjort var sin fil, en kopia av en upphovsrättsskyddad film.

Organisationer som Svenska Antipiratbyrån (intresseorganisation för film- och dataspelsbranscherna) och IFPI (dito för skivbolagen) arbetar mot fildelning på nätet. De ansluter till ”hubbar” där folk byter material. Där kan de se de olika datorernas IP-nummer och själva ladda ned material från någon ansluten användare för att sedan polisanmäla att denna olagligen till allmänheten har tillgängliggjort upphovsrättsskyddat material utan upphovsmannens tillstånd. Brottet kallas ”intrång i upphovsrätt”. Polisen begär sedan ut abonnentuppgifter från den internetoperatör i vars nummerserie det aktuella IP-numret ingår. Operatörerna är vid en sådan begäran tvingade att lämna ut uppgift om vilken abonnent som hade det aktuella numret vid den aktuella tidpunkten (förutsatt att de faktiskt har bevarat den informationen, vilket de i dag inte är tvingade till).

I praktiken innebär fildelningsdomarna att myndigheterna inte längre har rätt att begära ut abonnentinformation om en misstänkt endast delat med sig av en filmfil eftersom straffet endast blev böter. Organisationerna har nu polisanmält folk som delat ut mer material för att testa var gränsen för villkorlig dom eller fängelse går. Dock är detta administrativt knöligt eftersom de i så fall måste ha fullmakter från en massa olika upphovsmän.

Vi såg ju att Bodström in i det sista försökte få EU att kräva att operatörerna skulle lagra information om användarnas fildelningstrafik. Fildelning är en mycket kontroversiell fråga som jag inte direkt kommer att diskutera här. Men en stor del av svenska folket håller på med detta, förmodligen över en miljon människor. Dessa anser i allmänhet att de inte gör något moraliskt förkastligt eller något som borde vara olagligt. Det finns också en stark och ökande insikt hos forskare i bl a nationalekonomi och juridik om att upphovsrätten i det digitala samhället med stor sannolikhet är kontraproduktiv i sin nuvarande utformning samt att den är balanserad starkt till fördel för ett partsintresse på allmänintressets bekostnad.

Den 17 mars 2005 presenterade regeringen sin proposition för en skärpt upphovsrättslag, som bland annat skulle kriminalisera nedladdning av upphovsrättsskyddat material. Thomas Bodström har åtskilliga gånger i medierna uttalat att ”tanken med lagen” ju inte är att man skall gå efter tonåringar som byter musik med varandra. Bodström sade något han återkommit till flera gånger senare. I DN citeras han t ex när han säger: ”Med den nya lagen vill vi bekämpa dem som tjänar grova pengar på att sprida upphovsrättskyddat material. Men tanken är inte att polisen ska springa in i hus och hem och jaga tonåringar som sitter och laddar ner, säger Thomas Bodström.”[37] Och i SVT:s Uppdrag granskning uttryckte han i april 2006 att:

> *”Det man skall koncentrera sig på, enligt min uppfattning, det är förstås de personer som tjänar miljoner på bekostnad av unga killar och tjejer som gör musik och som framför musik.”*

Bodströms egen statssekreterare Dan Eliasson var tvungen att erkänna att det nog skulle vara svårt att hitta någon i Sverige som tjänar miljoner på det där viset. Fildelning är ju icke-kommersiell. Det bygger på solidariskt och broderligt delande utan pengar.

I sin offentliga retorik tonar Bodström ned allt som har med fildelning att göra, och på sitt vanliga vis hävdar han att hans initiativ bara handlar om grov brottslighet. Detta ägnar sig alltså Bodström åt samtidigt som han i Bryssel kämpar ända in på mållinjen (d v s långt in på hösten 2005) för att tvinga igenom lagring av varje persons trafikdata om just fildelning, en enorm mängd information som visar exakt vad man har gjort på nätet.

Ytterligare en händelse inträffar våren 2005: Ett mycket viktigt betänkande från Beredningen för Rättsväsendets Utveckling (BRU) presenteras. En av de första åtgärderna Bodström vidtog som minister år 2000 var att utse före detta Säpochefen Anders Eriksson att leda BRU. I november 2003 gavs denne ett tilläggsdirektiv (Dir. 2004:145) som skulle komma med bl a förslag på skyldighet för operatörerna att bevara trafikdata, vilka data detta skulle gälla samt förutsättningar för dessa att lämnas ut till myndigheter. Den 24 maj 2005 läggs resultatet fram som SOU 2005:38, *”Tillgång till elektronisk kommunikation i brottsutredningar”*.

I SOU 2005:38 presenteras en rad häpnadsväckande förslag gällande myndigheternas möjligheter till avlyssning och övervakning av enskilda människor, vilket redogörs för i korthet senare i denna rapport.

Man föreslår också en till synes liten förändring i *Lag om elektronisk kommunikation* som skall göra det enklare att få ut abonnentuppgifter från operatörerna. Abonnentuppgifter för telefoni är ju helt enkelt ”telefonkatalogen”, d v s vem som innehar ett visst telefonnummer. När det gäller ”hemliga nummer” är polisen i dagsläget frustrerad eftersom de inte med automatik kan få ut dessa från operatörerna. Det krävs, som vi nämnt ett antal gånger, misstanke om brott som kan ge fängelse och som i det en-

skilda fallet förväntas leda till annan påföljd än böter för att de skall få tillgång till den uppgiften.

När det gäller Internet definierar man i utredningen abonnentuppgift som information om vem som innehade ett visst IP-nummer vid en viss tidpunkt. För de flesta abonnenter ändras detta nummer ganska frekvent. Tekniskt delas det ut av ens internetoperatör och normalt behöver en användare inte bry sig om det. I princip ger det dock möjlighet att se vad ”ett visst IP-nummer har för sig” på nätet i olika sammanhang. Dock är det ju bara operatören som vet till vilken abonnemangsinnehavare ett visst IP-nummer har givits vid ett visst tillfälle.

Utredningen föreslår nu att operatörer skall vara tvungna att lämna ut abonnentuppgift:

1) till myndighet som skall ingripa mot visst brott förutsatt att man har misstanke om brottet (exempelvis Skattemyndigheten);

2) till polismyndighet och åklagarmyndighet ”även i andra fall”.

I klartext: polis och åklagare behöver inga skäl alls. De skall regelmässigt ha tillgång till abonnentuppgift som gäller t ex ett visst IP-nummer. *Utredningen föreslår till och med att operatörerna till en stor databas hos polisen skall överföra ständigt uppdaterad information om abonnentuppgifter.* Att tänka sig att alla internetoperatörer hela tiden skulle överföra en uppgift till en polisdatabas varje gång de delar ut ett IP-nummer till en abonnent som kopplar upp sig, det är en fullkomligt infernalisk övervakningstanke oavsett om det hela skulle ske online eller kanske i form av bulköverföring en gång per dygn. I Sverige sker det sannolikt minst en miljon ”nummerbyten” varje dag! Det här är något helt annat än en tryckt telefonkatalog.

När Bodström lägger en proposition om att kriminalisera nedladdning är han samtidigt ute i medierna och försöker köpa politiska sympatier för detta genom att hävda att man inte skall jaga tonåringar. Och samtidigt driver han alltså på i EU för att få igenom en lag som tillåter lagring av enorma mängder trafikdata om fildelning och innebär lagringstvång för IP-nummer – vilket han även lyckades med. Han får också på sitt bord ett lagförslag som vill ge polisen tillgång till ett ständigt uppdaterat register över alla svenskars IP-adresser på Internet. Detta lagförslag håller i skrivande stund på att beredas i justitiedepartementet. Att Bodströms uttalande i sig är falskt understryker ju bara det dubbelspel han ägnar sig åt: Hans åsikt om vem polisen skall jaga och vad ”tanken” med lagen är spelar ingen roll. Vi har inte ministerstyre i Sverige. Vi har en rättsstat, där polis och åklagare agerar i enlighet med de lagar och regler som finns. Får man förmoda.

Att Bodström vill ta i med hårdhandskarna mot fildelningen – men inte stå för det offentligt – är glasklart. Han (eller formellt regeringen) uppdrog den 2 mars 2006 (Ju2006/1993/PO) åt Rikspolisstyrelsen och Åklagarmyndigheten att

”tillsammans vidta åtgärder för en effektivare bekämpning av immaterialrättsliga brott, särskilt när det gäller immaterialrättsintrång som utförs med användning av Internet. Uppdraget skall genomföras inom ramen för myndigheternas befintliga anslag och skall redovisas gemensamt senast den 15 juni 2006.”

Det borde väl avse de där förmodade skurkarna som tjänar miljoner, får man anta? Nej, så är det inte:

”Åtgärderna skall i första hand inriktas på de brott som utförs med hjälp av Internet. Både brottslighet av större omfattning och av enklare beskaffenhet skall omfattas av åtgärderna.”

Justitiedepartementet gjorde två utskick med begäran om remissvar på SOU 2005:38. Den 9 september 2005 gick en begäran ut till 53 institutioner. Alla de vanliga i rättsväsendet, några människorättsorganisationer och dessutom åtta tele- och internetoperatörer. Den 11 november gjorde man ett utskick till vad man kallade sex ”tillkommande remissinstanser”. Alla sex var upphovsrättsorganisationer som är kända krigare mot fildelning. Speciellt ombads de kommentera den föreslagna ändringen som skulle innebära att polisen har ett ständigt uppdaterat register över IP-adresser på Internet. Vad förväntar sig departementet för svar av dessa? Självklart det svar de vill höra. Kritikern måste dock ifrågasätta varför man ber Svenska Antipiratbyrån om synpunkter och inte Piratbyrån? Eller Sveriges Konsumentråd? Eller några studentorganisationer. Till exempel.

Synpunkterna var inte oväntade. IFPI, skivbolagens organisation tillstyrker förstås men de vill gå längre: genom domstolsbeslut vill de själva kunna hämta ut abonnentuppgifter (uppgifter om IP-nummer) från operatörerna så att de slipper vänta på polis och åklagare. Skatteverket vill för övrigt i sitt remissvar ha tillgång till IP-nummer för ”underrättesleverksamhet”, inte bara för brottsutredningar. Man vill spana och upptäcka, förebygga och förhindra skattebrott.

Att man på justitiedepartementet överhuvudtaget diskuterar att omdefiniera IP-adresser till att jämställas med telefonnummer är anrmäkningsvärt, vilket Post- och Telestyrelsen kraftfullt påpekar i sitt remissvar på utredningen:

”Det behöver knappast påpekas att IP-nummer inte kan anses vara rena kataloguppgifter som är tillgängliga för var och en. Snarare är det så att IP-nummer kan användas för omfattande kartläggningar av individers nyttjande av elektronisk kommunikation på ett helt annat sätt än traditionella telefonnummer. Att sådana uppgifter som torde vara av stort skyddsvärde ur en integritetsaspekt mer eller mindre godtyckligt skall utlämnas till polis och åklagare även om ingen förundersökning eller misstanke föreligger ter sig olämpligt. Att en effektivisering medför att själva utlämnandet sker mer eller mindre automatiserat talar ännu starkare för denna PTS uppfattning.”[38]

PTS har tidigare gjort ett uttalande som skulle kunna indikera att IP-nummer är att betrakta som abonnentuppgift. Det tar TPS tillbaka i detta remissvar och ber departementet notera att deras uppfattning nu är att IP-nummer tillhör den kategori data som endast kan bli åtkomlig genom tvångsmedlet ”hemlig teleövervakning”, vilket alltså skulle göra det mycket svårare än i dag.

Men IP-nummer var alltså bara en liten – om än viktig – del av SOU 2005:38.

När dammluckorna öppnades: SOU 2005:38

Argument runt SOU 2005:38 har flugit genom medierna. Materialet är omfattande och ganska tekniskt och de praktiska effekterna inte uppenbara. Var och en som läser utredningen inser dock att förslagen är mycket långtgående. Det känns som om dammluckorna har öppnats. Bodströmsamhället börjar ta form.

I vanlig ordning skickar justitiedepartementet ut ett översvallande pressmeddelande[39] där man säger att:

- ”bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning skall moderniseras” *(ja, det var väl på tiden!)*;
- man skall ”förstärka rättssäkerheten” *(utmärkt!)*;
- man skall ”få en domstolsprövning till stånd i samtliga fall där uppgifter om kommunikation behövs i brottsutredningar” *(äntligen!)*;
- förbättra ”möjligheterna att bekämpa den grova brottsligheten” *(ja tack!)*;
- polisen skall få ”använda hemlig dataavläsning vid bekämpning av den allra grövsta brottsligheten” *(tja, det låter som ett lågt pris för att bli skyddad från gängen och terroristerna)*.

Förslaget om det enorma, ständigt uppdaterade registret över alla svenskars IP-adresser nämns inte ens. Vi kan därför misstänka att utredningen i övrigt innehåller en hel del som man helst inte vill tala högt om. Misstanken är fullkomligt korrekt.

Min slutsats är att utredningen öppnar för en fullkomligt infernalisk övervakningsregim som i bloggosfären har kommit att kallas Bodströmsamhället. Men inte ens där har man förstått vidden av det ”Thomas Bodström, justitieminister (s)” – som han brukar underteckna sina debattartiklar – håller på att genomdriva. Själv är jag förbluffad efter att i ganska stor detalj ha studerat hans olika initiativ. SOU 2005:38 måste på allvar bli en politisk fråga. Visst, det är en utredning och inget lagförslag finns ännu. Men Bodström har försvarat varje punkt som hittills har tagits upp till debatt. I jämförelse med den förra utvidgningen av övervakningsregimen sker nu följande:

1. Åtkomlig information utvidgas än en gång, och det rejält.
2. Brottskatalogen utökas så mycket att den avskaffas helt för att komma åt vissa uppgifter.

3. Reglerna för vem som kan bli utsatt för övervakning och avlyssning utökas återigen på ett anmärkningsvärt vis.

4. Nya maktbefogenheter för polis och åklagare.

1. Åtkomlig information utökas

Lokaliseringsdata: Man nämner att det finns osäkerhet i lagstiftning om positioneringsuppgifter för mobiltelefoner som är påslagna, men där samtal inte pågår. I praktiken verkar operatörerna ha varit ovilliga att försöka plocka fram sådan information till polisen, kanske med hänvisning till att det är arbetskrävande och att de inte är förpliktigade att lämna ut den. Det kan alltså röra sig om var en viss mobiltelefon som var påslagen men som inte användes för samtal befann sig vid ett visst tillfälle för en lång tid sedan, med stor sannolikhet en uppgift som de inte har enkelt åtkomlig om den ens finns. Detta vill man nu reglera explicit.

Hemlig dataavläsning: Utredaren föreslår införande av ett nytt hemligt tvångsmedel som skall ge en enorm utökning av den information myndigheterna kan komma åt om vår kommunikation. Tvångsmedlet är så anmärkningsvärt att det tas upp till separat behandling nedan.

2. Brottskatalogen utökas

Utredningen föreslår som jag redan diskuterat att åtkomst till IP-nummer i stort sett helt skall avregleras. Polisen skall helt enkelt ha en ständigt uppdaterad databas över abonnenternas IP-adresser och skall inte behöva begära ut information vid brottsmisstankar.

3. Fler får övervakas

Vid den förra utvidgningen fick man rätt att övervaka och avlyssna även abonnemang tillhörande människor som inte är misstänkta för brott men som man antog skulle komma att kontaktas av en person som är skäligen misstänkt. Nu vill man lyfta bort två ”hinder” mot myndigheternas övervakning: Kravet på att någon alls skall vara skäligen misstänkt samt kravet på att specifika abonnemang måste anges.

a) Man vill kunna använda hemlig teleövervakning, d v s komma åt information om tele- och datatrafik, utan att ha någon misstänkt person alls. Det kan exempelvis röra sig om att studera all teletrafik i anslutning till tid och plats för ett brott för att sedan lägga pussel. Man föreslår att detta skall få ske vid utredning av brott med samma straffsatser som gäller för hemlig teleavlyssning, d v s minst 2 års fängelse men med straffvärdesventil. Plus försöksbrotten.

b) Man vill också ta bort krav på att ange specifika abonnemang (teleadresser) för att få avlyssna och övervaka. Hittills har ju domstolarna givits rätt att initiera tvångsmedel

som avser speciella ”teleadresser”, (ett telefonnummer eller e-postadress t ex). Utredningens resonemang är att det nuförtiden är så svårt att veta hur folk kommunicerar och att de kan använda en sådan mängd olika telefoner, datorer eller andra ”tekniska hjälpmedel” att den begränsningen måste bort. Utredaren föreslår en lagändring som i stället ger åklagare och polis ett carte blanche att övervaka och avlyssna efter eget huvud:

> *”Det är enligt vår mening fullt tillräckligt att undersökningsledaren, efter domstolens beslut om att tillåta tvångsmedlen i förundersökningen, får avgöra utifrån vad lagstiftningen tillåter, t ex vilka identifierade enskilda telefonnummer eller e-postadresser som skall omfattas av verkställigheten. Verkställighet av tvångsmedelsbeslutet kan därefter begäras hos operatören.”*[40]

Förslaget är alltså att en domstol ger åklagaren rätt att avlyssna och övervaka en viss (skäligen misstänkt) person. Med domstolsbeslutet i handen kan åklagaren sedan kräva att man initierar avlyssning och övervakning på vilket abonnemang som helst hos en operatör. I och för sig skall regler finnas för åklagaren att följa, men det är han själv som skall se till att han följer dem och de är i vilket fall som helst vidöppna: Alla ”tekniska hjälpmedel” som den misstänkta har, har haft eller kan komma att använda, skall kunna avlyssnas och övervakas. Plus de tekniska hjälpmedel som den misstänka kan antas ha kontaktat eller kan komma att kontakta. Hela bekantskapskretsens datorer och mobiltelefoner alltså.

Men inte ens detta räcker för Bodsröms utredare: Det kan ju vara så att det finns tekniska hjälpmedel som åklagaren spontant inte kommer att tänka på eller inte vet om att han använder, men som den misstänkte ändå kanske använder på något sätt för att kommunicera. Man nämner anonyma kontantkort som ett problem här. Man föreslår därför att i definitionen av övervakning skall inkluderas uppgifter ”för identifiering av tekniska hjälpmedel” vilket man förtydligar med ”uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden”. Och denna hemliga övervakning skall få göras på ”sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från dem misstänkte”. Utredarens eget exempel är att man exemplevis vill kunna använda en speciell pejlingsapparat för att sekundsnabbt kunna samla in information om samtliga ”tekniska hjälpmedel” som finns inom ett visst geografiskt område. I princip talar man alltså om en basstationsliknande sak som kan identifiera alla påslagna mobiltelefoner runt omkring.

Men det intressanta är inte nödvändigtvis de exempel man ger eller vad ”tanken” bakom en lag påstås vara, utan vad den faktiskt ger för möjligheter. Så vitt jag kan se skulle den, så fort det finns en person som är skäligen misstänkt för ett brott som har ett minimistraff på 6 månader – eller några specifikt uppräknade brott med lägre minimistraff (dataintrång, barnpornografibrott, narkotikabrott) eller försöksbrott m m avseende dessa – kunna ge möjlighet för åklagare att begära teleövervakning hos domstol. Om domstolen inte utfärdar specifika restriktioner på hur myndigheterna får försöka

identifiera tekniska hjälpmedel, skulle dessa då kunna begära hos en internetoperatör att få kontinuerlig information om all trafik som går till eller från en mängd abonnenters datorer som man har synnerlig anledning att tro att den misstänkte kommunicerar med. Och det är alltså polisen själv som avgör om de har synnerlig anledning. Dessutom kan de förstås utföra GSM-scanningar eller scanning efter trådlösa datornät i hela kvarter etc.[41]

4. Nya maktbefogenheter för polis och åklagare

Hittills har vi en procedur som förutsätter att en domstol godkänner användning av hemliga tvångsmedel. Utredaren har dock inspirerats av *Lag (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål*, som tillkom under det kalla kriget och har speciella regler för t ex teleavlyssning när det gäller brott som har med rikets säkerhet och liknande att göra. Man föreslår nu att åklagaren – i likhet med den lagen – själv skall kunna bestämma om han vill initiera hemliga tvångsmedel, och fatta ett så kallat interimistiskt beslut. Rätten måste så fort den så kan pröva saken, men det är stor principiell skillnad. Regeringen har själv tidigare vid ett flertal tillfällen avvisat sådana förslag eftersom man tappar en viktig kontrollinstans som bör finnas i en demokratisk rättsstat. Brottsutredande myndigheter bör inte ensamma ha makten att vidta tvångsmedel mot medborgarna. Ett självständigt domstolsväsende skall anlitas för tillstånd. Exempelvis Justitieombudsmannen och Advokatsamfundet avstyrker proceduren i sina remissvar. Måste man ha snabb initiering av tvångsmedel får man omorganisera jourdomstolarna så att beslut kan ordnas den rättssäkrare vägen, hävdar de.

Man vill också kräva anpassningsskyldighet hos internetoperatörerna, alltså skyldighet att anpassa system och teknik på ett sätt som gör det lätt för polisen att avlyssna och övervaka. I princip kan Rikspolisstyrelsen kräva mycket kostsam anpassning som operatörerna måste ta alla kostnader för.

Det nya tvångsmedlet hemlig dataavläsning innebär också en utökad maktbefogenhet.

Hemlig dataavläsning

Utredningen anger två stora ”problem”: folk kan vara anonyma på nätet och de kan använda kryptering. Även om man exempelvis kan avlyssna någon är det inte säkert att man vet vem det är eller kan uppfatta vad som kommuniceras. Lösningen heter ”hemlig dataavläsning”. Det innebär att polisen hackar sig in i en dator. De kan då givetvis få tillgång till all information i datorn, men genom att placera ”trojaner” eller annan dold mjukvara i datorn kan de också exempelvis registrera varje tangenttryckning och så att säga ”spela in” allt som görs på datorn. All kommunikation blir tillgänglig och lösenord till olika sajter och krypteringar kan också registreras genom tangenttryckningarna. Advokatsamfundet noterar i sitt remissvar på SOU 2005:38 att

det väl i princip också kan låta programvaran aktivera webbkamera och mikrofon på datorn för att ta upp både ljud och bild i rummet också. Att få tillgång till någons dator i dag är att få tillgång till hela den personens liv. För att initiera tvångsmedlet skall polisen även ges möjlighet att fysiskt bryta sig in på platsen där datorn finns och installera både hård- och mjukvaror i den.

Vi förväntar oss att förslaget endast gäller oerhört grova brott, organiserade ligor och terrorister som hotar oss till livet. ”Den allra grövsta brottsligheten” som pressmeddelandet uttryckte det. Så är det inte. Tvångsmedlet föreslås få användas för brott med *lägre* straffvärde än lagen kräver för hemlig teleavlyssning. Den amerikanske doktorand i psykologi vid Uppsala universitet som bodde i samma studentkorridor som jag – och hade klätt sin garderob med aluminiumfolie, hängt en växthuslampa ovanför sina Cannabisplantor och ibland fick en liten sedel av studiekompisarna – hade kunnat komma ifråga för hemlig dataavläsning. Eller någon som är misstänkt för samma brott men kanske ”oskyldig”. Det skall även kunna användas i fall när det inte finns skäligen misstänkta. Och även polarens dator skall kunna hemligen dataavläsas om det finns synnerlig anledning att anta att den misstänkte kommer att använda sig av den.

Ett anmärkningsvärt remissvar vad gäller den hemliga dataavläsningen kom från SAMI, Svenska Artisters och Musikers Intresseorganisation, som alltså inkasserar framförandeavgifter för musik på radio, konserter, Internet m m. De anser det rimligt att polis och åklagare

> *”... på ett smidigare sätt kan få tillgång till innehållet i och uppgifterna om elektronisk kommunikation. Så vitt SAMI har kunnat tolka det nu aktuella förslaget rörande hemlig dataavläsning faller även sådana brott som upphovsrättsintrång inom ramen för de föreslagna utökade befogenheterna. Som nämnts ovan tillstyrker SAMI förslaget.”*[42]

Var det kanske detta justitiedepartementet tänkte på när man i sitt pressmeddelande hävdade att man genom att kapa enskilda människors datorer skulle bekämpa ”den allra grövsta brottsligheten”?

Men SOU 2005:38 är inte allt. Det är en utredning som bereds på justitiedepartementet för närvarande och skall resultera i lagförslag 2006/2007 tillsammans med lagförslag baserat på EU:s datalagringsdirektiv. Men två konkreta lagförslag har lagts fram våren 2006 angående hemliga tvångsmedel.

Ny princip för tvångsmedel

”Utvidgningen av tvångsmedlens användningsområde måste anses vara av stor principiell betydelse, eftersom den innebär att en person kan bli föremål för integritetsinskränkande åtgärder på grund av antaganden om avsikter som inte manifesterat sig ens i försöks- eller förberedelsebrott”. Detta är hämtat ur Lagrådets yttrande över förslaget till den proposition som ligger i riksdagen i skrivande stund, *Åtgärder för att förhindra vissa särskilt allvarliga brott*, (Prop. 2005/06:177).

Den nya principen är alltså att man skall kunna använda hemlig teleavlyssning, teleövervakning, kameraövervakning samt postkontroll *om det finns anledning att anta att en person kommer att begå* vissa allvarliga brott. Personen behöver alltså inte vara misstänkt för något brott, inte ens för förberedelse till brott.

Den här gången gäller det faktiskt riktigt allvarliga grejor och inte fildelning. Säpo har en lista inom sitt område (högmålsbrott, brott mot rikets säkerhet, allmänfarliga brott och terroristbrott). Dessutom får den vanliga polisen sätta in åtgärderna om man har anledning att anta att någon kommer att begå mord, dråp, grov misshandel, människorov eller olaga frihetsberövande om det finns anledning att anta att avsikten med dessa brott är att influera representanter för offentliga organ – såsom domare – eller den som bedriver nyhetsförmedling och journalistik. Typfallet är t ex ett MC-gäng som man kanske misstänker vill röja en åklagare ur vägen utan att egentligen ha några indikationer på det.

Jag nöjer mig med att konstatera att det handlar om att utvidga kretsen av människor som kan övervakas och avlyssnas. Nu alltså även sådana som inte är misstänkta för att ha begått ett brott eller för att försöka begå eller förbereda ett brott. I stället rör det människor som man *antar* har för avsikt att begå brott.

Just när det gäller ”systemhotande” brott, som kan underminera själva demokratin och rättsstaten, håller nog de flesta med om att man måste kunna ta i. Själva proportionalitetsprincipen indikerar ju att större integritetsintrång kan vara motiverade här – om än med rättsstatens kontroll och balanser förstås: Domstolsbeslut och andra restriktioner. Lagrådet vill dock vänta in Integritetsskyddskommittén, som slutredovisar sitt arbete den 30 mars 2007. Dessutom efterlyser man en bättre analys av om huruvida lagen är förenlig med regeringsformen och Europakonventionen.

Buggning

När detta skrivs ligger i riksdagen propositionen *Hemlig rumsavlyssning* (Prop. 2005/06:178) om ett nytt hemligt tvångsmedel: hemlig rumsavlyssning, eller buggning. Det gäller alltså att med våld bereda sig tillträde till exempelvis ett hem för att där installera tekniska anordningar som kan uppta och vidarebefordra eller lagra de samtal och ljud som förekommer i bostaden. Då buggning inte har med tele- eller internetkommunikation att göra går jag inte djupare in på det. För att få hela bilden av Bodströms gärning och drivkraft är det dock intressant.

Lagrådet påpekade att regeringen som skäl för ”buggning” anfört behov av att kunna bekämpa terrorism, spionage och författningshotande verksamhet samt organiserad och systemhotande brottslighet. Samtidigt konstaterar man – ganska häpet – att det tillämpningsområde som faktiskt föreslås i lagen *”ingalunda är begränsat till att avse dessa typer av allvarlig brottslighet”*. Vidare anser man att *”Om det ... är fråga om att allmänt utvidga polisens möjligheter att bekämpa grova brott, finner Lagrådet att förslaget inte är tillräckligt underbyggt...”*.

Lagrådet avstyrkte helt och hållet lagen, vilket inte är unikt men tämligen ovanligt och inträffar kanske ett fåtal gånger per år.[43] Ett av huvudskälen är att den förmodligen bryter mot Europakonventionens krav på rättssäkerhet, eftersom den buggade inte skulle bli underrättad efteråt om att buggning har ägt rum. Enligt konventionen måste man kunna få upprättelse om staten vidtagit åtgärder mot en som var obefogade. Här fanns ingen möjlighet för den enskilde att klaga i efterhand. Detta har påpekats av åtskilliga kommentatorer, exempelvis kriminologiprofessorn Janne Flyghed som Bodström citerades skälla ut i början av rapporten.

Lagrådet föreslår – tillsammans med många andra – att lagen skall vänta tills Integritetsskyddskommittén slutredovisar sitt arbete den 30 mars 2007. I skrivande stund ser det ut som om propositionen inte kommer att klara sig genom riksdagen. Vänsterpartiet, miljöpartiet, centern och kristdemokraterna verkar vilja kräva bordläggning. Om en lag gäller att inskränka vår grundlagsskyddade rätt till förtrolig kommunikation som slås fast i Regeringsformen 2 kap 6 §, kan en minoritet fördröja beslutet så att man skall kunna besinna sig och tänka över det hela en gång till.

En sak kritiker har fäst sig vid, bl a centerns partiordförande Maud Olofsson, är att även tidningsredaktioner skall kunna buggas. Journalistförbundets ordförande Agneta Lindblom Hultén skräder inte orden i DN:

> *”De är totalt galna! Vi har remissat på det här och uppmärksammat det på olika sätt i debatter. Buggningen innebär en uppluckring av både meddelarfriheten och källskyddet. Men det är inte allt. Det är fler lagförslag på gång i samma riktning. Det ligger mer skit i pipeline.”*[44]

Justitieministerns svar i samma artikel visar dock att han verkar ha något slags noll-vision av brottslighet i samhället, utan djupare funderingar kring att buggning (väl?) skall vara någonting som tas till i yttersta undantagsfall och att man i första hand (väl?) skall och kan utreda brott på många andra sätt som innebär mindre integritets- och rättssäkerhetsrisker:

> *”Tanken är förstås inte att man ska bugga tidningsredaktioner. Men en tidning är rätt så lätt att starta. Därför behöver vi en särskild bestämmelse. Annars skulle det kunna få till följd att människor som ägnar sig åt människohandel och bedriver en bordell bestämmer sig för att starta en tidning och kalla bordellen för tidningsredaktion för att värja sig mot buggning.”*

Överskottsinformation

Den 1 oktober 2004 utökades, som vi tidigare sett, möjligheten till hemliga tvångsmedel markant. Egentligen ville regeringen redan då införa buggning som ett nytt hemligt tvångsmedel. Lagrådet avstyrkte dock i ett mycket långt remissvar. En huvudpunkt var att man inte borde införa möjlighet för brottsutredande myndigheter att bugga innan man explicit reglerat hur de får använda överskottsinformation, d v s allt det man snappar upp genom avlyssning som inte har med det brott som utreds att göra. Man kanske får reda på att personen fildelar eller har kvar ett bankkonto i Tyskland där han jobbade för ett par år sedan och som han går in på via nätet, men inte har uppgivit för svenska skattemyndigheter. Frågan är vad myndigheterna får göra med denna information, om de får inleda nya förundersökningar,

Den 23 mars 2005 kom svaret i ett pressmeddelande från regeringen: ”Överskottsinformation ska förebygga och lösa brott” rörande den proposition man lade. Lagen började gälla 1 juli 2005 och säger i huvudsak att all överskottsinformation från hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning får användas för att utreda och förhindra brott. Förundersökning får dock inledas på grundval av informationen endast om det nu misstänkta brottet *kan ge* mer än 1 års fängelse och man kan anta att det inte bara kommer att ge böter i det aktuella fallet. *I förebyggande syfte finns ingen begränsning alls.*

Principen för polisens och åklagarmyndigheternas arbete är ju att de är förpliktigade att anmäla och utreda brott, men har frihet att underlåta att göra detta för mindre brott – av resursskäl och liknande. Att få klart vad som specifikt gäller vid hemliga tvångsmedel är dock av värde nu när deras tillåtna användning expanderas starkt och stora mängder överskottsinformation kan förväntas genereras i framtiden. Effekten kan bli stor och oväntad.

Framtiden i Bodströmsamhället

Jag skulle vilja avsluta med ett scenario som jag ser som fullt realistiskt genom att föra samman effekter från en rad olika genomförda lagar och liggande förslag från utredningar:

Antag att en person är misstänkt för försök till ett brott som ger minst 6 månaders fängelse. Antag att denna nu är medlem av en nätgemenskap, en webbaserad community som Lunarstorm eller QX, där folk kommunicerar med varandra på olika sätt, t ex via interna e-postsystem. På sajter som dessa, med tiotusentals användare, måste det givetvis finnas folk som kan vara misstänkta för brott som kan ge 6 månaders fängelse, låt säga någon som brukar sälja ett och annat piller i bekantskapskretsen. Skulle polisen kunna få utföra hemlig övervakning mot denne?

Ja, den virtuella gemenskapen torde falla under definitionen på elektroniskt kommunikationsnät enligt Rättegångsbalken. Och kommunikationen mellan användarna torde utgöra meddelanden. Så myndigheterna borde kunna kräva ut historisk information om alla meddelanden den misstänkte har skickat och tagit emot, alltså från vem, till vem och tidpunkter, samt från vilka IP-nummer han har anslutit när han var inne på communityn och kommunicerat. Dem han visar sig kommunicera med blir givetvis utsatta för samma sak, eftersom polisen har rätt att övervaka dem också. Dessutom skulle polisen kunna få ut abonnentuppgifter om alla dessa personer, som i det här fallet mycket väl kan innehålla deras ”normala” e-postadresser samt mobiltelefonnummer, eftersom man måste, eller har intresse av att uppge sådant när man ansluter sig till communityn.

Eftersom man sett att personerna kommunicerar inom communityn har man anledning att anta att de gör det utanför communityn också, och eftersom polisen inte längre behöver uppge i domstol vilka abonnemang man vill övervaka är det bara att köra vidare, d v s begära övervakning hos alla de olika operatörer som har hand om alla de e-mejladresser och telefoner som tillhör hela vänkretsen och som man har hittat på communityn. De får då ut alla gamla telefonlistor och information om e-posttrafik, och givetvis tillgång till detta framåt i tiden också. Inklusive alla positionsbestämningar enligt utredningen så att man i princip kan följa allas rörelsemönster så långt tillbaks i tiden som mobiltelebolagen har uppgifter. Ja, det är inte bara information om vem som har skickat post till vem som omfattas. Om operatören har information om annan trafik på nätet till och från den övervakade, t ex Bodströms favoriter webbsurfning och fildelning, kan de också tvingas lämna ut detta.

I dagsläget är det inte uppenbart hur mycket av den där eftersökta informationen som lagras historiskt hos operatörer av nät och tjänster. Med datalagringsdirektivet får de ett sådant tvång på sig även om det är en smula osäkert om det kommer att omfatta nätgemenskaper som exempelvis Lunarstorm, även om jag skulle tro det.

Låt nu säga att personen misstänks för ett narkotikabrott som kan ge 6 månaders fängelse (den tidigare nämnda Uppsalapsykologen till exempel). Då kan polisen få rätt att använda hemlig dataavläsning, alltså bryta sig in i personens lägenhet och installera hemliga programvaror som noterar allt som händer och sker på datorn, kopierar hela disken och vidarebefordrar till polisen.[45] De skulle även kunna bryta sig in i andras lägenheter och installera programvara om de har synnerliga skäl att anta att den misstänkte kommer att använda datorer som finns där.

Nu när den hemliga dataavläsningen är igång kommer mängder av överskottsinformation att genereras. Varje Instant Messaging och e-postmeddelande kommer att kunna läsas, varje nedladdad låt att bokföras, varje webbesök att noteras. För att förhindra brott får all överskottsinformation användas utan begränsning. Om någon av kompisarna snackar om att gå på party och ta ecstacy i helgen? Om någon säger att han skall ladda ned skitfilmen Rånarna som han hört är en total kalkon som man bara står ut med i 10 minuter? Om någon mejlar ett tips om en snickare som även en privatperson har råd med eftersom han tar pengar i handen? Om någon på chatten säger att visst, du verkar vara en skön typ att ha sex med men jag är ju student och lite pank, så om du är generös kan jag komma över i morgon? Och om överskottsinformationen gör att man misstänker att en person man fått överskottsinformationen om har gjort sig skyldig till något som i teorin kan ge 1 års fängelse men i praktiken villkorligt, ja då kan ny förundersökning startas.

Nu tror ju inte jag att ”tanken är” (för att använda en Bodströmare, det är ett av hans favorituttryck) att arbeta på det sätt jag skissat ovan. Det skulle i normalfallet inte läggas så mycket resurser på smågrejor. Så varför ifrågasätta vad som händer? Det leder oss in på riskerna med Bodströmsamhället.

Bodströmsamhälle eller robust västerländsk demokrati?

Det grundläggande perspektivet i det västerländska demokratiska samhället måste vara att staten finns till för vår skull. Medborgarna finns inte till för statens skull. Det låter möjligen märkligt att påminna om detta. Men ibland verkar det som om folk i offentliga maktpositioner tenderar att glömma det. De blir så fokuserade på att lösa sina uppgifter så effektivt som möjligt att de glömmer tjänarperspektivet. Denna poäng uttrycks redan i den första meningen i den första av Svea Rikes lagar. Regeringsformen 1 kap 1 §, 1 meningen: *”All offentlig makt i Sverige utgår från folket.”* Staten ”finns inte” och kan aldrig betraktas som en självständig aktör med en egen målsättning, frikopplad från folkviljan.

Europarådet bildades 1949 med främsta syfte att stärka mänskliga rättigheter, demokrati och rättssystem samt bevaka att medlemsstaterna uppfyller de krav man kan ställa på demokratiska rättsstater. De numera 46 medlemmarna i Europarådet har skrivit under den *Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna*, eller *Europakonventionen* som den helt enkelt brukar kallas. Europakonventionen finns inskriven i den svenska grundlagen: Regeringsformens andra kapitel handlar om grundläggande fri- och rättigheter. Enligt 2 kap 23 § får svenska lagar och föreskrifter som bryter mot Europakonventionen inte införas.

Europakonventionen är förstås ganska brett formulerad, som internationella konventioner om rättigheter ofta måste vara för att kunna undertecknas av alla. Artikel 8 ger oss Rätt till skydd för privat- och familjeliv.

1. *Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.*

Rätten är givetvis inte absolut utan får inskränkas

2. *Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.*

Om en rättighet i konventionen kränks skall man dock alltid kunna klaga på något sätt inom systemet. Artikel 13 slår fast Rätt till effektivt rättsmedel:

Var och en, vars i denna konvention angivna fri- och rättigheter kränkts, skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen utförts av någon i offentlig ställning.

Lagrådet gick så långt i sin lagrådsremiss om förslaget till lag om Hemlig rumsavlyssning att man ansåg att den inte skulle uppfylla Europakonventionens krav. Förslaget ger nämligen inte någon som helst rätt till den enskilde att i efterhand, när buggningen redan är utförd, få reda på att ett hemligt tvångsmedel har använts mot honom. Han kan därför inte klaga och rättssäkerhetskravet är inte uppfyllt.

Europakonventionen sätter den allmänna ramen (och har givetvis tolkats av Europadomstolen så att den blivit mer specifik). Men den svenska grundlagen ger mer detaljer.

Regeringsformen 2 kap:

6 § *Varje medborgare är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp även i annat fall än som avses i 4 och 5 §§. Han är därjämte skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande.* Lag (1976:871).

Detta skydd är givetvis inte heller absolut. Men man får inte hur som helst ändra på skyddet. I 11 § redogörs för hur begränsning av skyddet:

”får göras endast för att tillgodose ändamål som är godtagbart i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och ej heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsning får ej göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.”

Om regeringen trots allt lägger fram ett lagförslag som skall utöka exempelvis möjligheterna till avlyssning räcker det med att 10 riksdagsledamöter begär bordläggning för att beslutet måste skjutas fram i 12 månader. Riksdagen kan i alla fall rösta igenom förslaget direkt, men då krävs att minst 5/6 av ledamöterna röstar för, alltså 291 ledamöter av 349. En bordläggning verkar ske i buggningsutredningen. En lag som ändå instiftas i Sverige kan i slutänden prövas i Europadomstolen.

Det är lätt att tänka fel här: ”Visst, de där konventionerna är ju fina men den som inte har något att dölja, behöver inte oroa sig för övervakning, avlyssning och dataavläsning”.

Nu är ju jag av uppfattningen att i ett samhälle med allt mer omfattande morallagstiftning är det faktiskt många samhällsnyttiga, högproduktiva och allmänt goda människor som har något att dölja, även i legalt avseende. Jag tänker alltså på att man stiftar

lagar för att ”sända signaler” om vad som är acceptabelt beteende och kriminaliserar beteenden utan offer. Det kan vara fildelning, sexköp, personligt bruk av förbjudna substanser, innehav av bilder av nakna tonåringar, mindre skattebrott, svartjobb, rysk importvodka m m. Och många vill helt enkelt ”dölja” saker som inte är olagliga utan bara personliga. De där grundlagarna erkänner att vi har rätt till en privat sfär.

Men de är mycket viktigare än så. Att ge makten långtgående befogenheter att i hemlighet övervaka, avlyssna, registrera, notera allt vi gör öppnar för missbruk av makten. Vi är inte så vana att tänka i de termerna, men grundlagar finns just för att förhindra sådant och göra systemet robust över tiden.

Jag kan ta fildelningen som exempel eftersom den är viktig i Bodströms värv: om en miljon människor fildelar och inte ser något fel med det, samtidigt som man ger makten långtgående befogenheter att spionera på dem, ja då har vi givit staten ett jurdiskt medel att potentiellt komma åt politiska dissidenter eller vilka de själva vill. Kan Piratbyråns intellektuelle ideolog, samtidshistorikern och skribenten Rasmus Fleischer, i Bodströmsamhället bli betraktad som en Thomas Möller, Hells Angels förre president i Sverige? Kan hans bekanta betraktas som ingående i det kriminella gänget? Kan Piratbyråns forum bli övervakat? Piratpartiets? Kan vi som har regelbundna samtal med både Rasmus Fleischer, Piratpartiets ledare Rick Falkvinge och politiskt aktiva sexarbetare på en mejlinglista bli övervakade och avlyssnade?

Kanske finns det till och med en och annan sosse som sålt hembränt, tjuvjagat och bytt tjänster med grannen utan att betala skatt, varit sjukskriven när han inte borde, kört på grön diesel och betalat för sex. Ni sitter löst om det blir maktskifte och Bodström lämnar över Bodströmsamhällets arsenal till sina efterträdare.

Alla människor har en grå zon, och bör få ha det. Om staten via långtgående befogenheter kan få hållhakar på en stor del av folket öppnar detta för trakasserier, maktmissbruk, styrning via hot, avpollettering av motståndare via skitbrott som man snappar upp på nätet. Då får vi en situation när makten inte utgår från folket utan från Makten själv, och där åsiktsfriheten i slutänden trängs tillbaka. Tro mig! Bodströmsamhället kommer att utvecklas i en disciplinerande riktning. Folk som tror att de kan vara övervakade börjar, som Michel Foucault förstod, disciplinera sig själva. Men vi är alla olika. Vi vill inte leva exakt den typ av liv som den ständigt övervakade gör. Inger Segelström må ha sin uppfattning om ett gott liv, men alla delar den inte.

Publicisten Anders R Olsson skriver i Sydsvenskan:

> *”Av flera skäl har svenskarna ett hyfsat förtroende för offentlig förvaltning. Dessvärre spiller detta förtroende över också på de delar av polisväsendet som inte förtjänar det. … Här handlar det överhuvudtaget inte om ’personlig integritet’. Det handlar om att makt korrumperar. Och att mer makt korrumperar mer.”*[46]

Pär Ström refererar[47] den av regeringen tillsatta Säkerhetstjänstkommissionen och ger exempel på några maktmissbruk:

- Mer än 100 000 svenskar har registrerats för sina åsikters skull. Det kunde räcka med att prenumerera på en viss tidning.

- Förbudet mot åsiktsregistrering kringgicks genom att registreringen skedde i vad som kallades arbetsanteckningar.

- Både Säpo och IB buggade kända möteslokaler. ABF-huset i Stockholm hade fast installerade mikrofoner.

- Telefonavlyssning skedde i stor skala – i ett fall avlyssnades en person i tio år trots att inget misstänkt avslöjades.

Sidoinformation om andra personer som kom fram vid avlyssning lagrades i register trots att det var förbjudet. Kamouflerat som uppgifter som lämnats av påhittade personer.

I Bodströmsamhället får tusentals människor, enskilda personer, i olika statliga myndigheter medel att övervaka och trakassera oss. Det är inte Bodström själv som kommer att sitta med IP-registren. Det är enskilda poliser och åklagare, utredare och skattekontrollanter. En del är i det privata Livets Ordare, homohatare och antiporrfeminister. Bodströmsamhället vingklipper oss och hotar i slutänden demokratin genom att den ger stora friheter för Makten att komma åt precis den motståndare den vill komma åt.

Summering

Justitiekanslern (JK) skrev i sitt remissvar på SOU 2005:38 att:

> *” ... jag saknar en helhetssyn i lagstiftningsarbetet med tvångsmedel, en samlad analys av förhållandet mellan den totala verkan av tvångsmedel och annan övervakning och skyddet för den personliga integriteten. Jag framhöll därför att det finns anledning att avvakta resultatet av Integritetsskyddskommitténs arbete innan ytterligare förändringar av stor betydelse genomförs. Min uppfattning i denna fråga har förstärkts sedan jag har tagit del av förslagen i det nu remitterade delbetänkandet.”*

JK nämner också den mängd av förslag remisser, promemorior i tangerande ämnen som vräkts över dem under de senaste åren och påpekar att endast ett fåtal remissinstanser har fått alla dessa och därför knappast förstår vidden av vad som håller på att ske.

Jag hoppas ha bidragit med en genomgång som kan ge en något bättre helhetssyn på den förvirrande mängden genomförda, föreslagna och förestående lagar som justitiedepartementet under Thomas Bodströms ledning har presenterat. Det finns korskopplingar mellan lagarna som gör att det reella hotet från Bodströmsamhället framstår som klarare. När datalagring, utvidgning av hemliga tvångsmedel i alla riktningar, tillgång till IP-nummer på enkelt vis samt upphovsrättslagar rörande den digitala världen analyseras som ett paket, får vi en nation där myndigheterna har hållhakar på stora delar av folket – och legala möjligheter att använda dem. En nation som nog inte uppfyller Europakkonventionens krav på skydd för de mänskliga rättigheterna.

Jag har också givit konkreta förslag på vad som bör undersökas – och ställas till politiska bråk om – när det gäller implementeringen av EU:s datalagringsdirektiv.

Vidare har jag föreslagit att justitieminister Thomas Bodström skall granskas av KU för sitt agerande när Sverige stenhårt drev ett maximalistiskt datalagringsdirektiv i EU. Hur var denna position förankrad i Konungariket Sverige egentligen?

Svenska Journalistförbundet röt till ordentligt i sitt remissvar på SOU 2005:38:

> *”Förslagen om dessa hemliga tvångsmedel är de andra och tredje på mycket kort tid som kan innebära mycket allvarliga intrång i den personliga integriteten, som åtminstone till viss del är trendbrytande i svensk rättsbekämpning och svensk rättstradition. Det blir samtidigt omöjligt för journalister att granska verksamheten eftersom den i sig innebär sekretess över verkställighet och resultat.* ***Journalistförbundet anser att det räcker nu.*** *Man ska inte lagstifta i ursinne. En rättsstat får inte överge sina vägledande principer om rättssäkerhet, insyn och medborgarnas förtroende för rättsskipningen. Det måste*

finnas sans och måtta även när det gäller bekämpning av så allvarliga brott som terrorverksamhet." [fetstil adderad]

Glöden finns där, men även ett grundläggande fel. Det gäller ju inte terrorverksamhet, vilket jag hoppas jag visat.

Anne Ramberg, generalskreterare för Advokatsamfundet (där Bodström tidigare varit aktiv) varnar för utvecklingen under Bodström:

"En rättsstat kännetecknas av att de enskilda medborgarna har ett skydd mot statens maktutövning men det börjar vi distansera oss ifrån och då finns det anledning att se upp. Och det är förvånande att det inte föreligger större motstånd, tycker jag, ute i Riksdagen mot de här förslagen."[48]

Motstånd kan nu skönjas. En debattartikel på SvD Brännpunkt[49] i år krävde att alla förslag om vidare tvångsmedelsanvändning stoppas så att man kan invänta den så kallade Integritetsskyddskommitténs betänkande i mars 2007 innan vissa kontroversiella lagar införs. Artikeln undertecknades av riksdagsledamöter från samtliga partier – utom socialdemokraterna. Dessutom de högsta företrädarna för organisationer som Journalistförbundet, Reportrar utan gränser, Svenska Helsingforskommittén för mänskliga rättigheter, Advokater utan gränser, Svenska avdelningen av Internationella juristkommissionen, Svenska Amnesty och Föreningen grävande Journalister. Lagrådet kom med samma uppmaning i sina remisser som vi såg. Vad gäller buggningspropositionen verkar just detta hända.

Jag avslutar med ett citat från en bekant (s) som tidigare jobbade i justitiedepartementet och som jag betraktade som hyfsat liberal men här låter vara anonym. När vi i augusti 2005 började samtala om Bodströms många initiativ på området fick jag häpen lyssna till maktens språk:

"När Bodström kom till departementet hade han huvudet fullt av en massa bullshit eftersom han hade varit aktiv i Advokatsamfundet. Men vi lyckades vända honom 180 grader!"

Om departementet eller ministern är värst vet jag inte. Men här krävs politisk, medial och folklig opposition.

Noter

1. *Dagens Nyheter*, ledarsidan, 2005-10-19.

2. *Aftonbladet* 2005-10-17.

3. *Svenska Dagbladet* Brännpunkt 2006-01-21.

4. I faktapromemoria 2005/06:FPM41 från 2006-01-31 konstaterar man att det enda vi behöver göra i Sverige för att uppfylla EU-direktivet är att införa obligatorisk lagring av trafikuppgifter eftersom myndigheternas användning av sådana redan är reglerad.

5. *Svenska Dagbladet* Brännpunkt 2006-03-03, ”Lagring kartlägger boven” av Thomas Bodström.

6. *Magazin DIrekt* nr 1/2006 (Datainspektionens tidning)

7. *Svenska Dagbladet* Brännpunkt, 2006-03-03, ”Inte heller denna gång ger Bodström besked”, av Janne Flyghed och Jan Garfelt.

8. *SVT,* Aktuellt, 2006-02-02.

9. SOU 2005:38, p. 126f. ”Förbudet” gäller endast för telemeddelanden som operatören fått del av i samband med sitt tillhandahållande av ett elektroniskt kommunikationsnät eller elektronisk kommunikationstjänst samt uppgifter som angår dessa meddelanden, inklusive abonnentuppgifter, d v s de uppgifter som omfattas av tystnadsplikten enligt Lag (2003:389) om elektronisk kommunikation 6 kap. 20 §. Begreppet ”operatören” skall förstås i vid bemärkelse eftersom paragrafen gäller *alla* som tillhandahåller ”ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst”. Husrannsakan, beslag och editionsföreläggande kan dock användas mot sådan tillhandahållare för att komma åt *andra uppgifter*, ibid. p 132.

10. För längre definitioner se Appendix 1.

11. Prop 2002/03:74 bilaga 5, sid 93.

12. Prop 2002/03:74 bilaga 5, sid 98.

13. Prop. 2002/03:74 sid 36.

14. Riksåklagaren och Rikspolisstyrelsen, Hemlig teleavlyssning m m vid förundersökning avseende grova brott år 2004, 2005-09-07.

15. Referenser finns i Prop 2002/03:74, sid 21.

16. Lagrådets yttrande, utdrag ur protokoll 200-05-09, återgivet i prop. 2002/03 : 74, bilaga 5, sid 96f.

17. EU-nämndens stenografiska anteckningar 2003/04:25, 20040318.

18. EU-nämndens stenografiska anteckningar 2003/04:27, 20040326.

19. EU-nämndens stenografiska anteckningar 2003/04:29, 20040423.

20. Europeiska Unionens Råd, *Utkast till rambeslut om bevarande av uppgifter som har behandlats och lagrats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller uppgifter i allmänna kommunikationsnät för förebyggande, utredning, upptäckt och lagföring av brott och straffbara gärningar, inklusive terrorism,* Dokument nr 8958/04, 20040428.

21. Ibid, Artikel 2, punkt 3 c.

22. Dataexperter hävdar att det inte ens är möjligt att skilja på olika typer av trafik nu när många tjänster transporteras över webben: ”Med den teknik som finns är det inte möjligt att se om en viss signal på Internet är webbsurfande, e-post eller telefoni, utan att läsa innehållet, om Bodström inte tror oss kan han be någon expert förklara hur HTTPS-protokollet fungerar”, IDG.se ”Vad är det för dumheter Bodström?”, 2006-01-19.

23. EU-nämndens stenografiska anteckningar 2004/05:11, 20041126

24. Följande är hämtat från <www.eu-upplysningen.se>: ”Under Ministerrådet finns en särskild kommitté som kallas Coreper. Namnet kommer av den franska förkortningen för Ständiga representanternas kommitté (Comité des représentants permanents). Många beslut fattas i praktiken av Coreper innan de formellt bekräftas av ministrarna i Ministerrådet. Enligt rådets arbetsordning skall alla frågor som finns på dagordningen för ett ministerråd förberedas av Coreper, om inte Coreper beslutar något annat. Coreper skall också sträva efter att nå enighet inom en fråga som sedan kan antas av rådet. Varje medlemsland i EU har en ständig representation i Bryssel som förbereder Ministerrådets möten. Förberedelserna sker i Coreper, som samlar representationernas EU-ambassadörer och deras ställföreträdare. Utöver dessa deltar även sakhandläggare från representationerna, tjänstemän från representationernas samordningsgrupper och företrädare för kommissionen.”

25. Europeiska Unionens Råd, Dokument nr 15098/04, 20041123.

26. Europeiska Unionens Råd, Dokument nr 8864/1/05 REV 1, 20050524.

27. EU-nämndens stenografiska anteckningar 2004/05:42, 20050831.

28. EU-nämndens stenografiska anteckningar 2005/06:4, 20051007.

29. *Svenska Dagbladet*, ”Telefondata viktigt i kampen mot grova brott” av Thomas Bodström, 2005-12-19.

30. Justitiedepartementets egen rättssakkunnige, Christopher Démery, bekräftade detta i sitt tal på Internetdagarna i oktober 2005.

31. *Ny Teknik,* ”Musikbranschen lobbar hårt i Bryssel”, 2005-12-09, <http://www.nyteknik.se/art/43687>.

32. *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communication networks and amending Directive 2002/58/EC.*

33. Denna punkt är oklar eftersom ett av huvudmotiven bakom kravet på att operatörerna skulle tvingas lagra information om verkligt namn och fysisk adress i punkt a) och b) bakom varje abonnemang var just att ”få bukt med” anonyma konton.

34. Intervju på Oscar Swartz blogg Texplorer,
<http://swartz.typepad.com/texplorer/2005/12/datalagringen_c.html>, 2005-12-09.

35. Artikel 29-gruppen för skydd av personuppgifter, Yttrande/Opinion. dok nr 1868/05/SV WP113, 2005-10-21 samt dok nr 654/06/EN WP119, 2006-03-25.

36. Europeiska ekonomiska och sociala kommittén, Yttrande/Opinion TEN/230 2006-01-19 samt *Official Journal of the European Union,* C 69/16, 2006-01-23.

37. *Dagens Nyheter,* "Polisen ska inte jaga tonåringar som laddar ner", 17 mars 2005.

38. Post- och Telestyrelsen, Yttrande över SOU 2005:38, Dnr 05-1103, 21 december 2005,

39. Justitiedepartementet pressmeddelande: Tillgång till elektronisk kommunikation i brottsutredningar, 2005-05-24.

40. SOU 2005:38 sid 199.

41. Det är inte omöjligt att just detta redan sker. Thomas Bodström har ett antal gånger sagt att SOU 2005:38 bland annat handlar om att lagreglera sådant som polisen redan ägnar sig åt. Man skulle ju kunna spekulera i att det i sådana fall rör sig om metoder som inte kräver någon annans medverkan, till exempel operatörernas. Att använda en GSM-scanner, vilket varje innehavare av en sådan apparat kan göra, är dock något ganska annorlunda än att med statens makt bakom sig tvinga en operatör att lämna ut information om enskilda människors internetkommunikation för att man tror att de kanske kommunicerar med någon annan. Så även om polisen skulle utföra sådana pejlingar i dag kommer lagförslaget att utöka deras möjligheter rejält och utsträckas till helt nya områden. Man bör kanske även notera att avlyssning av trådlös kommunikation inte ens är ett brott i dag även om ett sådant förslag ligger på remissnivå, Ds 2005:6, *Brott och brottsutredningar i IT-miljö.*

42. Telefonsamtal 2006-05-03 med f d justitierådet Hans Danelius, ordförande i det Lagråd som yttrade sig över förslaget till lag om hemlig rumsavlyssning. Justitierådet och lagrådsledamoten Leif Thorsson hävdade samma sak i personligt samtal 2006-05-16.

43. SAMI, 8 dec 2005. Yttrande över SOU 2005:38.

44. *Dagens Nyheter,* "Polisen kan få bugga läkarmottagningar", 2006-02-10.

45. Det paradoxala är att myndigheterna inte skulle ha rätt att avlyssna kommunikation vid så lågt straffvärde vid misstanke om narkotika- eller barnpornografibrott. Men de skulle ha rätt att utföra hemlig dataavläsning.

46. sydsvenskan.se, Kultur, 27 feb 2006, "Anders R Olsson om hotad integritet".

47. *Aftonbladet* 2006-02-20, "Ska staten få veta allt?"

48. *SVT* Aktuellt 2006-02-02.

49. *SvD* Brännpunkt 2006-02-14 "Privatlivet först av allt".

Appendix I

Här följer korta definitioner av en del termer som återkommer i rapporten. Jag använder inte de formella legala definitionerna som givetvis är formulerade på juristsvenska Men det blir enklare att tänka i konkreta vardagliga termer.

Hemlig

Hemlig i det här sammanhanget innebär att myndigheterna agerar utan att personen är medveten om det (d v s övervakar personer och skaffar sig information om deras kommunikation och beteende utan att meddela personen). En del av den aktuella informationen kan ju myndigheterna även få fram genom icke-hemliga tvångsmedel. Exempelvis genom en husrannsakan där man beslagtar en dator och läser igenom e-posten i datorn. Med ett hemligt tvångsmedel vet alltså inte individen att hans e-post kanske har lästs och kontinuerligt läses av polisen.

Hemlig (tele)övervakning

Uppgifter inhämtas i hemlighet om telemeddelanden (t ex telefonsamtal och internettrafik). Sedan den 1 oktober 2004 ingår även historisk kommunikation. Det rör alltså information om själva meddelandena, inte innehållet i dem. Man kan tänka i termer av ”vilket telefonnummer ringde till vilket nummer vid en viss tidpunkt”. Eller ”vilken dator användes för att skicka ett mejl vid en viss tidpunkt” eller ”vilken dator besökte denna webbsajt och fyllde i ett formulär vid en viss tidpunkt”. Det kan röra sig både om att gräva upp historiska data och om ett faktiskt få information om i stunden pågående trafik.

Hemlig (tele)avlyssning

Själva meddelandena avläses i hemlighet. Sedan den 1 oktober 2004 ingår även historisk kommunikation. Det kan alltså röra sig om att rent faktiskt lyssna på ett telefonsamtal eller spana på pågående internetkommunikation men även att få tillgång till exempelvis lagrade röstmeddelanden och e-postbrevlådor.

Hemlig dataavläsning

Allt som händer på en dator registreras genom att man i hemlighet installerat programvaror för syftet. Varje tangenttryckning och all information på datorn kan registreras och sändas till polisen via Internet. Polisen kan även bryta sig in fysiskt i loka-

len/lägenheten där datorn finns för att installera antingen program- eller hårdvaror i den för att senare bryta sig in igen och tömma den på dessa inklusive den information som sparats.

Hemlig rumsavlyssning (= ”buggning”)

Mikrofoner installeras så att samtal och ljud i rummet kan registreras och sparas eller lyssnas till i realtid.

Hemlig kameraövervakning och hemlig postkontroll

Definition bör framgå av begreppen.

Åtkomst av abonnentuppgifter

Notera att hemlig teleövervakning och teleavlyssning kan utföras utan att man vet *vem* som kommunicerar. Man vill givetvis kunna koppla ihop kommunikationen med en viss person. Detta gör man främst genom abonnentuppgifter, d v s information om vem som innehar abonnemanget för ett visst telefonnummer. I internetvärlden tilldelas man en IP-adress (en fyrställig kombination av upp till 12 siffror) av sin internetleverantör. Denna adress kan vara tillfällig och bytas ganska ofta och man behöver själv inte bry sig om vilken den är. Leverantören kan dock i princip se vilken abonnent som tilldelades en viss IP-adress vid en viss tidpunkt. SOU 2005:38 anser att detta är abonnentuppgift. PTS ansåg det tidigare men har nu ändrat sig.

Datalagring

I princip all elektronisk kommunikation är digital i dag, åtminstone under någon del av sin ”färd”. All vår kommunikation passerar som bitar genom tele- och internetoperatörernas kraftfulla växlar och routrar. I princip skulle varje ord vi yttrar via mobiltelefon, varje bild vi studerar på nätet och varje sökning vi gör – ja all vår kommunikation – kunna lagras av operatörerna. För att historisk teleavlyssning och teleövervakning skall vara möjlig på ett systematiskt vis måste polisen ha tillgång till lagrade data av något slag. Datalagring handlar alltså om hur man skall reglera vem som måste lagra vilken information och hur länge.

Trafikdata

I princip den information myndigheten kan ha rätt att komma åt via hemlig teleövervakning, d v s information om trafiken (kommunikationen) men inte innehållet i den.

(Hemlig) frysning av elektronisk kommunikation

Delvis ett lindrigare alternativ till datalagring där trafikuppgifter, men även meddelanden genom ett snabbförfarande beordras sparas av operatören, redan innan en domstol hunnit initiera hemlig teleövervakning eller hemlig teleavlyssning. Ett nytt tvångsmedel som föreslagits i Departementspromemoria Ds 2005:6.

Appendix II

Kronologisk översikt över införda eller föreslagna lagar som har med hemliga tvångsmedel att göra samt deras huvudsakliga innehåll

PRESSMEDDELANDE 2003-05-22

”Offentliga ombud införs i ärenden om hemlig teleavlyssning”

Propositionens titel: Prop 2002/03:74 2003-05-22

”Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering m m”

Lagar började gälla: 1 oktober 2004

1) Avlyssning och övervakning av *historisk kommunikation* (d v s sådant som redan skett) blir möjlig även med hjälp av Rättegångsbalkens regler, inte endast enligt Lag om elektronisk kommunikation.

2) Straffgränserna för fall där polisen får använda hemlig teleövervakning, hemlig teleavlyssning och hemlig kameraövervakning sänks genom att s k straffvärdesventiler införs.

3) Nya brott som inte betraktas som så grova att man normalt skulle få tillgripa hemlig teleövervakning listas explicit så att åtgärden skall kunna tillgripas även för dem.

4) Möjlighet införs att använda hemlig teleövervakning och hemlig teleavlyssning på abonnemang som inte tillhör den misstänkte men som denne kan antas komma att kontakta.

5) Hemlig kameraövervakning skall få ske även om någon skäligen misstänkt för brott inte finns.

6) Offentliga ombud skall bevaka integritetsintressen för den enskilde när domstol prövar om hemlig teleövervakning eller hemlig teleavlyssning skall få ske. Regeringen utser ombuden.

PRESSMEDDELANDE 2005-04-01

Nya samarbetsformer i den internationella brottsbekämpningen

Prop. 2004/05:144 2005-03-31

Internationell rättslig hjälp i brottmål: Tillträde till 2000 års EU-konvention m m

Lagar började gälla: 1 juli 2005

1) Enklare förfaranden för att svensk polis skall hjälpa utländsk polis att bedriva hemlig teleavlyssning och hemlig teleövervakning i Sverige.

2) Ny form av rättslig hjälp till andra länder införs: Tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning.

3) Ny form av rättslig hjälp till andra länder införs: Tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning.

PRESSMEDDELANDE 2005-03-23

Överskottsinformation ska förebygga och lösa brott

Prop 2004/05:143 2005-03-23

Överskottsinformation vid användning av hemliga tvångsmedel m m

Lagar började gälla: 1 juli 2005:

1) Uppgifter som kommer fram i samband med hemlig teleövervakning, hemlig teleavlyssning och hemlig kameraövervakning skall få användas för att inleda förundersökning för andra brott än det som skulle utredas från början.

2) Uppgifter som kommer fram skall utan begränsningar få användas för att förhindra brott av varje slag.

PRESSMEDDELANDE 2006-02-09

Polisens möjlighet att förhindra allvarliga brott ökar

Prop 2005/06:177, 20060316

Åtgärder för att förhindra vissa särskilt allvarliga brott

Lagar börjar gälla: 1 juli 2006

1) Hemlig teleövervakning, hemlig teleavlyssning, hemlig kameraövervakning samt hemlig postkontroll skall kunna användas mot person som man har anledning anta kan komma att begå vissa allvarliga brott, dock utan att misstanken behöver ha manifesterats i försöks- eller förberedelsebrott.

PRESSMEDDELANDE 2006-02-09

Buggning införs för att bekämpa de allra allvarligaste brotten

Prop 2005/06:178, 20060316

Hemlig rumsavlyssning

Lagar skulle börja gälla: 1 juli 2006 (blockerade av kd, c, mp, och v i riksdagen den 31 maj).)

1) Nytt hemligt tvångsmedel införs: Hemlig rumsavlyssning

PRESSMEDDELANDE 2005-03-24

SOU 2005:38

Tillgång till elektronisk information i brottsutredningar

1) Hemlig teleavlyssning och hemlig teleövervakning regleras endast av Rättegångsbalken, d v s de tas bort ur Lag om elektronisk kommunikation.

2) Hemlig avlyssning och hemlig övervakning skall få användas även om ingen misstänkt person finns.

3) Polisen skall ej längre behöva ange vilket specifikt abonnemang som skall övervakas eller avlyssnas.

4) Domstol skall ej behöva anlitas innan beslut om hemlig övervakning och avlyssning tas.

5) Övervakning utvidgas till att omfatta pejling/lokalisering av exempelvis trådlösa kommunikationsinstrument.

6) Övervakning skall kunna ske av all kommunikationsutrustning som kan komma att användas för att sända eller ta emot meddelanden till eller från en misstänkt person, d v s även andra personers utrustning.

7) Polisen får direkt tillgång till hemliga telefonnummer utan att behöva gå via operatörerna.

8) Polisen får tillgång till ett ständigt uppdaterat register över vem som tilldelats ett visst IP-nummer på Internet vid en viss tidpunkt medan de i dag under vissa villkor kan begära ut dessa från operatörerna.

9) Straffsatsen för att få använda IP-nummer i brottsutredningar sänks kraftigt så att alla brott inkluderas.

10) Nytt hemligt tvångsmedel införs: Hemlig dataavläsning, vilket innebär att polisen i hemlighet kan installera programvaror och hårdvaror i datorer för att registrera allt som försiggår i dem.

11) Internetleverantörer blir skyldiga att anpassa sin tekniska utrustning för att underlätta polisens avlyssning och övervakning (endast teleoperatörer behöver göra detta i dag).

Datalagringsdirektivet

från EU torde lagtekniskt handla om att införa en obligatorisk datalagring med syfte att utvidga tvångsmedlet hemlig teleövervakning på ett mycket långtgående vis.

1) Operatörer skall tvingas lagra uppgifter om kundernas kommunikation så att

    a) För varje telefonsamtal skall lagras en mängd uppgifter som kan identifiera namn och adress på uppringare och uppringd för varje telefonsamtal, likväl som vilken utrustning som användes och var de befinner sig (vid mobiltelefoni).

    b) För varje accesskoppling mot Internet skall lagras namn och adress på abonnenten, det IP-nummer denne fått sig tilldelad vid uppkopplingen samt identifiering av den fysiska ändpunkt som uppkopplingen skett från (DSL-linje, telefonnummer vid uppringd access etc).

    c) För varje e-post-meddelande som skickas eller IP-telefonisamtal som utföres skall lagras namn och adress på sändare och mottagare plus de uppgifter som finns under b).

2) Polisen skall ges tillgång till denna data för att upptäcka, undersöka och lagföra brott med frihet för medlemsstaterna att själva besluta vilka brott det gäller.

Brott och brottsutredning i IT-miljö

Departmentspromemoria (Justitiedepartementet Ds 2005:6), *Brott och brottsutredning i IT-miljö*, förordar ratificering av Europarådets konvention om brott i cyberrymden (Convention on Cybercrime, European Treaty Series 185, Budapest 2001-11-21) och föreslår i anslutning till detta bl a följande lagändringar. Översikten har utförts parallellt med annat lagstiftningsarbete och delar av konventionen blir sannolikt uppfyllda.

1) Nytt hemligt tvångsmedel införes: Frysning av elektronisk kommunikation. Detta skall kunna beslutas av åklagare själv utan att gå till domstol.

2) Förbud mot rubbande av bevisning i elektronisk form införes.

3) Husrannsakan via elektroniska kommunikationsnät införes som nytt tvångsmedel.

4) Tvångsmedlet kvarhållande av elektronisk post införes.

5) Hemlig teleövervakning och hemlig teleavlyssning skall bli möjlig även på vissa kommunikationsnät där det ej var tillåtet tidigare.

6) Operatörer skall tvingas röja utökade trafikuppgifter angående enskilda meddelanden.

Försvarsdepartementet DS 2005:30

En anpassad försvarsunderrättelseverksamhet

Försvarets Radioanstalt, som hittills endast signalspanat på eterburen kommunikation (d v s trådlös, i luften).

1) Signalspaning skall få ske även på trådbunden kommunikation (telefoni och Internet) som korsar landets gränser

2) Trådägande operatörer skall förpliktigas ”leda av” en kopia av den dataström som passerar Sveriges gränser till en samverkanspunkt som bestäms av myndighet.

3) Vid denna samverkanspunkt får FRA rätt att på automatiserat vis gå igenom all trafik och applicera vissa sökbegrepp. Generaldirektören för FRA bestämmer vid varje tidpunkt vilka sökbegreppen skall vara men rapporterar detta till Försvarets underrättelsenämnd, som skall granska verksamheten.