

Storebror har blivit automatisk och digital

| av Pär Ström

Vi lämnar allt fler elektroniska spår i vardagslivet. Och staten är inte sen att samla upp dem. Men ett politiskt program i 7 punkter kan stoppa den tysta marschen in i det automatiserade övervakningssamhället.

UNDER SOMMAR-OS i Aten ska en programvara automatiskt läsa igenom epostmeddelanden i jakt på något suspekt. Vidare vill EU göra det obligatoriskt för teleoperatörer i alla EU-länder att under upp till tre års tid spara information om sådant som vilka webbplatser människor besöker och vilka de ringer. I England byggs ett system av kameror längs vägnätet som ska läsa in passerande bilers registreringsnummer och genomföra automatiska kontroller i realtid.

Kära 2000-talsmedborgare – välkommen till övervakningssamhället! Jag hoppas att de nya åtgärderna från ordningsmakt och andra myndigheter gör att du känner dig trygg och skyddad från all ondska. För det är naturligtvis för ditt eget bästa som dina elektroniska fotspår från vardagen börjar samlas in, analyseras och användas för övervakning och kontroller. Och du som har rent mjöl i påsen har naturligtvis inget att frukta. Eller hur?

Ett samhälle kan välja att lägga sig någonstans längs en skala mellan två ändpunkter. Den ena ändpunkten är anarki (total frihet helt utan kontroll), den andra är polisstaten (allt övervakat in i minsta detalj). Nästan alla människor anser nog att båda ändpunkterna är tämligen motbjudande – alltså ska vi ligga någonstans mellan dem. Så är det också i demokratiska länder som Sverige. Vi ligger sedan länge någonstans på mitten av skalan.

Men på senare tid har vi börjat röra oss i riktning åt polisstaten. Det är en global utveckling som även omfattar Sverige.

HELTÄCKANDE ÖVERVAKNING

Varför har det blivit så här? Vad kommer det att leda till? Vilka för- och nackdelar har snokarsamhället? Vilka poli-

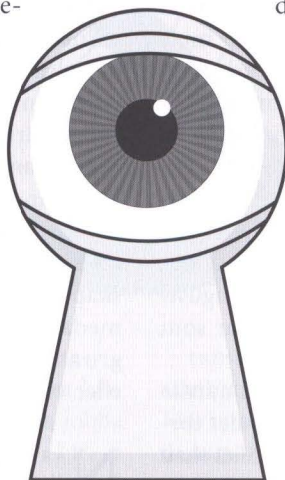
tiska åtgärder bör vidtas? Låt oss börja med vad som gör det hela möjligt: Den tekniska utvecklingen med den digitala revolutionen i spetsen.

I gårdagens "analog" värld, där information fanns på papper, var det svårt, tidskrävande och dyrt att samla in uppgifter om människors göranden och låtanden. I dagens digitala värld, däremot, lämnar vi av bara farten efter oss stora mängder elektroniska fotspår som det är förhållandevis lätt och billigt att samla in och bearbeta.

Ibland är skillnaden extrem. I dagens digitala samhälle kan polisen hos internetleverantörer installera en programvara som automatiskt sätter upp alla som besöker barnpornografiska webbplatser på en lista. En hel befolkning kan övervakas automatiskt, och brottslingarna kan snärjas, omedelbart och med kirurgisk precision. Hur skulle man i den gamla världen, där det kontroversiella materialet främst fanns i tidskrifter, ha kunnat åstadkomma motsvarande kontroll? Med en polisman i varje svenskt vardagsrum?

Den digitala revolutionen medför att allt fler system och produkter i vardagen är elektroniska, "intelligenta" och försedda med en möjlighet att kommunicera med omvärlden (så kallad datakommunikation). Det är en utveckling som bara har börjat. Vi kommer att få kylskåp, stereoapparater, oljepannor, hissar, leksaker, TV-apparater och mycket annat med inbyggd datakommunikation.

Redan idag, 2004, lämnar vi elektroniska fotspår efter oss exempelvis när vi handlar, lånar på biblioteket, hyr en video, parkerar i P-hus (ibland), ringer, mailar, surfar, passerar in på jobbet och ser på TV (gäller digital, interaktiv TV). Det finns nöjesparker och färjor där man får tillträde genom att trycka sitt finger mot en fingeravtrycksläsare (då uppstår fotspår). I Storbritannien finns redan bevak-



statlig. Mått björta finns kvar i solex. Alpha och jag känner som nu intressen i distrikt. Verksamheten ska stoppas vi igen i en ny fas med nya pro-

Digitalboxen skvallrar på dig

Statligt bolag ska sälja uppgifter om surfvanor

Margaret von Platen

Statliga Teracom, vars finanser urgröpts av miljardinvesteringen i det nya digitala TV-nätet, arbetar nu febrilt på att hitta nya intäktskällor. Teracom ska sälja information om tittarna till hushålls spekulanter.

Det är ovanligt för ett statligt bolag att sälja data kommersiellt. Information. Boxer har redan reklamutbud och olika innehållsleverantörer på sin portal, som bland annat innehåller informationstjänster. Boxer kan registrera tittarna varje gång de besöker reklamutbud, och även registrera vilka innehållstjänster de besöker via

med drygt 3 000 kronor. Den kostar knappt 2 000 kronor. Men vi måste också tjäna pengar. Kunden skriver på ett avtal med oss om att bland annat betala räkningskostnader för att se tv. Vi kan till exempel utifrån kundregistret sälja adresser. Vi kan registrera varje gång tittaren besöker en sida. Denna information kan vi sälja vidare. Vi ska eventuellt utnyttja denna information", säger Katariina Forsberg, informationsansvarig på Boxer.

Boxer har i dag drygt 80 000 kunder. Drygt 50 000 har en box som hanterar Boxers portal, det vill säga att boxen har ett inbyggt modem med en webbläsare.

"Hotar integriteten"

Den moderata riksdagsmannen Ola Karlsson har lagt en motion om detta med titeln "Personlig in-

"Bolaget kommer att kunna sälja uppgifter om tittaren har besökt en porsida, ett politiskt parti eller information om graviditetstest. Jag tycker inte att ett statligt bolag ska ägna sig åt sådant. Kulturförvaltningen utövar statens turdepoteringar inte ska ägna sig åt sådant. Teracom eller av Teracom delägda bolag", säger Ola Karlsson.

700 Mkr kvar

Teracom har kvar 700 Mkr av en kreditlinje om 1,8 miljarder kronor. Med nuvarande takt på investeringarna tar pengarna snart slut.

"Det stämmer att om vi fortsätter med investeringar om 460 Mkr per halvår så är pengarna snart slut. Men det är en hypotetisk fråga. Vi har gjort en medveten investering utifrån att det inte kommer att bli ett problem att finansiera investeringarna", säger Ola Karlsson.

KRITIKER: Den moderata riksdagsmannen Ola Karlsson vill att statligt bolag ska sälja uppgifter om kundna.

2002-2003. I kassalöset i kapitaltillskott från så säger Capet Tamm, finans Teracom.

Freedom looks fragile when banks ask for thumbprints

Americans are taking to the streets in protest over homeland security moves, reports Susan Mazur



While the first confirmed police officers at the New York event conducted their duties professionally, they also saw police suspended troops. Back to the future, the previous Class action lawsuit and criminal complaints are likely to follow, says Yale professor David Graeber, who was detained for 14 hours last week in protest, and filed a lawsuit for "failure to obey."

Greater: The federal security forces are becoming more and more aggressive in their actions against the protesters. The federal security forces are becoming more and more aggressive in their actions against the protesters. The federal security forces are becoming more and more aggressive in their actions against the protesters.

ningskameror på gator och torg med inbyggd automatisk ansiktsgenkänning. Inom ett fåtal år kommer vi förmodligen också att lämna fotspår efter oss när vi kör bil (bland annat via biltullar och "telematik" i bilarna), åker med kollektivtrafik (via smarta kort), och kanske till och med när vi lyssnar på musik (via upphovsrättsskyddande system såsom det planerade Palladium).

BILTULLARNAS

Stockholms kommande biltullar skall, av pressuppgifter att döma, utformas så att bilars unika identitet läses in vid varje passage. Syftet är förvisso bara att ta betalt, inte att genomföra några kontroller – men enligt principen om ändamålsglidning är det stor risk för en ändrad inställning på den punkten. När systemet väl är på plats är det ju frestande att börja använda det också för andra syften än vad som var tänkt från början.

Det skulle exempelvis inte vara något större ingrepp att komplettera biltullsystemet så att varje bils genomsnittshastighet mellan två passager automatiskt beräknas. Informationen skulle kunna användas för automatisk fartövervakning. Ännu lättare skulle det vara att matcha passerande bilars registreringsnummer mot en databas med oskattade, oförsäkrade eller obesiktigade bilar, liksom bilar ägda av efterlysta personer. Vidare skulle det vara relativt enkelt att samköra de bilnummer som passerar ofta och på regelbundna tider med registren över personer som uppbär A-kassa eller sjukpenning, för att hitta dem som kan misstänkas för bidragsfusk.

Min tro att en sådan utveckling inte bara är möjlig, utan sannolik, stärks av allt det som sker i Storbritannien. För det första har Londons nya biltullar redan börjat användas för övervakning, genom att passerande bilars registreringsnummer matchas mot en databas med fordon som polisen är intresserad av. Det finns även digitala kameror vid tullstationerna som kan ta närbilder av intressanta bilförare och passagerare.

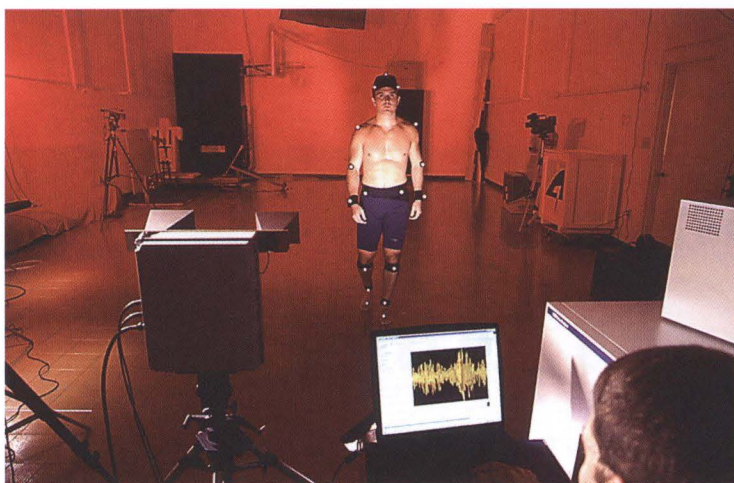
För det andra använder 23 poliskåre i England och Wales sedan förra året ett system med kameror längs vägarna (alltså inte bara i städerna) som läser in passerande bilars registreringsnummer. Numren matchas i realtid mot ett flertal databaser, och om en bil visar sig intressant går larmet på ledningscentralen och en polisbil rycker ut. Polismännens produktivitet, mätt i antal gripanden per person och år, har mer än tiodubblats. Förmodligen kommer systemet, kallat "Automatic Number Plate Recognition", att utökas till att täcka hela Storbritanniens vägnät. Den uttalade målsättningen är att "göra vägnätet oåtkomligt för brottslingar".

För det tredje finns funderingar på att förse bilar i Storbritannien med en elektronisk krets, ett så kallat spionchip, som kommunicerar trådlöst med stolpar längs vägnätet. Chipet ska bli en digital angivare, som rapporterar exempelvis fortkörning, körning mot enkelriktat och körning med oskattad bil.

Sträcker man sig den lilla biten över sundet till Irland kan man notera uppbyggnaden av ett system med elektronik i bilar som vid en krock omedelbart sänder den senaste tidens kördata (såsom fart och hantering av ratt, broms, blinkers etc) via mobiltelefonnätet till polisen och försäkringsbolaget. Bilföraren anses uppenbarligen inte ha äganderätten till denna information. Och i Frankrike har man testat användning av satellitnavigering i kombination med trådlös datakommunikation ("telematik") för att på distans automatiskt stänga av bränsletillförseln på bilar som överskrider hastighetsbegränsningen.

TERROR OCH EKONOMI DRIVER PÅ

Alltså: Information, i vid bemärkelse, är i allt större utsträckning digital, och det byggs en infrastruktur i samhället som samlar in människors elektroniska fotspår i vardagen. Därmed håller vi på att lägga den tekniska grunden för att möjliggöra glidningen åt polisstatshället. Men vilka krafter är det som driver på?



Svar: Terrorism och budgetnedskärningar. Den väldiga rädslan för terrorismen i kombination med den breda uppslutningen för kraftfulla åtgärder har skapat ett mentalt klimat i hela västvärlden, mest i USA men i ökande utsträckning även i Europa, där begrepp som rättssäkerhet, personlig integritet och mänskliga rättigheter mest uppfattas som hinder för en effektiv terroristbekämpning.

Samtidigt är det billigare att låta programvaror sköta kontroll och övervakning än att låta människor göra det. De flesta andra samhällssektorer är ju sedan ganska länge inne i en radikal förändring av sitt arbetssätt med anledning av den digitala revolutionen, ofta med tydliga effektivitetsvinster som följd, så varför skulle inte även polisen få surfa på denna våg?

I allt större kretsar inom polisväsendet runtom vårt klot talar man om "automated law enforcement" som framtidens melodi – automatiskt polisarbete baserat på avancerade övervaknings- och kontrollsystem, kanske till och med kompletterat med automatiska "domstolar". Sätt till exempel satellitnavigering och datakommunikation på alla bilar (det får vi snart ändå), låt en centraldator följa deras framfart och automatiskt skriva ut böter så snart hastighetsgränsen överskrids med 1 km/h. Böterna kan med fördel dras direkt från medborgarens bankkonto via autogiro samma dag så slipper man administrativa kostnader. Traditionella fartkontroller blir överflödiga.

Eftersom digital övervakning och kontroll medför väsentliga besparingsmöjligheter inleddes marschen in i övervakningssamhället långt före den 11 september 2001. Terrordåden har egentligen bara accelererat en utveckling som redan förelåg. Besparingspotentialen gör det också sannolikt att trenden mot ökad övervakning skulle fortsätta även om dagens akuta terrorishot skulle klinga av.

Ibland kommer besparingarna även medborgarna tillgodo, ekonomiskt eller i form av inbesparad möda. Detta bidrar till att minska medborgarnas vilja att skydda sin personliga integritet.

Vart är utvecklingen på väg? Det framstår som högst

sannolikt att inskränkningarna av den personliga integriteten kommer att fortsätta i accelererande tempo. I bästa fall går vi därför mot en kraftmätning mellan å ena sidan stat och myndigheter, som har diverse goda syften för att registrera och övervaka människor, och den del av befolkningen som känner obehag och ser faror i detta. I värsta fall är det ingen som bryr sig, ingen debatt uppstår och förskjutningen åt polisstatshållet fortsätter i det tysta.

Nu kanske någon läsare invänder: "Men den som har rent mjöl i påsen har väl inget att frukta? Den personliga informationen är ju inlåst och ingen obehörig kommer åt den."

I en perfekt värld är invändningen i stort sett korrekt (med undantag för den känslomässiga sidan av det hela). I den verkliga världen finns däremot risker med digital övervakning även för "vanliga människor". Jag ser två huvudrisker: Att dåligt underbyggda svartlistningar skapar problem för oskyldiga, och att känslig personlig information kommer i orätta händer.

SVARTLISTNINGAR UTANFÖR RÄTTSSYSTEMET

När exempelvis mönsterigenkännande programvaror går igenom email- och telefontrafik i jakten på något suspekt, hur hanteras resultatet? Sannolikheten är mycket stor för att en lista upprättas med namn på misstänkta personer, och att denna lista sedan används som underlag för olika former av säkerhetsåtgärder. Sådana listor lär också utväxlas mellan olika myndigheter och mellan olika länders säkerhetstjänster, och därmed snabbt spridas.

Eftersom det är programvaror som gör automatiska bedömningar är det oundvikligt att en hel del oskyldiga hamnar på en sådan lista, kanske till och med högt upp på den. Alla automatiska system besväras av två slags felindikeringar: Dels så kallade "false positives" (systemet bedömer något ofarligt som ett hot), dels så kallade "false negatives" (systemet missar ett reellt hot). Det är "false positives" som utgör ett hot mot människors personliga integritet.

Innehåll i polisregister såldes

Nu fälls en polis för dataintrång, tjänstefel och brott mot tystnadsplikten.

Polisen hade sålt sekretessbelagda uppgifter om anställda i stora svenska företag.

En fälls han för dataintrång, tjänstefel och brott mot tystnadsplikten. Påföljden: villkorslöst dom och 3 000 kronor böter.

Under förra året i höstas hade åklagare Roy Engblom fått en 32-årig polis att döma för att ha lämnat ut sekretessbelagda uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag. Enligt domstolens beslut hade polisen lämnat ut uppgifter om anställda i stora svenska företag.

Vi ä
allt
imp
köt



komma i orätta händer – och det är en väsentlig skillnad. Det finns fyra sätt på vilka den faktiskt kan spridas till obehöriga:

För det första har vi den mänskliga faktorn. Exempelvis dömdes en polisman i Stockholm i höstas för att ha sålt sökningar i det sekretessbelagda kriminalregistret till företagsledningen på Coop.

För det andra finns risken att så kallade hackers, externa eller interna, bryter sig in i systemen och kommer åt sekretessbelagd information. Verkligheten uppvisar ett pärlband av exempel på att så har skett.

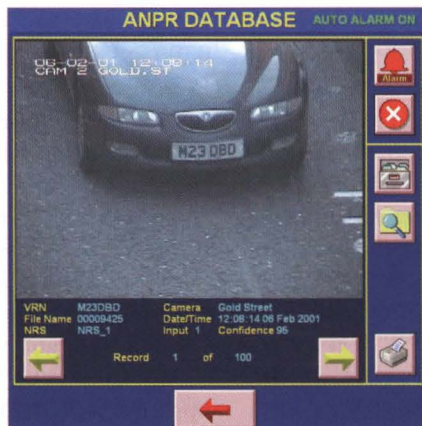
För det tredje finns risken att system och programvaror innehåller buggar som åtminstone tillfälligt öppnar de digitala dörrarna på vid gavel. Även detta har skett gång på gång.

För det fjärde kan bristfälliga regler för informationshanteringen sätta den personliga integriteten i fara. Nyligen lyckades exempelvis en man i Oslo, som förföljde och spionerade på sin före detta fru, få ut information från stadens biltullar om exakt var och när hon kört med sin bil. Han bara ringde och frågade.

Jag kontrollerade saken och fick veta att förfarandet var helt i enlighet med rutinerna (som dock ändrats efter att ärendet togs upp i Stortinget).

Möjligheten att personlig information slinker iväg åt fel håll är inte försumbar, den är högst realistisk, och det behövs inte särskilt mycket fantasi för att inse att konsekvenserna för individen i vissa fall kan bli stora. Elektroniska fotspår kan exempelvis avslöja sådant som amorösa snedsteg, ekonomiska problem, nattliga besök på dubiösa gator, spelberoende, sexuella vanor, kontroversiella åsikter, hälsoproblem, extraknäck som inte uppskattas av arbetsgivaren, och mycket annat.

Därtill kommer förstas den rent känslomässiga aspekten, det blotta obehaget av att vara övervakad, även om



INFORMATION MED VINGAR

Digital information har "vingar" – den har en vidunderlig förmåga att sprida sig och hamna på oväntade platser. Digital information drar också till sig intresserade som en öppen syltburk drar till sig getingar. När beslutsfattare och de tekniskt ansvariga för systemarkitekturen försäkrar oss om att insamlad personlig information inte kan komma i orätta händer så tänjer de på sanningen. Det korrekta är att informationen normalt inte ska

informationen förblir inlåst. Våra känslor är inte irrelevanta, även om det finns en stark tendens att behandla dem så (till exempel genom att hävda att om man bara är hederlig så bör man inte ha något att dölja). Rätten att bli lämnad ifred hör till de grundläggande mänskliga rättigheterna.

ANPASSLIGHET OCH ÄNDAMÅLSGLIDNING

Vi riskerar också att få ett samhälle där människor väljer anpasslighetens väg istället för att ta risken att hamna på någon svart lista. Morgondagens människa kanske drar sig för att besöka vissa webbplatser, köpa vissa böcker, ringa vissa personer och så vidare. Förutom att detta minskar våra referensramar och därmed skapar fördumning kan det bli en fara för demokratin, eftersom det hämmar informationsinhämtning och opinionsbildning.

Man måste också väga in risken för ändamålsglidning. Verkligheten visar att denna risk är stor. När det så kallade PKU-registret med blodprover från svenska barn användes av polisen i Anna Lindh-mordet var det ett exempel på ändamålsglidning. Detsamma gäller när de nya biltullarna i London började användas av polisen i jakten på efterlysta, och när EU nu vill använda fotspåren efter vår telekommunikation som polisiärt verktyg.

Efter att ha avhandlat riskerna med digital övervakning, låt oss diskutera nyttan. För det är otvetydigt att det finns en nytta – ibland är den liten, ibland stor, men visst finns den. På vissa områden går det att med relativt enkla medel skapa en närmast heltäckande kontroll, kanske med automatisk bötfällning även av minimala lagöverträdelse (såsom i fallet med hastighetsövervakning, och besök på kända barnpornografiska webbplatser). Om laglydnad är det enda man mäter måste i sådana fall den potentiella nyttan med digital övervakning anses vara mycket stor.

Tyvärr är det förmodligen betydligt lättare att med digital övervakning avslöja mindre brott än att avslöja terrorism. Terroristerna kommer rimligtvis att lära sig innebörden av elektroniska fotspår, den hårda vägen om inte annat. Vi kan därför komma att få ett samhälle med en digital övervakning som med stor effektivitet sätter dit Svensson för fortkörning och bidragsfusk men inte är särskilt verkningsfull mot terrorism.

"Säkerhet" är en komplicerad vetenskap, och det som på ytan ser ut att vara utmärkta säkerhetshöjande åtgärder kan ibland vara tomma gester. Den amerikanska säkerhetsexperten Bruce Schneier varnar i en nyutgiven bok för något han kallar "security theatre", det vill säga åtgärder från myndigheternas sida som får människor att känna sig säkra och myndigheterna att framstå som handlingskraftiga – men som egentligen är helt verkningslösa. Skådespel som lugnar massorna, helt enkelt.

I värsta fall kan säkerhetsåtgärder vara kontraproduktiva, det vill säga motverka sitt syfte. Det finns de som hävdar att en överdriven förlitan på tekniska former av övervakning och kontroll, på bekostnad av traditionellt polis- och underrättelsearbete, bidrog till att göra den 11 september möjlig. En blind tro på tekniken kan skapa en falsk trygghet som är farlig.

ÄR FÖRDELARNA VÄRDA NACKDELARNA?

Vid en värdering av för- och nackdelar med digital övervakning måste man också lägga stor vikt vid frågan vilket slags samhälle vi vill bo i.

- Är det värt att ge upp en stor del av den personliga sfären, och acceptera en långtgående övervakning av alla, för att minimera brottsligheten? Eller är det bättre att acceptera en högre brottslighet för att kunna bibehålla en personlig sfär?

- Är det exempelvis värt att avstå från den fulla kontrollen över bilen vi kör, och acceptera satellitbaserad avstängning av bränsletillförseln, om det kan minska antalet dödsoffer i trafiken?

Vid en första anblick kan det kanske verka cyniskt att medvetet acceptera att människoliv förspills för något så futtigt som människors möjlighet att köra fort, i synnerhet om fortkörandet är lagvidrigt. Men är den möjligheten verkligen något futtigt? Eller är det tvärtom en oerhört viktig mänsklig rättighet att få styra sitt liv och få chansen att själv välja att följa lagen (eller bryta lagen och ta konsekvenserna)?

Personligen anser jag att det är värt en viss extra brottslighet, som kanske hade kunnat elimineras med en långtgående övervakning, för att bibehålla en viss personlig frihet. Jag anser vidare att människor inte får fråntas sitt personliga ansvarstagande och den omedelbara kontrollen över sina handlingar, även om det kan motiveras med ett gott syfte.

Jag vet dock att inte alla delar min syn. Frågan borde upp på den politiska agendan. Där är den inte idag. Vi är mitt inne i en stor och mycket viktig förändring av balansen mellan samhälle och individ – samtidigt som det råder fullständig tystnad om saken på den politiska arenan. Det är oerhört märkligt. Om vi nu ska förflytta oss på den ovan nämnda skalan åt polisstatshållet ska det åtminstone klargöras att det är folkets vilja. Det ska baseras på en grundlig och bred diskussion, och därefter beslutas i demokratisk ordning.

SJU POLITISKA ÅTGÄRDER

Själv vill jag som sagt stoppa marschen in i övervakningssamhället. Därför föreslår jag, till att börja med, sju konkreta åtgärder. De kan indelas i två huvudslag:

Punkt 1-4: Åtgärder för att motverka att elektroniska fotspår över huvud taget uppstår, genom att värna om

den fortsatta möjligheten för den som så önskar att vara anonym i vardagen. Anonymitet är ju ett mycket viktigt socialt skydd. Detta är den första försvarslinjen mot storbror.

Punkt 5-7: Regler för att styra hur de elektroniska fotspår som trots allt uppstår ska hanteras. Detta är den andra försvarslinjen. Observera att detta skydd är väsentligt svagare och inte kan stå på egen hand. Regler kan ju brytas och politiska beslut ändras.

När frågan stötts och blötts i den offentliga debatten kommer kanske fler eller bättre åtgärder fram, men som ett startskott för debatten vill jag lansera denna förslagslista:

1. Vi bör införa principen att mängden identifierande elektroniska fotspår som människor lämnar efter sig i samhället ska minimeras. En lag bör stiftas om att detta ska beaktas vid förändringar i samhällets system, infrastruktur och regelverk. Ett "fotspårsperspektiv" ska genomsyra allt offentligt arbete (ungefär som regeringen har deklarerat att allt politiskt arbete idag genomsyras av ett genusperspektiv). För att fortsätta att använda Stockholms kommande biltullar som exempel innebär det att den tekniska lösningen för dessa ska utformas så att passager och betalningar kan ske anonymt (vilket går alldeles utmärkt).

2. En del i ovanstående kan vara att förändringar i system och infrastruktur ska föregås av en integritetskonsekvensutredning, i analogi med de miljökonsekvensutredningar som idag görs. En annan del skulle kunna vara en årlig genomgång och poängsättning av integritetens och anonymitetens ställning i samhället, utförd av en betrodd, kompetent och oberoende part – kalla det gärna integritetsrevision.

3. Vi bör utreda de juridiska möjligheterna att lagstifta om individens rätt att vara anonym vid sådana vardagsaktiviteter som bilresor, resor med allmänna (markbundna) kommunikationer, inköp i publika butiker och vistelse på allmän plats. Kanske bör exempelvis butiker som vänder sig till allmänheten åläggas att som betalningsmedel acceptera kontanter (som är en mycket viktig anonymitetsskyddande företeelse). Det gäller att förebygga ett samhälle, som inte alls är osannolikt, där anonymiteten är utrotad – ett samhälle där det helt enkelt inte går att ta bilen till stranden eller ta en promenad och köpa kvällstidningen utan att det registreras med namn och allt i loggfiler och databaser både hur man rört sig och vad man köpt. Jag är dock medveten om att gränsdragningarna för en sådan lag kan bli svåra.

4. Rätten för individer (och företag, organisationer etc) att använda sig av kryptering, anonymisering av

epost och surfande samt andra anonymitetsbevarande och integritetsskyddande teknologier (så kallade "PET", Privacy Enhancing Technologies) bör skyddas i grundlagen. Det synsätt som lurar strax under ytan hos en hel del politiska beslutsfattare runtom i världen (inklusive Sverige), att egentligen skall ingen få ha några hemligheter för staten, bör avfärdas.

5. Vi måste noga reglera om och i så fall i vilka situationer som polisen, skattemyndigheterna och andra myndigheter har rätt att ta del av elektroniska fotspår som uppstått i offentliga eller privata system. Reglerna måste också styra exakt vem som får ta del av vilken information, hur informationen får hanteras, hur länge den får sparas, och liknande. Polisen ska bara få använda elektroniska fotspår vid grova brott och bara i konkreta brottsutredningar (och alltså inte för att leta efter brotts-

lighet som inte är känd i förväg, något som kallas "fisketurer"). Det är tveksamt om andra myndigheter över huvud taget ska kunna få tillgång till elektroniska fotspår.

6. Användningen av svarta listor över personer som anses "misstänkta" ska vara ytterligt begränsad, förbehållen situationer som i

sanning är extrema.

7. Den klassiska frågan "Vem övervakar övervakarna?" måste ha ett tydligt svar. Den begränsade övervakning som trots allt tyvärr behövs i samband med mycket grov brottslighet ska stå under sträng demokratisk kontroll. Reglerna och de tekniska systemen ska vara så utformade att ett personligt ansvar kan utkrävas då överträdelser sker. Det ska resultera i åtal och kanske skadestånd. Straffskalan ska väljas så att frågans betydelse markeras. Tillsynen av att myndigheterna följer reglerna ska utföras av en instans med hög kompetens, goda resurser och ett stort mått oberoende. Det måste finnas enkla och effektiva vägar för medborgarna att kontrollera information om sig själva, att få felaktig information korrigerad, och att få skadestånd när så är motiverat.

Brottslighet ska bekämpas med stor kraft. Därför ska polisen ha goda resurser för att utreda begångna brott och för att övervaka personer som misstänks för grova brott. Där emot ska polisen inte övervaka hela befolkningen i förebyggande syfte. Vi ska inte på nationell nivå ta till oss det synsätt som hr polis Paulus Bergström i Grönköping har:

"Det finns två slags människor, de anhållna och de ännu inte anhållna."

Pär Ström (par@atomer.se) är IT-strateg och författare till boken Övervakad. Han ger ut ett kostnadsfritt epost-nyhetsbrev om utvecklingen inom storebrorssamhället, Big Brother Bulletin (se www.atomer.se/bbb).