Integritetens

LILLA RÖDA

Så kan övervakning skada människor -
Argumentsamling för storebrors kritiker

PÄR STRÖM

PÄR STRÖM

Integritetens LILLA RÖDA

Så kan övervakning skada människor –
Argumentsamling för storebrors kritiker

Den Nya Välfärden

den
nya
välfärden

Box 5625, 114 86 Stockholm
08-545 038 10 | www.dnv.se

Utgivet av Den Nya Välfärden

Regeringen har fel om arbetsrätten – företagarnas egen uppfattning (2008)
Förenkla reglerna för småföretagare (2007)
Den stora obalansen – hur lagarna missgynnar småföretagare (2007)
Varför straffa den som försöker göra rätt (2007)
Värsta krånglet (2007)
Mansförtryck och kvinnovälde (2007)
Fullt fokus på företagare
– europeiska företagare ger råd till Sveriges regering (2007)
Med storbror i byxfickan – integritetsrisker med RFID-chips (2007)
Roligt värre (2007)
Med storbror i uppfinnarverkstan
– ny digital övervakning från automatiska öron till internetdammsugare (2006)
Med storebror i baksätet – digital övervakning av dina bilfärder (2006)
Nya beska droppar – korta kritiska krönikor (2006)
Första hjälpen
Om dina anställda blir sjuka – en liten handbok (2006)
Var tredje får inte vara med
– en studie om arbetslösheten bland invandrare (2006)
Hur hög är arbetslösheten, egentligen? (2006)
Ole, dole, arbetslös
– nästan 3 av 10 ungdomar 16-24 år saknar jobb (2006)
Ge de arbetslösa en chans
– 150 000 nya jobb genom halverade arbetsgivaravgifter (2006)
Så lyckas du som företagare
– de bästa tipsen från svenska entreprenörer (2005)
Bakom skurkar och skandaler (2004)
Värsta krånglet (2004)
Jobbet är att mata puman
– hur och varför försäkringskassorna slarvar bort 40 miljarder om året av skattebetalarnas pengar (2004)
Tankebok för entreprenörer
– 222 citat från Aristoteles till Ingvar Kamprad (2003)
Entreprenören bakom allt
– 101 svenska succéer från ABBA till ölburkar (2002)
Beska droppar – korta kritiska krönikor (2002)
Skärp dig, Svensson
– med deklarationen om medborgerliga skyldigheter (2002)

Personvalsparti – bot för trötta partier (1999)
Berättelsen om jobben (1996)
Baksmällan – förutsättningar för politisk tillnyktring (1995)
Molnstoden – en vision för svenska folket (1994)

Den Nya Välfärden har även givit ut Medborgarnas offentliga utredningar

MOU 2000:1 Sveriges två gränser – om invandrarpolitiken
MOU 1999:1 För Sverige – på tiden!
MOU 1998:1 Samhällsmoral i praktiken
MOU 1997:1 Entreprenören i högsätet
MOU 1996:2 Kommunala företag – hot mot demokrati
MOU 1996:1 Den nya arbetsrätten – ett förslag
MOU 1995:3 Järntrianglar – förnyelsens fiende nummer ett
MOU 1995:2 Irrfärdens slut – för sunda statsfinanser
MOU 1995:1 När folkhemmets barn blivit vuxna
MOU 1994:1 HSF-modellen – patientmakt och kvalitet
MOU 1993:2 Charta Nova – politik för entreprenörskap
MOU 1993:1 Barnomsorg enligt kundvalsmodellen
MOU 1992:2 Hälso- och sjukvård för 2000-talet
MOU 1992:1 Eget val i äldreomsorgen – handledning
MOU 1991:6 Hur man säljer allmännyttehus – handledning
MOU 1991:5 På egna ben – reformera organisationsstödet
MOU 1991:4 Skolpeng hösten 92 – en handlingsplan
MOU 1991:3 Självständiga kommuner
MOU 1991:2 Sänkta skatter för en ny välfärd
MOU 1991:1 Företagsamhetens förutsättningar
MOU 1990:3 En marknad för bostäder åt alla
MOU 1990:2 Medborgarnas miljömanifest
MOU 1990:1 Minska statsskulden – sälj tillgångar
MOU 1989:1 Sänkt skatt för alla
MOU 1988:1 En ny grundlag – ett förslag

Ladda ned denna skrift

Denna skrift kan laddas ned gratis i pdf- eller mp3-version (talbok) från www.dnv.se/roda. I alla sina versioner får skriften spridas fritt så länge det sker utan att ta betalt och utan förändring av innehållet.

Mer material om ”storebror”

Du finner en hel del annat material om personlig integritet och övervakningssamhället på www.dnv.se/podcast. Där finns tre tidigare rapporter för nedladdning som pdf eller mp3, intervjuer du kan lyssna på samt opinionsbildande musik och ringsignaler.

Innehåll

1. Vad är det för fel med övervakning?

Ingen ifrågasätter nog att vi befinner oss i en utveckling där övervakningen av medborgarna kraftigt ökar, däremot är det många som frågar sig vad det är för fel med det. Frågan ställs både inom det politiska etablissemanget och, märkligt nog, bland medborgarna. Därför vill jag inleda denna skrift med att penetrera frågeställningen och ge min version av svaret.

För det första: Övervakning är absolut inte något som generellt sett är av ondo. Det behövs en viss övervakning i ett samhälle, för att hålla kriminellt beteende i schack och för att ge människor en känsla av trygghet (det förtjänar att nämnas att verklig trygghet inte är samma sak som upplevd trygghet - båda behövs).

Varje samhälle väljer var det ska lägga sig på en skala någonstans mellan noll övervakning (=anarki) och total övervakning (=1984-samhället). Se bilden nedan. Båda dessa extrempunkter är lika obehagliga, om än på olika sätt. Följdriktigt har de demokratiska länderna traditionellt placerat såg någonstans i mitten på den skalan, och där hör vi hemma.

Övervakning blir däremot ett problem om den är alltför omfattande eller av fel karaktär. Det är en fråga om balans. För lite övervakning ger problem i form av kriminalitet och otrygghet, för mycket övervakning ger problem i form av ... ja vadå? Vad gör det om vi är rejält övervakade? Den som har rent mjöl i påsen har väl inget att dölja?

Jo, det har vederbörande, och den saken vill jag nu utveckla. Det finns flera skäl till att få ha sitt privatliv ifred, och därmed flera problem med en övervakning som går för långt. Här följer, som jag ser det, den personliga integritetens olika försvarslinjer:

1. Vi har rätt till ett privatliv – punkt

Den första försvarslinjen tar avstamp i våra mänskliga rättigheter. Det är faktiskt något speciellt med att vara människa, jämfört med att vara djur. *Privatlivets skydd har ett egenvärde*. Eftersom den värderingen är allmänt accepterad har den skrivits in i ytterst grundläggande konventioner som FN:s deklaration om mänskliga rättigheter och Europakonventionen (se faktarutorna nedan).

FN:s deklaration om de mänskliga rättigheterna, artikel 12
(Universal declaration of human rights)
Ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.

Europakonventionen, artikel 8

1. Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.
2. Offentlig myndighet må icke störa åtnjutandet av denna rättighet med undantag för vad som är stadgat i lag och i ett demokratiskt samhälle är nödvändigt med hänsyn till landets yttre säkerhet, den allmänna säkerheten, landets ekonomiska välstånd, förebyggande av oordning eller brott, skyddandet av hälsa eller moral eller av andra personers fri- och rättigheter.

Grundprincipen enligt människorättskonventionerna är alltså mycket tydlig: Vi har rätt att ha privatlivet ifred utan att motivera det, som en mänsklig rättighet på samma nivå som rätten till liv. Sedan kommer undantagen, som förstås ger upphov till tolkningssvårigheter. I FN:s deklaration är det ordet "godtycklig" som utgör undantaget. Ingen får utsättas för "godtyckligt" ingripande (däremot icke godtyckliga ingripanden). I Europakonventionen finns som framgår i faktarutan en lista på undantag - skyddet för privat- och familjeliv får brytas igenom om det "är nödvändigt med hänsyn till landets yttre säkerhet, den allmänna säkerheten, landets ekonomiska välstånd, förebyggande av oordning eller brott, skyddandet av hälsa eller moral eller av andra personers fri- och rättigheter".

Det är fullständigt självklart att integritetsskyddet måste ha inskränkningar och undantag. Integritet kan aldrig bli total, vilket ingår i det resonemang om balans som fördes tidigare. Telefonavlyssning, exempelvis, utgör ett tvångsmedel som nog ingen invänder mot om det används vid misstanke om ett grovt brott efter beslut i domstol.

Men faktum är ändå att undantagen är undantag, och huvudprincipen är att varje människa har rätt att ha sitt privatliv ifred för det offentliga. Skälet till att detta har skrivits in i de mest grundläggande dokumenten, på samma nivå som rätten till liv, är förstås att de flesta människor upplever det som ett mycket väsentligt värde att ha ett skyddat privatliv. Det är helt enkelt obehagligt att vara iakttagen. Detta har inget med brottslig verksamhet eller andra suspekta aktiviteter att göra. En människa vill ha sina privata omständigheter ifred, och det behöver hon inte motivera.

Jag hävdar att en del av vår tids digitala övervakningsåtgärder måste anses strida mot FN:s deklaration om mänskliga rättigheter och Europakonventionen, eftersom det inte finns tillräckligt med underlag för att åberopa undantagen från grundprincipen om skydd för privatlivet. Dessa deklarationers underförstådda krav på proportionalitet, att nödvändigheten av övervakning ska vara så uppenbar att den väger tyngre än grundprincipen om skydd för privatlivet, är inte uppfyllda när det gäller exempelvis trafikdatalagringen (lagring av information om vilka vi ringer och mejlar, med mera) och den föreslagna FRA-övervakningen (generell möjlighet för Försvarets Radioanstalt att avlyssna/läsa kommunikation som passerar landets gränser, utan brottsmisstanke).

Det är anmärkningsvärt och allvarligt att ingen diskussion förekommer om hur dessa två övervakningsåtgärder står sig gentemot de ovan nämnda deklarationernas garantier för privatlivets helgd. Det finns en uppenbar risk att deklarationerna kommer att betraktas som historiska dokument utan relevans i dagens samhälle (ungefär som när president Bush hävdade att Genevekonventionen inte är "relevant" längre). Det vore oerhört allvarligt. Människo-

rättsdeklarationerna är oerhört väl genomtänkta, och de försvarar grundläggande värden som är tidlösa och som alltid kommer att vara utsatta för hot.

2. Information kan missbrukas eller hamna i orätta händer

Nästa försvarslinje för den personliga integriteten är betydligt mera konkret till sin karaktär. Alla databaser läcker (mer om detta längre fram). Personlig information som genom olika övervakningsåtgärder samlas in och lagras av polisen eller andra representanter för det offentliga kan både missbrukas av personalen och läcka ut och därmed hamna i orätta händer. I båda fall kan det förorsaka individer stor skada. Därmed måste man konstatera att digital övervakning visserligen må gagna medborgarna genom att motarbeta brottslighet, men samtidigt skapar den nya risker för medborgarna.

Här brukar man mötas av motargumentet att "den som har rent mjöl i påsen har inget att dölja". Det är storebrors viktigaste argument. Men det håller inte, för den som har rent mjöl i påsen har ändå något att dölja - oftast en hel del. Och det är naturligt och rätt! Mer om detta längre fram i denna skrift.

Det finns många sätt på vilka en laglydig medborgare kan lida skada av att elektroniska fotspår missbrukas eller hamnar i orätta händer. Några exempel:

- En person som via surfande eller elektronisk kommunikation får sin politiska åsikt röjd kan drabbas av utstötning från sin sociala krets eller bli motarbetad på arbetsplatsen.
- En person som får sina hälsoproblem röjda kan uppleva det som pinsamt, vilket är illa nog. Detta kan resultera i

negativa konsekvenser för det sociala livet. I värsta fall kan det resultera i bromsad karriär, nekad livförsäkring eller avslag på jobbansökningar.

- En person som får sin geografiska uppehållsort röjd kan råka ut för samma sak som hände en kvinna i Oslo: Hon var förföljd av sin före detta make och försökte hålla sig gömd. Han ringde biltullsföretaget och uppgav hennes bilnummer, och fick då reda på var och när hon brukade passera med sin bil. Därmed kunde han hitta henne, vilket var det hon minst av allt ville.

I Sverige (liksom i alla länder) dyker det kontinuerligt upp nya fall där sekretessbelagd information har läckts eller missbrukats av personalen. Personal på Försäkringskassan i Göteborg använde sekretessbelagda personuppgifter för att hämnas på sina privata fiender, och poliser har flera gånger avslöjats med att sälja information från sekretessbelagda polisregister eller lämna ut sådan till den undre världen. Se fler exempel bland bilderna. Man kan förmoda att mörkertalet är stort.

Innehåll i polisregister såldes

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

Polismannen sålde sekretesstämplade uppgifter om anställda i stora svenska företag.

rande uppgifter hade sedan lämnats ut till företagens ledningar. Svea hovrätt anser dock att

Polis åtalas för snatteri

Inför ögonen på butikspersonalen stoppade en kvinnlig

Säkerhetscheferna på Silja Line och Coon

påstod hon

Polis delade ut hemliga uppgifter till kriminella

GÖTEBORG. En polis i Västra Götaland tog under flera månader ut stora mängder hemliga

som tagit emot utgifterna utan också om andra anmälda brott och

område och för en person som inte

som är

STAFFAN KIHLSTRÖ

DAGENS NYHETER.

En utskrift från Dagens Nyheters nätupplaga, DN.se.

Publicerad 26 sep 06:48

Skyddade uppgifter läcks ut av teleoperatörer

MALMÖ. Post– och telestyrelsen (PTS) har tröttnat på teleoperatörer som lämnar ut skyddade uppgifter. Varje månad lämnas uppgifter om personer som har skyddad identitet ut till upplysningföretag som hitta.se och eniro.se.

Arbetssökandes cv spreds av Ams

Internt fusk på sjukkassorna

Anställdas fiffel med bidrag ska stävjas. Uppgifter ur personregistren används i privata vendettor.

VÄRLDEN

40 miljoner kontokort hackade

Av Gustav Svensson

Senast uppdaterad 18 juni 2005 21:02

Vad som kan vara historiens största datastöld har avslöjats, rapporterar New York Times. Kontokortsfiler har tömts på

Myndigheter avslöjar skyddade identiteter

Försäkringskassan och socialtjänsten sviker ofta kvinnor och barn som lever med skyddad identitet, genom att lämna

Sekretessuppgifter hamnade på nätet

Känsliga uppgifter i ett faderskapsmål hos socialnämnden i Norsjö hamnade på internet. ›

Detta var bara några exempel på hur det kan gå snett, variationsrikedomen är förstås oändlig. Det är viktigt att komma ihåg att även de mest triviala elektroniska fotspår

kan vara bärare av information som i fel händer är ytterst skadlig för en människa. Detta är förstås inget skäl till att helt avstå från att upprätthålla offentliga register eller genomföra viss övervakning, men det visar att medaljen har en tydlig baksida.

3. Anpassлighet minskar livskvaliteten och urholkar demokratin

Även om känslig information från exempelvis elektronisk kommunikation, inköp eller resor inte skulle läcka eller missbrukas utgör ändå rädslan för att så skulle kunna ske ett väsentligt problem. Risken är uppenbar att den alltmer omfattande digitala övervakningen gör att människor drar sig för att besöka vissa sajter, söka på vissa sökord, mejla vissa personer eller köpa vissa föremål. En sådan självcensur, som jag vill påstå redan i viss utsträckning har börjat göra sig gällande i Sverige, är på två sätt av ondo. För det första minskar den livskvaliteten, eftersom människor känner sig hindrade att göra det de egentligen skulle vilja göra. För det andra urholkar den demokratin.

Låt mig utveckla det senare. Demokratins livsnerv är information. Medborgarna kan inte fatta beslut i den demokratiska processen utan att skaffa sig underlag. Detta beslutsunderlag måste inkludera allt som behövs för att ge de fullständiga referensramarna, inte bara tillrättalagd information. Ett konkret exempel: För att ta ställning i ett riksdagsval kanske en medborgare vill inhämta information även om odemokratiska eller hatiska rörelser, för att själv bedöma deras argument och ta ställning till i vilken mån de utgör ett hot mot samhället. Om medborgaren då inte vågar besöka dessa rörelsers sajter, av rädsla för att hamna på en svart lista, så har vi ett demokratiskt problem. Observera

att det problemet föreligger oavsett om den svarta listan verkligen existerar eller inte. Rädslan att bli svartlistad skulle till och med kunna hjälpa fram odemokratiska rörelser, genom att medborgare börjar misstänka att dessa har något viktigt att säga som det politiska etablissemanget av egenintresse vill sopa under mattan.

4. Kritisk journalistik försvåras

Till det demokratiska problemet hör också att journalisters rörelsefrihet inskränks av digital övervakning. Ju mer digital övervakning vi har desto mer riskabelt blir det för tipsare att kontakta media, och desto svårare blir det för journalister att ägna sig åt grävande journalistik. Detta kan på sikt väsentligt försämra den tredje statsmaktens viktiga roll som granskare av makten och avslöjare av missförhållanden.

Det finns ett antal uppmärksammade exempel från senare tid där olika former av digitalt snokande och användning av elektroniska fotspår har använts som vapen mot obekväma journalister, av både statsmakten och det privata näringslivet. Exempelvis gjorde polisen i Belgien nyligen ett mycket uppmärksammat tillslag mot en Bryssel-baserad reporter på den tyska tidskriften Stern som utredde korruption inom EU. Polisen tog med sig dator och annan utrustning som enligt reportern helt röjer alla hans källor. Jag har själv fört samtal med en framstående grävande journalist i Sverige som berättat om hur krångligt hans arbete numera blivit på grund av alla åtgärder han måste vidta för att skydda källor från att röjas av elektroniska fotspår.

5. Är morgondagens stat lika snäll som dagens?

En del debattörer som försvarar den personliga integriteten tar avstamp i risken för att en framtida mera auktoritär re-

gim i Sverige skulle kunna missbruka olika övervakningssystem. Detta argument förfäktas ofta av personer med personlig erfarenhet av auktoritära politiska system, exempelvis sådana som växt upp bakom järnrån medan Sovjetunionen fortfarande fanns. "Tänk om Hitler hade haft tillgång till den digitala världens hela övervakningspotential, då hade han kunnat hitta varenda jude och politisk motståndare på några dagar", säger dessa personer. Det är sant och tänkvärt. Även om det idag känns som en avlägsen tanke att Sverige skulle kunna bli en diktatur så vet vi ingenting om framtiden. Och det är sant att ett färdigbyggt digitalt kontrollsystem över en natt skulle kunna förvandlas från brottsbekämpande till förtryckande, om makten byter karaktär.

6. Varning för ändamålsglidning

Ovanstående risk, en eventuell framtida auktoritär stat, utgör ett specialfall av de risker som följer med ändamålsglidning. Sådan innebär att insamlad information, eller uppbyggda övervakningssystem, med tiden börjar användas för andra syften än de som gällde från början. Ändamålsglidning är så vanlig att den måste betecknas som mera regel än undantag. Vi kan därför räkna med att råka ut för en ändamålsglidning, och förskjutning mot skärpt övervakning, oavsett vad som händer. Ifall samhällsklimatet väsentligt skulle försämras, exempelvis som ett resultat av fler spektakulära terrorattentat, skulle ändamålsglidningen kunna bli mycket långtgående och resultera i att de övervakningssystem som nu byggs upp börjar användas på sådana sätt som politikerna idag försäkrar aldrig kommer att ske.

2. Databasers inneboende problem

En del av de risker för medborgarna som digital övervakning för med sig beror på vissa fundamentala problem som karaktäriserar databaser och det sätt på vilka dessa används. Problemen med databaser är:

1. Alla databaser läcker

Att påstå något annat är att luras. Även de databaser som borde vara allra mest skyddade, exempelvis kontokortsföretagens, bankernas och polisens databaser, har i verkligheten visat sig läcka en hel del. Digital information har vingar - den har en vidunderlig förmåga att sprida sig och hamna där det inte är meningen. Dababaser läcker på tre sätt:

- *Den mänskliga faktorn.* Det största källan till läckor är ofta den personal som är satt att sköta databaserna. Hur mycket tekniska skydd man än bygger in måste det finnas människor som kommer åt informationen, och de karaktäriseras förstås av alla mänskliga svagheter. Personalen kan helt enkelt vara nyfiken och falla för frestelsen att tillfredsställa sin nyfikenhet genom databassökningar på grannar, arbetskamrater och vänner (eller ovänner). Personalen kan också vara girig och söka fram information som sedan säljs

till obehöriga, såsom kommersiella intressen, privatdetektiver eller den undre världen. Dessutom kan personalen genom slarv av misstag lämna känslig information öppen för obehöriga.

- Externa intrång. I den fysiska världen finns det inga lås som står emot alla inbrottsförsök, det handlar bara om hur svårt och tidskrävande det är att bryta sig in. Likadant är det i den digitala världen, fast egentligen värre. På grund av den enorma komplexiteten i digitala system händer det titt som tätt att en okänd svaghet i ett datasystem upptäcks av en utomstående, och vips är intrånget ett faktum. De som tränger in kan vara allt ifrån ungdomliga så kallade hackare till mycket målmedvetna och välfinansierade personer från exempelvis den organiserade brottsligheten, främmande makt eller mäktiga kommersiella intressen.

Kontokortsnummer stulna från SJ

Tusentals tågpendlare i Mälardalen har fått sina kontokortsnummer stulna. Hackare har kommit över 7.000 kontokortsnummer från SJ:s datasystem. Det är användare av timkortsautomaterna som har drabbats.

- Buggar. Det har hänt ett antal gånger - plötsligt visar det sig att den känsliga informationen ligger vidöppen. Kanske är den till och med åtkomlig för vem som helst över internet. En bugg i systemet bär skulden. Buggen åtgärdas snabbt, de ansvariga ber om ursäkt och lovar att det aldrig kommer att hända igen. Men varför skulle det inte göra det?

2. Blind tilltro till felaktig information

Vi har nog alla hört argumentet att "det står i datan". Det finns en stark tendens hos människor att utgå från att det som dyker upp på en dators bildskärm per definition är en korrekt beskrivning av verkligheten. Problemet är bara att bristande registerkvalitet - stora mängder felaktigheter - är ett problem som mer eller mindre alla databaser lider av. Detta kan få stora konsekvenser för de människor som drabbas av felaktiga registeruppgifter, särskilt i kombination med informationens klibbighet (se nästa punkt).


Grava fel i registret över näringsförbud

Ett uppmärksammat fall där låg registerkvalitet kan ha fått mycket stora konsekvenser finns att hämta i USA, där många anser att felaktigheter i ett register över brottslingar i Florida via flera tungan-på-vågen-situationer ledde till att Al Gore förlorade presidentvalet till förmån för George Bush. Till saken hör att en så kallad "felon" (ungefär "grov brottsling") inte har rösträtt i USA, medan mindre grova brottslingar får rösta. I det aktuella registret betecknades ett stort antal lindriga brottslingar felaktigt som "felons" varför deras röster (huvudsakligen på Al Gore) inte räknades.

3. Information är klibbig

Det har visat sig att det ofta är svårt att bli av med information som en gång är insamlad. Den klibbar fast. Det kan finnas flera skäl till att man vill ta bort information – den

kanske har visat sig vara felaktig eller det kan vara dags att gallra bort den för att regelverket föreskriver borttagning efter en viss tid. Men då visar det sig att informationen har spritt sig, och blir kvar på de andra ställena. Därifrån fortsätter den att sprida sig vidare - trots att den teoretiskt sett är raderad. Spridning kan exempelvis ske genom att backup tas i olika led, genom samarbete och samkörning med exempelvis andra företag, myndigheter eller länder, och genom försäljning av innehåll i databasen.

4. Information feltolkas

Det är ett vanligt problem att korrekt information i en databas övertolkas eller feltolkas på annat sätt, vilket kan leda till stora konsekvenser för individer. Problemet kan bli särskilt påtagligt när information vandrar från en databas till en annan. Låt oss konstruera ett exempel – se faktarutan på nästa sida.

Hur en trist dag blev livslång depression

En sajt för socialt nätverkande har en programvara som automatläser allt som medlemmarna skriver om sig själva för att kunna sälja personligt anpassad reklam. När en medlem skriver ”idag känner jag mig lite deppad” känner programvaran igen ordet ”deppad” och visar en annons för antidepressiva läkemedel. Så långt är ingen skada skedd. Men sedan får sajten knackig ekonomi och behöver pressa fram pengar till varje pris, och kommer på idén att sälja listan på alla medlemmar som fått den där annonsen visad för sig (liksom andra listor för den delen). Ett läkemedelsbolag köper listan och anser sig ha fått en databas med ”depressiva personer”. Sedan kommer databasen genom försäljning eller läckage i händerna på ett försäkringsbolag, som snabbt upprättar en svart lista på personer som inte ska beviljas livförsäkring eftersom självmordsbenägenheten är kraftigt förhöjd för depressiva människor. I värsta fall sprids denna lista genom samarbete försäkringsbolag emellan, vilket leder till att den där personen som en dag var ”lite deppad” under resten av sitt liv får mycket stora problem med allt som har med försäkringar att göra. Att bli struken från listan är inte att tänka på - för det första vet personen förmodligen inte om den, för det andra är den kanske informell och står därmed i praktiken utanför lagstad-gade rättigheter till korrigering.

Är exemplet i faktarutan hårddraget? Kanske en aning. Men i grunden är det en beskrivning av en fullt tänkbar händelseutveckling.

En kvinna i Norsborg utgör ett svenskt exempel på hur databasinformation kan övertolkas. Hon fick avslag på sin ansökan om banklån eftersom hon hade en tre år gammal obetald skuld om två (2) kronor, som hon inte ens visste om. Registret sa bara "obetald skuld", varpå banken bedömde henne som en kreditrisk.

5. Anonyma data kan återidentifieras

Ibland försvaras lagring av personliga data med argumentet "vi av-identifierar uppgifterna och sparar dem anonymt för statistik och forskning". Då är det dags att dra öronen åt sig, eftersom det ganska ofta är möjligt att återskapa identiteter genom att kombinera olika karakteristika för anonyma personer. För att ta ett enkelt exempel, det kanske bara finns en enda person i Sverige som är av manligt kön, brunögd, född 1949, 181 cm lång, ogift, bor i postnummerområde 113 40 och har varit signalist i det militära - och vips är den anonyma personen identifierad.

Enligt Latanya Sweeney, professor på Carnegie Mellon University i USA, kan 87 procent av den amerikanska befolkningen identifieras enbart med tillgång till tre uppgifter: födelsedatum, kön och postnummer. Hon menar att detta exempelvis gör det möjligt för sajter som frågar om vissa personliga data utan att fråga om namn att kombinera denna information med offentliga databaser och genom uteslutningsmetoden omvandla sitt anonyma register till ett namnsatt register.

6. Moores lag gör det omöjliga möjligt

Hårdvaran i datorer utvecklas mycket snabbt. Det gör att analyser som bygger på enorma mängder data eller oerhört komplicerade beräkningsalgoritmer, och som därför betrak-

tas som omöjliga att genomföra, kan visa sig möjliga i framtiden. Den berömda "Moores lag" säger att beräkningskapaciteten hos en mikroprocessor fördubblas ungefär var 18:e månad. Om lagen fortsätter att gälla kan man rent matematiskt förutspå att datorer om 20 år är cirka 8.000 gånger snabbare än idag. Framtidens mycket kraftfullare hårdvara kan komma att sätta tänderna i gamla databaser och därigenom finna nya samband och hota den personliga integriteten på oförutsägbara sätt.

Det är intressant att notera att precis den sortens utveckling redan har blivit verklighet inom DNA-området. Med dagens avancerade DNA-teknik kan polisen i en del fall lösa mord och andra allvarliga brott som ligger flera decennier tillbaka i tiden. Underlaget har funnits där hela tiden (i detta fall i form av biologiska prover), men först nyligen har tekniken utvecklats tillräckligt långt för att man ska få fram den eftersträvade informationen. (Detta är i och för sig utmärkt i just detta fall, men belyser det fenomen som i andra sammanhang kan vara av ondo).

Ett annat exempel på hur tekniken faktiskt har gjort det omöjliga möjligt kan hämtas från Tyskland, där forskare är i full färd med att återställa de hemliga dokument som den östtyska hemliga polisen Stasi förstörde i panik när berlinmuren föll. Papperen strimlades i dokumentförstörare. Nu har forskare scannat in strimlor från tusentals plastsäckar och satt en programvara på att para ihop strimlorna genom att analysera sådant som pappersstruktur, typsnitt och textens storlek och svärta.

3. Vilken övervakning är mest integritetskänslig?

Det är stor skillnad mellan olika övervakningsformer när det gäller graden av skadlighet för den personliga integriteten. I media har man länge haft en viss tendens att fokusera på övervakningskameror på offentliga platser. Det är kanske begripligt mot bakgrund av att kameror är så påtagliga och lätta att förstå sig på. Tyvärr slår det fel, eftersom övervakningskameror i dagens utförande inte utgör något större hot mot den personliga integriteten. Kort formulerat är det databaser som är farliga. Men låt oss tränga lite djupare in i problematiken.

För att bedöma vilket hot en viss övervakningsform utgör för integriteten finns det två viktiga frågor att ställa. Dessa är: Är övervakningen manuell eller automatisk? Är övervakningen identifierande till sin karaktär? Låt oss diskutera dessa frågor en i taget.

1. Är övervakningen manuell eller automatisk?

Med manuell övervakning menas sådan som måste hanteras av människor, medan automatisk övervakning kan fortgå utan mänsklig inblandning. Exempel på manuell övervakning är:

- Dagens svenska övervakningskameror - det är ju människor som tittar på bilderna
- Dagens svenska fartkameror - det är människor som går igenom bilderna och läser av registreringsnummer
- Polisbilar på vägarna, fotpatrullerande poliser på gator och torg
- Telefonavlyssning
- Buggning (rumsavlyssning)

All övervakning som innehåller en manuell komponent kännetecknas av att den är mycket personalintensiv, vilket sätter en naturlig broms på tillämpningen. Att övervaka mycket kostar mycket. Man kan ju leka med tanken på om vi skulle införa avlyssning av samtliga telefonsamtal som rings i Sverige och läsning av all post som skickas. Det skulle gå åt så många poliser att det förmodligen inte skulle räcka till ens om hela befolkningen blev poliser.

Så snart en övervakningsform blir automatisk, däremot, är situationen en helt annan. Möjligheterna att, om så önskas, skala upp övervakningen blir väldigt mycket större. I princip blir det med automatiska system möjligt att införa allomfattande övervakning av alla medborgare. Faktum är att detta redan håller på att ske. Några exempel:

- Den av EU och Thomas Bodström initierade trafikdatalagringen innebär ju att kontaktuppgifter och geografisk uppehållsort för samtliga medborgare i hela EU ska lagras.
- Den föreslagna FRA-övervakningen går ut på att all trafik som passerar landets gränser ska granskas med hjälp av de hemliga filtren.

- Den automatiska registreringsnummeravläsningen i Stockholms biltullar innebär generell övervakning av alla passerande fordon.

Slutsats: Om man väljer att se de stora penseldragen så är all övervakning som innehåller en manuell komponent att betrakta som ett måttligt eller litet hot när det gäller risken för ett storebror-ser-dig-samhälle. Detta hindrar naturligtvis inte att manuell övervakning kan vara mycket påträngande för dem som drabbas. Men dessa kan inte bli särskilt många.

2. Är övervakningen identifierande till sin karaktär?

Den andra stora frågan att ställa för att bedöma en viss övervakningsform är om den är identifierande till sin karaktär. Om övervakaren ser att någon ägnar sig åt en viss aktivitet, utan att veta vem det är, så är integritetskränkningen av naturliga skäl mycket liten. Kanske noll. Om identifiering äger rum, däremot, *kan* övervakningen vara synnerligen känslig.

Här följer några exempel på icke identifierande övervakning:

- Traditionella övervakningskameror på gator och torg. Här kan man visserligen invända att det går att känna igen människor. Men i praktiken torde så gott som alla som passerar vara obekanta för observatören i övervakningscentralen, om det inte rör sig om ett mycket litet samhälle. Övervakaren ser inte mer än "där kommer en äldre man i grön jacka" eller "där kommer en tonårsflicka i vit T-shirt".

- Jag anser också att buggning huvudsakligen kan klassificeras som en icke identifierande övervakning. Den lyssnande polisen hör ju röster i rummet utan att veta vilka personerna är. Undantag finns förstås: Om den tjänstgörande polisen känner igen en röst sedan tidigare eller har fått hjälp av annan spaning (såsom hemlig kameraövervakning eller manuell spaning utanför byggnaden) så kan identifiering ske. Men huvudprincipen är ändå att rösterna saknar identitet för avlyssnaren.

Nu är det dags att sätta samman de två frågeställningarna till en matris. De mest känsliga övervakningsformerna är de som är både automatiska och identifierande till sin karaktär. De minst känsliga är de som är manuella och icke-identifierande. Se figuren nedan.

	Manuellt	*Automatiskt*
Identifierade	—Manuell legitimationskontroll (pass, körkort...) —Traditionella poliskontroller i trafiken, trad. fartkameror	– Data om elektronisk kommuniktion —Automatläsning av epost, sms, fax – Automatisk nummerskyltsläsning i trafiken —Övervakningskameror med ansiktsigenkänning
Ej identifierade	—Traditionella övervakningskameror	—Övervakningskameror med tolkning av beteende, kroppsspråk etc

Detta innebär att bland de övervakningsformer som vi ska se upp mest för finns dessa:

- Trafikdatalagringen (lagra vem vi ringer, mejlar, geografiskt läge, med mera)
- Den föreslagna FRA-övervakningen
- Automatisk nummerplåtsinläsning i trafiken
- Lagring av resor med kollektivtrafiken (om trafikanten lämnar ut sitt namn)
- Lagring av information om inköp
- Övervakning av kommunikationen på internet

Till de minst integritskänsliga övervakningsformerna hör, enligt denna modell, övervakningskameror av traditionellt snitt. Liksom buggning.

Naturligtvis är jag medveten om att många betraktar buggning som höjden av integritetskränkning, och det är den också - på ett sätt. Den som drabbas av buggning, och på något sätt dessutom blir identifierad, råkar naturligtvis ut för ett synnerligen långtgående integritetsintrång. Men de kommer att vara mycket få. Jag har valt att som grund för min analys summera den totala integritetskränkningen i samhället, och med den modellen utgör buggning inte något stort problem. Modellen kan naturligtvis ifrågasättas, och andra modeller skulle kunna utformas, men för mig känns denna modell som en lämplig startpunkt för diskussionen.

För att ta resonemanget ytterligare ett steg framåt kan man konstatera att övervakningskameror och buggning hamnar i den minst integritetskänsliga rutan *bara under förutsättning att dagens teknologi används.* Så kommer inte att ske särskilt länge till:

- Övervakningskameror befinner sig i mycket snabb utveckling, och utomlands förekommer det redan sådana med inbyggd automatisk ansiktsigenkänning. När

övervakningskameror tar det teknikspråget förflyttar de sig också från den minst till den mest integritetskänsliga rutan i matrisen, eftersom de i ett slag blir både automatiska och identifierande. Det blir ju i princip möjligt att skapa ett system som utan mänsklig inblandning fyller på en databas med samtliga medborgares rörelser på gator och torg.

- Motsvarande utveckling finns avseende telefonavlyssning, men har inte alls kommit lika långt. I USA finns ett forskningsprojekt där man försöker utveckla automatiska öron. En programvara ska lyssna på telefonsamtal, översätta dessa till engelska, tolka betydelsen i konversationen, leta efter nyckelord, sammanfatta samtalets innebörd och leverera denna i textform till mänskliga övervakare. Om detta mjukvarumonster blir verklighet så hamnar telefonavlyssning med råge i den mest integritetskänsliga rutan i matrisen (i princip möjliggörs ju övervakning och analys av alla människors samtliga telefonsamtal).

Tvångsmedel kontra fisketurer

När vi talar om olika slags övervakning passar det att understryka den fundamentala skillnaden mellan övervakning av misstänkta och generell, förebyggande övervakning. Få, om ens någon, har invändningar mot förekomsten av polisiär telefonavlyssning och andra så kallade tvångsmedel som sätts in efter domstolsbeslut mot en viss person som misstänks för ett visst brott (som är grovt). Det går emellertid en rågång mellan denna berättigade övervakning och den nya förebyggande övervakningen som riktar sig mot hela befolkningen. I det senare fallet betraktas samtliga medbor-

gare som presumtiva brottslingar, och det gäller att vaska fram om och när brott begås.

Internationellt kallas sådan övervakning för ”fishing expeditions” – fisketurer. Kasta ut nätet så får vi se om det fastnar något! De mest långtgående polisfundamentalisterna förespråkar vad de kallar ”automated law enforcenemt” – automatiskt upprätthållande av lagen eller automatisk polis. Därvid åsyftas statliga programvaror som ständigt går igenom alla medborgares detaljerade elektroniska fotspår på en evig jakt efter tecken på brott.

De olika storebröderna

Denna skrift ägnas huvudsakligen åt ”storebror” i sin klassiska tappning, alltså övervakning från statsmakternas sida riktad mot medborgarna. Det bör dock understrykas att det även finns andra typer av ”storebröder” som kan vara väl så farliga för den personliga integriteten. Alla storebröder är ungefär lika nyfikna, men har olika drivkrafter. De fyra huvudslagen är:

- *Statsmakten*. Detta har redan kommenterats och utgör huvudfokus för denna skrift.
- *Företag.* Dessa riktar sin nyfikenhet åt två håll: De vill samla in information om sina kunder, i syfte att kunna öka sin försäljning. De vill också ha kontroll på sina anställda i syfte att skydda affärshemligheter och upprätthålla produktiviteten. Även eventuellt blivande anställda utsätts för företags nyfikenhet – jag tänker då på digitala kontroller av kandidater i samband med rekrytering.
- *Privatpersoner.* Fruar snokar på sina makar (och tvärtom) i syfte att undersöka om otrohet föreligger. Grannar snokar på grannar av ren nyfikenhet, människor snokar på arbetskamrater. Och så vidare. Ett annat skäl till privat-

snokandet, utöver ren nyfikenhet, kan vara strävan efter ekonomisk vinning (säljbar information, utpressning etc).

- *Främmande makt*. När stora ekonomiska och politiska intressen står på spel korsar övervakningen ofta de nationella gränserna. Detsamma gäller det så kallade kriget mot terrorismen. Att IT-samhället i grunden är gränslöst gör detta möjligt.

4. Drivkrafter bakom övervakningsvågen

Vad beror det på att vi är inne i en utveckling där samhällets övervakning av medborgarna ökar i ett tempo som ingen kunde drömma om för bara tio år sedan? Jag anser att dessa fem faktorer samverkar:

1. Den digitala revolutionen

Digitaliseringen av vår vardag gör att människor efterlämnar allt fler elektroniska fotspår, vilka enkelt låter sig användas för övervakningsändamål. Den digitala revolutionen utgör därför en möjliggörare för övervakningssamhället. För bara 10-15 år sedan fanns inte tillnärmelsevis så många elektroniska fotspår som idag. Det var exempelvis inte länge sedan som all information om vem som ringt vem var borta i samma ögonblick som luren lades på. Nu går vi mot en situation där nästan varje vardagshandling loggas elektroniskt och hamnar i en databas. Ett av de senaste inslagen i denna utveckling är digitala lås i bostäder, som förstås resulterar i loggfiler som visar när varje lägenhetsinnehavare har kommit hem.

2. Ett rädslans klimat

Terrorattackerna i New York år 2001, liksom efterföljarna i Madrid och London, har skapat ett klimat präglat av rädsla. Den som tillämpar vetenskaplig riskanalys skulle dra slutsatsen att rädslan för terrorism är mycket större än vad som är sakligt motiverat, medan andra risker som egentligen är betydligt större istället nedvärderas. Detta är psykologiskt betingat – så fungerar vi människor. Det klimat av rädsla som vi har fått underblåses av media, som har ett kommersiellt intresse av att hålla det vid liv. Mord, våldtäkter och fall av grov misshandel får ofta en enorm medial uppmärksamhet, även om dessa brott statistiskt sett utgör en mycket mindre risk för genomsnittssvensken än en del andra företeelser (såsom trafikolyckor och sjukdomar).

3. Rationaliseringar och besparingar

Polis och andra rättsvårdande myndigheter strävar naturligtvis precis som alla andra efter att effektivisera sin verksamhet med hjälp av moderna verktyg. Detsamma gäller många andra, såsom de myndigheter som har att hindra bidragsfusk. Där kommer tekniken in. Ifall dessa aktörers verksamhet kan utföras på ett mera kostnadseffektivt sätt med hjälp av IT är det förstås naturligt att så sker. På sätt och vis. Det är i alla fall naturligt att de strävar efter att ta till verktygen – sedan är det upp till de politiskt ansvariga att väga in andra värden (såsom integritet) och vid behov säga nej.

4. Människor prioriterar bekvämlighet

De IT-lösningar som möjliggör övervakning skänker ofta medborgare ett stort mått av bekvämlighet. Det gör det frestande för människor att strunta i den personliga integriten,

och med hull och hår acceptera upplägg som är rena drömmen för storebror. Visst är det praktiskt att besöka en sajt som redan ”vet” vad man tittade på förra gången och vad man skrev in då. Ett annat exempel är att många människor gärna vill knyta sina personuppgifter till kollektivtrafikens nya chipförsedda resekort, eftersom det ger möjlighet att få ett nytt kort om det gamla tappas bort. Att kollektivtrafiken sedan sätter deras personnummer på den lagrade informationen om varje genomförd resa blir sekundärt.

5. Säkerhetsbranschens kommersiella intressen

Vi får inte glömma att det finns en stor säkerhetsbransch som sedan terrordåden 2001 mot World Trade Center i New York åtnjuter ett uppsving som överträffar dess vildaste drömmar. Det rör sig om allt ifrån tillverkare av övervakningskameror och diverse annan apparatur till utvecklare av olika slags programvaror, konsulter och bevakningsföretag. Denna bransch, eller kanske man ska säga dessa branscher, har allt att vinna på att rädslan bibehåller sitt järngrepp om människor.

6. Den offentliga makten vill breda ut sig

Jag påstår att det politiska etablissemanget tar tillfället i akt att utöka sin egen maktsfär. Detta utvecklas i nästa kapitel.

5. Maktförskjutningen och undersåtefieringen

På det tyska språket finns en obehaglig term som lyder ”die Machtergreifung” (maktövertagandet). Den syftar på det maktövertagande från nazistpartiets sida som resulterade i tolv års terrorvälde. Kommer morgondagens uppslagsverk även att innehålla den snarlika termen ”die Machtverschiebung” (maktförskjutningen)?

Sedan många hundra år har det pågått en positiv utveckling där makt har förskjutits från staten till medborgaren. Forna tiders ”konung av Guds nåde”, som kunde styra och ställa allt efter sitt dagshumör och som bara ansåg sig vara ansvarig inför Gud, har successivt pressats tillbaka till förmån för demokrati och medborgerliga rättigheter. Denna utveckling har de allra flesta av oss all anledning att vara mycket glada för.

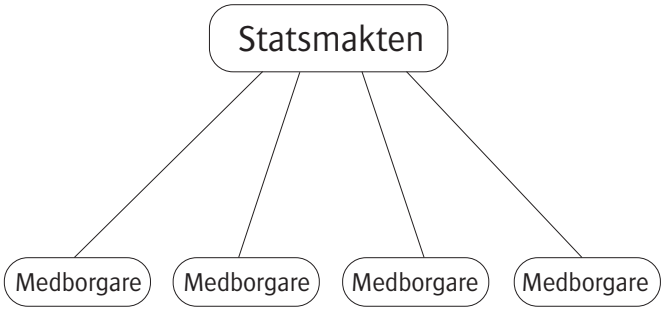
Därför är det mycket oroande att tecknen nu är tydliga på att utvecklingen börjar reverseras. Medborgarnas landvinningar rullas tillbaka. Det är nämligen precis vad som håller på att hända. Viktiga medborgerliga rättigheter, och till och med mänskliga rättigheter, utsätts för den ena inskränkningen efter den andra med hänvisning till det så kallade kriget mot terrorismen.

Det går en röd tråd mellan svenska politiska beslut såsom avlyssning utan misstanke, EU-direktivet om lagring

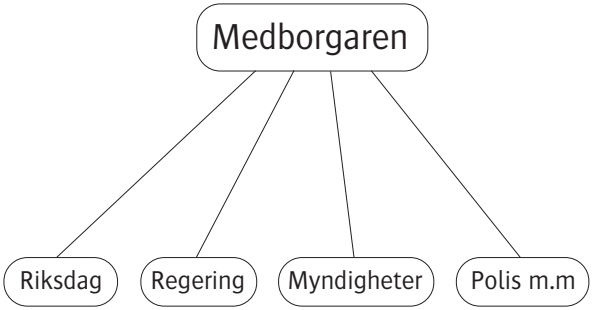
av alla medborgares kommunikationsmönster och massbrotten mot mänskliga rättigheter på Guantánamo-basen. Och den röda tråden heter undersåtefiering. Våra makthavare, som teoretiskt utgör folkets representanter, har påbörjat en utveckling tillbaka mot en värld där vi är undersåtar igen.

Gång på gång hör man uttalanden från myndigheter, ministrar och andra makthavare i stil med: ”Myndigheterna *behöver* den här informationen för att kunna bekämpa brott”. Det brukar vara betoning på ”behöver”. Vad de då talar om är människors känsliga elektroniska fotspår som avslöjar mycket om de mest privata delarna av våra liv. Hela debatten utstrålar attityden att det inte är fråga om att *be* medborgarna att öppna sitt privatliv, och motivera sig, utan om att *kräva* in den.

Därmed måste man konstatera att det politiska etablissemanget har ett attitydproblem. Min uppfattning är att de flesta personer verksamma inom det som brukar kallas politiken beter sig som om de äger sina medborgare. Om inte annat lägger de sig till med den inställningen så snart de når makten. Vi undersåtar har bara att foga oss. De förstår vårt eget bästa bättre än vi. Så här kan deras världsbild ritas:



Jag anser att detta är fundamentalt fel. Medborgarna äger staten, inte tvärtom. Regering, riksdag och samtliga myndigheter är till för att tjäna medborgarna. Vi medborgare är uppdragsgivare och därmed ytterst chefer för alla som arbetar i den offentliga sektorn. Vänd upp och ned på pyramiden, storebror! Så här är det egentligen:



Det är på tiden att politiker och myndighetsföreträdare börjar förstå vilken deras roll är. Om så krävs så får vi, deras chefer, upplysa dem om hur det ligger till. När det gäller integritetsfrågan blir konsekvensen att makthavarna får sluta med sitt kaxiga ”myndigheterna *behöver* den här informationen”, och börja formulera sig lite mer hovsamt. Ungefär så här: ”Hur mycket information om er själva kan ni medborgare tänka er att lämna ut?”.

6. Storebrors vanligaste argument bemöts

I det här kapitlet tänker jag ge lite hjälp till de integritetsförespråkare som vill ta debatten mot storebrorsanhängare. Det figurerar ett antal argument mot personlig integritet, varav ”rent mjöl i påsen” är det vanligaste. Alla kan bemötas. Här följer ett antal argument med förslag på bemötande.

”Den som har rent mjöl i påsen har inget att dölja”

Jo. Vi har alla en hel del som vi vill behålla privat, och det har ingenting med olaglig verksamhet att göra. Det kan finnas tusen och en orsaker till att en människa inte vill få detaljer om sitt privatliv utlämnade, och hon har ingen som helst skyldighet att motivera sig. Bara obehagskänslan räcker. Att vilja ha, och få ha, ett privatliv för sig själv är något som ingår i att vara människa. Det är till och med inskrivet i FN:s deklaration om mänskliga rättigheter och Europakonventionen. Den som ifrågasätter människors rätt att ha sitt privatliv ifred visar prov på att ha en auktoritär människosyn.

”Nya teknologier gör att integriteten ändå är förlorad”

Nej. Allt som är tekniskt möjligt behöver inte genomföras. Framför allt behöver det inte beslutas i politiska försam-

lingar och bli lag. Riksdagen måste inte alls ändra lagarna för att underlätta olika former av övervakning. Än mindre måste riksdagen genom lagstiftning tvinga fram övervakning. Om det politiska etablissemanget skyddade integriteten, istället för att angripa den, skulle förlusterna för den personliga integriteten bli mycket mindre än med dagens situation. Nog stämmer det att vi aldrig kan få tillbaka 1980-talets integritetsskyddande anonymitet, men vi kan ändå i hög utsträckning påverka hur mycket av integriteten som förloras.

”De teknologier som hotar integriteten ger faktiskt stor samhällsnytta”

Visst är det ibland så, och i en del lägen måste vi därför acceptera vissa integritetskränkningar. Men samma samhällsnyttor kanske kan uppnås med en annan teknologi, som inte utgör samma hot mot integriteten. Om så inte är fallet måste ändå samhällsnyttan med den nya teknologin vägas mot risken för intrång i den personliga integriteten – är nyttan verkligen tillräckligt stor? Detta brukar kallas proportionalitetsbedömning. Om ett samhälle okritiskt inför varenda teknisk lösning som erbjuder någon form av samhällsnytta är risken överhängande att det snabbt utvecklas till vad vi brukar kalla en polisstat.

”Åtgärder som skyddar integriteten blir för dyra”

Det beror på vilka värderingar man har, hur mycket man anser att skyddad integritet får kosta. Därmed är det delvis en politisk fråga. Avgasrening i bilar kostar stora pengar, men de flesta länder i världen har kommit fram till att det är värt kostnaden och har därför lagstiftat om avgasrening. De flesta teknikområden är omgivna av fördyrande lagkrav.

Dessutom är merkostnaden oftast inte stor, om den alls finns, ifall integritetsskydd byggs in i nya tekniska system redan från början. För övrigt skulle samma argument kunna användas gentemot domstolar. Tänk vad mycket kostnader man skulle spara in om man avskaffade rättegångar och dömde människor summariskt. Vissa saker måste få kosta.

"Varför är du motståndare till brottsbekämpning?"

Frågan är fel ställd, eftersom saken inte kan förenklas till att vara antingen för eller emot brottsbekämpning. Det är intellektuellt ohederligt att antyda att den som inte accepterar vilka åtgärder som helst från statsmaktens sida därmed automatiskt skulle stå på brottslingarnas sida. Vi medborgare bör förhålla oss till polisen på samma sätt som till militären: Naturligtvis behövs den, men om den ska stå i medelpunkten och styra allting i samhället är vi inne på en farlig väg.

"Hotet från terrorismen kräver extrema åtgärder"

Terroristerna vill krossa vår samhällsform. Om vi försöker försvara det fria samhället genom att förfalla till metoder som hittills varit utmärkande för auktoritära regimer har vi ju förlorat det vi skulle försvara. Naturligtvis måste polis och andra samhällsorgan få använda sig av IT och elektronik som alla andra, men den användningen måste vägas mot andra värden såsom respekt för privatlivets helgd. För övrigt föreslås ofta olika former av övervakning med terrorhotet som argument utan att det finns några vetenskapliga belägg för att åtgärderna verkligen skulle ha tydlig verkan mot terroristerna. Det tas ofta för givet, utan att styrkas, att ny övervakning minskar terrorismen. Vi är många som tror att inte ens ett riktigt 1984-samhälle skulle eliminera terro-

rismen – terroristerna skulle bara byta arbetssätt. För övrigt kan man fundera över vilken effekt mot terrorismen man skulle kunna uppnå genom att använda en del av de mycket stora summor som idag satsas på övervakning på andra sätt.

”Om du tror att någon bryr sig om dina förehavanden är du paranoid”

Riskerna för den personliga integriteten ligger oftast inte i möjligheten att en viss person utsätts för myndigheters eller företags fokuserade förföljelse. Varje person är bara en i mängden, det stämmer, men det hindrar inte att han eller hon kan åsamkas stor skada genom att personuppgifter läcker, missbrukas eller blir föremål för ändamålsglidning.

När detta är sagt måste man konstatera att risken ändå faktiskt finns att enskilda personer blir föremål för fokuserad förföljelse. Detta kan framför allt komma att drabba obekväma sanningssägare i privat eller offentlig sektor liksom politiskt oliktänkande. I många demokratiska länder finns dokumenterade fall där laglydiga ”dissidenter” utsatts för myndigheternas egentligen olagliga övervakning. Även i Sverige, där Säpo under många år i stor skala bröt bröt mot lagen. Faktum är att Sverige har ett uselt track record på området.


AFTONBLADET

TISDAG 17 DECEMBER 2002

100 000 svenskar åsiktsregistrerade


AFTONBLADET

TORSDAG 19 DECEMBER 2002

Säpo hade sexregister på SVT-folk

Samlade in uppgifter om 240 anställda

GÖTEBORG.

Homosexuella medarbetare på

7. Ett politiskt paket för integritetsskydd

Den dag våra politiker blir intresserade av att skydda medborgarnas personliga integritet finns ett antal åtgärder de kan vidta. Det handlar både om ett förhållningssätt som leder fram till vissa grundprinciper och om konkreta lagar som kan stiftas. Här följer ett förslag till politiskt paket för integrietetens skydd. Fler punkter är tänkbara, men dessa ser jag som viktigast.

1. Inför principen att de elektroniska fotspåren ska minimeras

Övervakningssamhällets bränsle är elektroniska fotspår. Det enda riktigt säkra sättet att hindra att känsliga personuppgifter missbrukas, hamnar i orätta händer eller blir föremål för politisk ändamålsglidning är att personuppgifterna över huvud taget inte finns. Därför bör regeringen uttala som en generell målsättning att inom de områden där det offentliga har ett ord med i laget ska mängden elektroniska fotstpår alltid minimeras. Om detta hade tillämpats skulle en konsekvens exempelvis bli att Stockholms biltullar hade utformats så att passagerna varit anonyma (vilket vore tekniskt möjligt om viljan funnits).

2. Skapa en integritetsbalk

Alla de lagar som på något sätt har bäring på skyddet av den personliga integriteten bör samlas i en integritetsbalk. Det skulle medföra ett antal viktiga fördelar. Överblicken skulle förbättras och luckor i lagstiftningen skulle lättare identifieras. Lagstiftaren skulle tvingas ta ett helhetsgrepp om integritetsfrågan (som idag ofta hamnar mellan två stolar). Dessutom skulle man uppgradera statusen för den juridiska disciplinen ”integritetsrätt”, vilket förmodligen skulle leda till ökat utrymme vid universitetens juristutbildningar och mera forskning på området. Allt detta skulle verka främjande på den personliga integritetens ställning i samhället.

3. Inför integritetskonsekvensutredning

Precis som det måste genomföras en miljökonsekvensutredning inför politiska beslut som kan påverka miljön bör regeln införas att en integritetskonsekvensutredning ska föregå politiska beslut som kan påverka integriteten.

4. Lagstifta om visst integritetsskydd

På vissa sätt behöver den personliga integriteten skyddas i lag. Det gäller exempelvis rätten för envar att använda sig av kryptering och andra integritetsskyddande teknologier (så kallade PET, privacy enhancing technologies). Det är också lämpligt att lagstifta om förbud mot generell, automatisk övervakning av medborgarna. Manuell generell övervakning ska naturligtvis få förekomma, exempelvis i form av patrullerande poliser och traditionella övervakningskameror, men automatisk övervakning (exempelvis utförd av programvaror som analyserar trafiken på internet) som riktar sig mot personer mot vilka brottsmisstanke inte finns

ska inte få förekomma. En av konsekvenserna blir att den föreslagna FRA-övervakningen inte blir tillåten.

5. Inför en författningsdomstol

När Integritetsskyddskommittén nyligen la fram sitt slutbetänkande ingick förslaget att skriva in ett skydd för den personliga integriteten i grundlagen. Tanken är att denna grundlagspassus ska stoppa politiska beslut där samhällsnyttan med en åtgärd inte väger tillräckligt tungt för att motivera eventuella kränkningar av den personliga integriteten som kommer med på köpet.

Förslaget är utmärkt, men inte tillräckligt, eftersom det kan förväntas att de politiska beslutsfattarna många gånger kommer att vara färgade av sin övervakningsvänliga grundinställning när de genomför den proportionalitetsbedömning som grundlagen kommer att kräva. Sverige behöver en författningsdomstol, eftersom det visat sig att regeringen ofta kör över lagrådet. Det är intressant att notera att den nyligen införda tyska lagen om trafikdatalagring har överklagats till Tysklands författningsdomstol av en grupp medborgare med krav på omedelbart upphävande.

Fördelen med en författningsdomstol är att en hel lag kan förklaras ogiltig. En annan åtgärd för att göra det svårare för regeringen att bryta mot grundlagen vore att ta bort det så kallade uppenbarhetsrekvisitet ur lagprövningslagen. Det handlar om den formulering som säger att tillämpningen av en lag kan prövas i domstol om den ”uppenbart” strider mot grundlagen. Många menar att om ordet ”uppenbart” togs bort skulle det bli mycket vanligare att domstolar på medborgares initiativ ifrågasatte det sätt på vilket en lag tillämpas.

8. Så tipsar du en journalist anonymt

Avslutningsvis: För att visa hur insnärjda i elektroniska fotspår vi medborgare håller på att bli vill jag beskriva vilka åtgärder som krävs om du vill ringa ett samtal och vara hundra procent säker på att inte lämna några spår efter dig. Såvitt jag känner till är det fortfarande möjligt (?) om du vidtar dessa åtgärder:

1. Skaffa ett kontantkort för mobiltelefoner. Betala det med sedlar, inte kontokort, eftersom alla slags betal- och kreditkort efterlämnar elektroniska fotspår.

2. Köp en ny mobiltelefon. Om du skulle sätta in det nyköpta kontantkortet i din gamla telefon kan du lätt spåras, eftersom varje mobiltelefon har ett nummer (IMEI-nummer) som inte kan tas bort eller ändras och som skickas med vid varje samtal. Den nya telefonen måste naturligtvis betalas med kontanter.

3. Ring inte några andra samtal med telefonen än det samtal där du vill vara anonym. Om du ringer nummer som du vanligtvis brukar ringa kan du bli avslöjad eftersom programvaror för mönsterigenkänning kan koppla samman ringmönstret med ringmönstret för din gamla telefon (som ju

är knuten till ditt namn). Du behöver inte ringa vänner eller släktingar för att avslöja dig, det kan räcka med kanske tre samtal till något sånär ovanliga nummer för att mönsterigenkänningen ska kunna genomföra matchningen.

4. Tänk på var du befinner dig när du slår på och av telefonen. Den lämnar ju geografiska fotspår efter sig. Använd bara telefonen när du befinner dig på betryggande avstånd från din bostad eller andra platser som kan knytas till dig.

5. Vill du vara riktigt försiktig bör du förställa din röst under samtalet, med tanke på risken för programvaror med röstidentifiering. Ifall du skickar sms, tänk på att uttrycka dig på ett sätt som avviker från ditt vanliga, eftersom det finns mönsterigenkännande programvaror som känner igen det sätt på vilket sms-meddelanden är formulerade (exempelvis val av förkortningar) och kan koppla dig till tidigare (identifierade) sms-meddelanden. Gör över huvud taget så lite som möjligt med telefonen.

6. När du har tipsat journalisten måste telefonen kasseras. Men tänk på dina DNA-spår. Förmodligen förstörs dessa om telefonen bränns efter att ha begjutits med bensin. Efter brännandet kan resterna plockas upp med stor försiktighet och kastas i havet eller en stor sjö långt bort från din bostad.

7. Förmodligen räcker dessa åtgärder, men det finns en svaghet i åtgärdsskedjan. Det kan finnas bilder från butikens säkerhetskamera som visar dig när telefonen eller kontantkortet köptes. Det kan gå att via tidpunkten koppla samman bilden på dig med den aktuella telefonen eller det ak-

tuella kortet. Identifiering kan naturligtvis försvåras genom bärande av peruk, lösmustasch, glasögon och liknande. Ett sätt att vara säker på att inte bli fotograferad är förstås att köpa kort och telefon av en privatperson på begagnatmarknaden – men hur tar du kontakt med säljaren utan att lämna elektroniska fotspår efter dig? Det är naturligtvis oetiskt, men att stjäla en telefon skulle kunna vara ett framkomligt sätt att införskaffa en utan att efterlämna några spår. Snällare är då att dyka på en främling på stan och erbjuda vederbörande en lockande summa pengar om du omedelbart får telefonen.

*

Gå gärna in på www.dnv.se/podcast där det finns mycket material samlat om övervakning och personlig integritet.

Rent mjöl i påsen?

Vad är det för fel med övervakning, den som har rent mjöl i påsen har väl inget att dölja? Vilka drivkrafter ligger bakom dagens våg av ökad övervakning? Hur bedömer man graden av integritetshot hos en viss övervakningsform jämfört med en annan? Vilka politiska åtgärder skulle kunna vidtas för att stoppa marschen in i övervakningssamhället?

Detta är några av de frågor som behandlas i Integritetens lilla röda, som också finns för fri nedladdning som pdf och mp3 på: www.dnv.se/roda

Pär Ström är integritetsombudsman vid Den Nya Välfärden. Läs även hans tidigare rapporter ”Med storebror i baksätet”, ”Med storebror i uppfinnarverkstan” och ”Med storebror i byxfickan”. De kan laddas ned eller beställas från: www.dnv.se/podcast

den nya välfärden

Box 5625, 114 86 Stockholm | tel 08-545 038 10
www.dnv.se | integritetsombudsmannen@dnv.se