

**22 TEKNOLOGIER  
SOM HOTAR DIN  
INTEGRITET**



# **Med storebror i uppfinnarverkstan**

Ny digital övervakning, från

automatiska öron till internetdammsugare

**PÄR STRÖM**

PÄR STRÖM

# Med storebror i uppfinnarverkstan

Ny digital övervakning, från

automatiska öron till internetdammsugare

Den Nya Valfärden

# Utgivnet av Den Nya Valfärden

## Med Storebror i baksätet

– *digital övervakning av dina bilfärder (2006)*

## Nya Beska droppar

– *korta kritiska krönikor (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)

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

den  
nya  
välfärden

Box 5625, 114 86 Stockholm  
08-545 038 10 | [www.dnv.se](http://www.dnv.se)

Stockholm, 2006

© Stiftelsen Den Nya Välfärden och Pär Ström.

# Innehållsförteckning

Förord	7
1. Den digitala revolutionen har bara börjat	8
2. Automatisk ansiktsigenkänning och humördetektering	10
2.1 Gångigenkänning – identifiering via gångstil	14
3. Automatiska öron möjliggör massavlyssning	16
3.1 Manipulerade insekter och smart damm	19
4. Automatisk sanningskontroll i stat och näringsliv	22
4.1 Avläsning av människors känslor via telefon	25
5. Mobiltelefonen som diskret spion	27
5.1 Mobilen avlyssnar hela rummet	27
5.2 Osynlig närvarolista vid fotbollsmatch	29
5.3 Övervakning av biltrafik	30
5.4 Människokartor i Rom	30
6. Skrivare och kopiatorer som tjallar	32
6.1 Programvaror får inbyggd polis	34
7. Mönsterigenkänning – analys av totalt beteende	37
7.1 Automatisk övervakning i Aten och EU-planer	43
8. Umgängesanalys och automatisk kompisdetektering	46
9. Automatisk övervakning av våra banktransaktioner	49
10. Internetdammsugare patrullerar nätet – även i Sverige	52
10.1 Svenska skatteverket skaffar dammsugare	55
11. Andra kreativa metoder för kontroll och övervakning	57
11.1 Kommunikationsdammsugare	57
11.2 Flygande övervakningskameror	57
11.3 Nakenscanner - med eller utan fikonlöv	58
11.4 Myndigheterna fjärrstyr våra bilar	58
11.5 Kreativa sätt att bekämpa anonymiteten	59
12. Övervakning – bra eller dåligt?	61



## Förord

Vi har fått ett samhällsklimat där ”säkerhet” prioriteras högre än allting annat – inklusive personlig integritet. Men är det så säkert att ens ett övervakningsamhälle á la 1984 kan ge oss skydd mot ondska? Tänk om vi offerar den personliga integriteten förgäves?

Jag har studerat vad som håller på att ske i ”storebrors uppfinnarverkstad” och jag blir rädd. Det som dagens teknik kan åstadkomma i övervakningsväg, med lite målmedvetenhet och en bra budget, det är mycket. Betydligt mer än de flesta är medvetna om. Och med morgondagens teknik – ja, det ska vi bara inte tala om.

Ska vi verkligen acceptera att vi med ”de små stegens tyranni” bygger ett samhälle där alla undersåtar, förlåt, medborgare, lever sitt liv som i glashus? Har FN:s deklaration om mänskliga rättigheter – där vår rätt att ha privatlivet ifred är garanterad – i det tysta upphört att gälla? Det är två av de frågor jag tycker man ska ha i bakhuvudet när denna rapport läses.

*Pär Ström*

Integritetsombudsman vid Den Nya Valfärden  
par.strom@dnv.se

Denna rapport kan laddas ner gratis i fulltext (pdf-format) på Den Nya Valfärdens hemsida: [www.dnv.se](http://www.dnv.se)

# 1. Den digitala revolutionen har bara börjat

Den digitala revolutionen har bara börjat. I takt med att den rullar vidare utvecklas allt fler, och alltmer avancerade, metoder för teknisk övervakning och kontroll. Det som var science fiction igår är genomförbart idag och (kanske) en del av vår vardag imorgon. Det är grundregeln, och så kommer det att fortsätta under överskådlig tid. Något som bidrar till att kasta bensen på brasan är att mängden ”elektroniska fotspår” som vi människor lämnar efter oss i vardagen hela tiden ökar – sådana fotspår utgör ju råvara för många övervakningssystem.

Denna rapport handlar om övervakningsteknologier som upplevs som ”avancerade” (många fler finns). Vissa av dem befinner sig ännu så länge bara i forskningslabbet, medan andra redan är tagna i drift på sina håll (men fortsätter att förfinas i laboratorierna). Långtifrån allt har ännu kommit till Sverige, men det vore naivt att tro något annat än att de flesta av de metoder som med framgång provas av polis och underrättelsetjänst utomlands med en viss fördröjning kommer till vårt land. Dessutom kan vi räkna med att utländska intressen övervakar svenskar, eftersom IT-världen är gränslös.

Många av de teknologier som beskrivs i denna rapport är mycket påträngande och integritetskränkande till sin karaktär när de används var för sig. Än värre blir det om teknologierna kopplas samman. Ifall ansiktsgenkännande kameror på stan lämnar data till centrala programvaror för mönsterigenkän-

ning och beteendetolkning som även hämtar data från system för sanningskontroll installerade hos teleoperatörerna, och så vidare – då blir ”storebror” stark. Man kan med en sannolikhet som gränsar till visshet utgå ifrån att en sådan sammankoppling kommer att ske, eftersom den utvecklingen redan har börjat.

Den tekniska evolution som beskrivs i denna skrift påverkar i betydande utsträckning den känsliga maktbalansen mellan staten och medborgarna. Den öppnar också för omfattande missbruk och läckor som kan åstadkomma stora skador för individerna. Dessa konsekvenser, liksom frågan om vilken grad av övervakning som trots allt är nödvändig för att hålla brottsligheten stängd, diskuteras i det sista kapitlet.

Denna rapport tar av naturliga skäl bara upp sådana övervakningsteknologier som nått offentlighetens ljus. Vi kan lugnt räkna med att det finns betydligt mera på gång i labben – eller kanske redan infört – som vi inte känner till. Så här sa Gilman Louie, VD för In-Q-Tel, ett investmentbolag som ägs av den amerikanska underrättelsetjänsten CIA, till nyhetstjänsten News.com: ”Vi har tagit lite mer än 100 teknologier i bruk i underrättelsevärlden. Vissa av dem känner ni till, men andra basunerar vi inte ut.”

*Länk:*

In-Q-Tel: [www.in-q-tel.com](http://www.in-q-tel.com)

## 2. Automatisk ansiktsigenkänning och humördetektering

Automatisk ansiktsigenkänning fungerar så att en programvara jämför ansikten i digitala bilder med en databas som innehåller tidigare lagrade porträttfoton. Teknologin kan exempelvis användas som komplement till vanliga övervakningskameror, vilket man också börjat göra på sina håll, exempelvis i tunnelbanan och på pubar.

Den vanligaste formen av ansiktsigenkänning bygger på mätningar av avstånd mellan olika kroppsdelar i ansiktet, såsom näsa, ögon och mun. Om tillräckligt stora likheter mellan aktuell bild och jämförelsebild konstateras så meddelar programvaran träff. Känsligheten kan ställas in.

Den tekniska utvecklingen i denna färska bransch har redan gått vidare, och kompletterande teknologier som sägs öka tillförlitligheten i identifieringen har dykt upp. Exempelvis finns nu programvaror med hudanalys, vilket innebär att de avlästa människornas hudstruktur analyseras och används tillsammans med ansiktets form i identifieringsprocessen. En leverantör har lanserat ett system med tredimensionell ansiktsigenkänning (digitala lermasker) som fungerar i mörker på grund av att nära-infrarött ljus används.

Ansiktsigenkänning är ändå en ny teknologi, som ännu inte helt lever upp till alla leverantörers löften. Den fungerar relativt bra i kontrollerade miljöer för ”verifiering” (vilket innebär att systemet kontrollerar om en viss person är den han eller hon



“In God we  
trust. All others  
we monitor”

*Talesätt inom National Security Agency (NSA)*

inte kan gå runt kvarteret med hunden utan att passagen lagras i en databas (med motiveringen att informationen är till nytta i kampen mot grov brottslighet).

*Några exempel på genomförda eller planerade satsningar på automatisk ansiktsgenkänning:*

- Brittisk polis har i Birmingham och Newsham (en förort till London) installerat kameror med ansiktsgenkänning på offentliga platser. Brittisk polis har också använt automatisk ansiktsgenkänning för att i förebyggande syfte identifiera kriminella besökare på musikfestivalen V Festival i Weston Park i Staffordshire. Av de 75.000 besökarna greps 79, men det är inte känt vilken roll ansiktsgenkänningen därvidlag spelade.

- Övervakningskameror med automatisk ansiktsgenkänning ska på försök införas på en av Tokyos tunnelbanestationer. Ett digitalt foto ska tas av alla som passerar spärrens, och fotot ska omedelbart matchas mot en databas med foton på misstänkta terrorister. Testet ska pågå i en till tre månader.

- Forskare vid Queensland University of Technology i Australien tänker utveckla vad de kallar ”den ultimata ansiktsgenkänningen”. Systemet ska sätta samman tredimensionella rörliga videobilder på människor från olika övervakningskameror och därigenom kunna använda fler ansiktskaraktistika än tidigare för identifiering. Därigenom ska kvaliteten i identifieringen ökas, och man ska bli mindre beroende av ljusförhållanden. Systemet ska också kunna upptäcka onormalt beteende. Som tänkbara platser för användning nämner forskarna flygplatser, banker och shoppingcentra.

- En professor vid det kinesiska Tsinghua-universitetet har utvecklat en programvara för automatisk ansiktsgenkänning. Denna har godkänts av en expertpanel på Ministeriet för allmän säkerhet, och ska inom en nära framtid börja användas på offentliga platser såsom postkontor, flygplatser och bostadsområden. Bland annat ska ansiktsgenkänningen under de olympiska spelen 2008 spana efter kända huliganer i folkmassor.

- Alla Pekings 3.000 bankomater kommer att förses med automatisk ansiktsigenkänning och kopplas till polisens nätverk, så att ordningsmakten kan få ett automatiskt larm om en efterlyst person försöker ta ut pengar.

- BioBouncer är ett nyligen lanserat system för ansiktsigenkänning avsett för pubar och barer. Det är önskad kund som ska "studsas" i dörren. En övervakningskamera läser av ansiktet på varje person som kommer, och när en bråkmakare försöker komma in går larmet och personalen kan "studsas" vederbörande. Det finns också ett nätverk med vilket pubar och barer kan dela med sig av bilder på bråkmakare.

## 2.1 Gångigenkänning – identifiering via gångstil – och annat kreativt

Ansiktsigenkänning är inte det enda sätt på vilket övervakningskameror utvecklas på ett kreativt sätt. Några exempel:

- Sony har presenterat en "intelligent" kamera som självständigt kan följa någon – den "förstår" alltså att det rör sig om en och samma person som förflyttar sig.

- Den militära forskningsmyndigheten Darpa (Defence Advanced Research Project Agency) i USA har genomfört forskning kring gångigenkänning ("gait recognition"), alltså identifiering av en människa via automatisk avläsning av vederbörandes gångstil. Målet är att ingen ska kunna komma närmare en amerikansk regeringsbyggnad än 150 meter utan att vara automatidentifierad. Liknande forskning drivs även i Storbritannien.

- Vid State University of New Jersey har man börjat utveckla ett system som ska läsa av människors kroppsspråk via en kamera, och ge besked om huruvida de ljuger eller inte. Tanken är att systemet ska användas vid exempelvis gränstationer, inpassering till känsliga byggnader och vid polisförhör. Finansiär är det amerikanska säkerhetsdepartementet, Department of Homeland Security, som lägger 3,5 miljoner dollar på projektet.

Forskningsledaren, Dimitris Metaxas vid universitetets Center for Computational Biomedicine Imaging and Modeling, berättar att ”mikrogester” och ”mikroansiktsuttryck” ser olika ut beroende på om en människa ljuger eller talar sanning, och detta kroppsspråk är mycket svårt att dölja.

- Forskare vid University of Cambridge i Storbritannien är i samarbete med Massachusetts Institute of Technology i färd med att utveckla en programvara som läser av människors sinnesstämning. Det sker genom att avläsa 24 grundläggande ansiktsuttryck, såsom höjda ögonbryn och rynkad panna, eftersom en viss kombination motsvarar ett visst humör. En japansk biltillverkare uppges vara intresserad av att bygga in teknologin i framtida bilmodeller. Den amerikanska bankomat tillverkaren NCR har studerat möjligheten att bygga in humörigenkänning i bankomatens digitalkamera.

*Några exempel på leverantörer:*

A4Vision: [www.a4vision.com](http://www.a4vision.com)

Aurora: [www.auroraserv.co.uk](http://www.auroraserv.co.uk)

Cybula: [www.cybula.com](http://www.cybula.com)

Darpa: [www.darpa.mil](http://www.darpa.mil)

Guardia: [www.guardia.com](http://www.guardia.com)

Identix: [www.identix.com](http://www.identix.com)

NSA: [www.nsa.gov](http://www.nsa.gov)

### 3. Automatiska öron möjliggör massavlyssning

Din digitala världen sväller över av både talad och skriven information. Underrättelsetjänster och polismyndigheter lägger stor energi på att utveckla och införa programvaror som hjälper dem att mer eller mindre automatiskt finna nålen i höstacken – de viktiga detaljerna i informationshavet.

Så länge en människa måste sitta och lyssna sig igenom varje avlyssnat telefonsamtal kan polisens och underrättelsetjänsternas telefonavlyssning inte skalas upp särskilt mycket. Situationen blir helt annorlunda om programvaror kan stå för lyssnandet – då skulle en teknisk grund läggas som i princip skulle göra det möjligt att avlyssna alla samtal som rings. Just sådana programvaror håller på att utvecklas – och forskarna har stora anslag till sitt förfogande.

Tänk dig att datorer avlyssnar mängder med telefonsamtal, ”förstår” vad som sägs och är programmerade att lyssna efter vissa ord eller namn. De samtal där dessa förekommer omvandlas i sin helhet till skriven text, efter att vid behov ha översatts till rätt språk. Därefter analyseras innebörden av meddelandet och programvaran skriver en sammanfattning, som skickas till en handläggare för bedömning. Fram till dess har ingen mänsklig inblandning förekommit. Detta är visionen.

En bit på väg har forskarna redan kommit. Exempelvis säljer det amerikanska företaget Verint Systems redan idag program som lyssnar på en mängd konversationer, känner igen vissa ord eller namn och spelar in dessa (men bara dessa) samtal.

”Vi har tagit lite mer än 100 teknologier i bruk i underrättelsevärlden. Vissa av dem känner ni till, men andra basunerar vi inte ut.”

*Gilman Louie, vd för In-Q-Tel, ett investmentbolag ägt av den amerikanska underrättelsetjänsten CIA, i nyhetstjänsten News.com*

En del av programvarorna kan också känna igen röster och dialekter, och använda detta som urvalskriterium. Kunderna hämtas huvudsakligen från polis- och underrättelsevärldarna, men även andra organisationer såsom call centers köper in systemen. CallMiner är ett företag som säljer en programvara liknande Verints. LanguageWeaver är ett av de företag som säljer programvaror för automatisk översättning till engelska.

Det totala greppet när det gäller automatisk avlyssning, enligt visionen ovan, är målet med ett utvecklingsprojekt kallat GALE, Global Autonomous Language Exploitation, som drivs av USA:s militära forskningsorganisation Darpa. Programvaran ska vara behjälplig i "kriget mot terrorismen" och även på andra sätt hitta hot mot Förenta Staterna i det väldiga globala informationsbruset.

"Automatiska öron"-programvaror kan naturligtvis användas på annan information än telefonsamtal. Exempelvis är de tillämpbara i samband med buggning (rumsavlyssning) och för att automatiskt analysera vad som sägs i olika länders radio- och TV-sändningar. Faktum är att en av Darpas underleverantörer i utvecklingen av GALE, företaget BBN Technologies, redan har ett system vid namn Broadcast Monitoring System som automatiskt skapar sökbara arkiv av internationella TV-sändningar (inklusive översättning till engelska och omvandling av det talade språket till text).

I många fall utgörs den information som ska analyseras inte av tal utan av skriven text, exempelvis epost. Då behövs förstås bara en delmängd av den funktionalitet som ska finnas i GALE.

I utvecklingen av GALE läggs stor vikt vid integration av de olika stegen (språkförståelse, översättning, omvandling till text samt sammanfattning). Dessutom är kvalitetskraven höga. Redan idag finns det dock ett flertal programvaror från olika leverantörer som utför ett eller flera av dessa steg, måhända med en något lägre precision än vad som ska bli slutresultatet av GALE.

Nedan följer några andra exempel på forskning och utveckling kring system med koppling till avlyssning.

- Den amerikanska rymdflygstyrelsen NASA, som ibland bistår amerikansk underrättelsetjänst, har utvecklat en metod för att avlyssna en byggnad från utsidan. Ljudisoleri-  
ng av rummen i byggnaden skyddar inte. Det hela går till så att en sändare placerad utanför byggnaden sänder ut mikrovågor med en frekvens mellan 30 och 100 GHz. Dessa frekvenser passerar genom alla väggar. Vål i rummet påverkas mikrovågorna av rörliga föremål (såsom kläder och gardiner) som fladdrar mikroskopiskt i takt med att mänskligt tal och andra ljud sätter luften i vibration. En extremt svag signal av vibrationspåverkade mikrovågor reflekteras och kan fångas upp ute på gatan. Ur denna signal kan en programvara extrahera ljudet inifrån byggnaden.

- Forskare vid University of California i Berkely har kommit fram till att en tio minuter lång inspelning av ljudet från klickandet på en dators tangentbord räcker som underlag för att en programvara med 90 procents sannolikhet ska kunna utläsa de skrivna orden. Ofta kan tekniken användas för att gissa en persons lösenord efter ett tjugotal försök.

### 3.1 Manipulerade insekter och smart damm

En svärm av fjärilar som sprider sig och diskret avlyssnar människors samtal, det låter onekligen som science fiction. Icke desto mindre startar Darpa ett projekt för att försöka uppnå detta.

Insekterna ska kunna fjärrstyras, och de ska även kunna användas för andra syften än avlyssning. Exempelvis talas det om att insekterna ska kunna överföra videobilder och lukta sig fram till dolda bomber. Som exempel på särskilt lämpliga insekter nämns dagsländor och nattfjärilar.

Meningen är att mikroskopiskt liten teknologi ska planteras i insekterna när de befinner sig i puppstadiet, och när insekterna sedan förvandlas är det meningen att utrustningen ska växa in och bli en del av dem. ”Vid varje förvandling genomgår insektskroppen en förnyelseprocess som kan läka sår och flytta om interna organ så att de omger främmande föremål”, skriver

”Vid varje förvandling genomgår insektskroppen en förnyelseprocess som kan läka sår och flytta om interna organ så att de omger främmande föremål [såsom en mikrofon]”

*Den amerikanska forskningsmyndigheten Darpa*

Darpa i ett dokument som utgör underlag för det privata näringslivets offertskrivande inför projektet.

Det företag som tar hem ordern måste kunna skapa ”en insekt [som kan styras till en plats] inom fem meter från ett visst mål som är beläget 100 meter bort”, står det i upphandlingsunderlaget. Sedan ska insekten ”förbli på denna plats antingen permanent eller tills den får andra instruktioner”. Insekten måste också ”kunna sända data från relevanta sensorer, med information om lokal omgivning. Sådana sensorer kan inkludera gassensorer, mikrofoner, video etc”. Allt enligt Darpa.

I USA pågår också forskning kring så kallat smart damm (”smart dust”), bland annat vid University of California i Berkeley. Tanken är att mikroskopiskt små elektronikchips med inbyggda sensorer och radiosändare, så kallade mikroelektromekaniska system (”MEMS”), ska sväva genom luften som dammpartiklar och rapportera hem. Det som rapporteras ska kunna vara ljud (avlyssning), men också många andra typer av data såsom temperatur, ljus, vibrationer och fuktighet. Denna forskning, som delvis är finansierad av Darpa, befinner sig i ett tidigt skede.

Brittiska och amerikanska militära forskare har inlett ett samarbetsprojekt syftande till att utveckla robotflugor som ska kunna flyga in i trånga utrymmen och rapportera. Här handlar det alltså inte om levande flugor utan om mekaniska apparater som ska likna flugor och flyga med flaxande vingar. Detta har rapporterats av nyhetstjänsten Ananova.

#### *Några länkar:*

BBN Technologies: [www.bbn.com](http://www.bbn.com)

CallMiner: [www.callminer.com](http://www.callminer.com)

Darpa: [www.darpa.mil](http://www.darpa.mil)

In-Q-Tel: [www.in-q-tel.com](http://www.in-q-tel.com)

Language Weaver: [www.languageweaver.com](http://www.languageweaver.com)

Nice Systems: [www.nice.com](http://www.nice.com)

SRI International: [www.sri.com](http://www.sri.com)

Verint Systems: [www.verint.com](http://www.verint.com)

## 4. Automatisk sanningskontroll i stat och näringsliv

Automatisk sanningskontroll kan realiserats med tre typer av teknologi: Baserat på ljud (röstanalys), baserat på ordval och talrytm samt baserat på bilder (kroppsspråk). Den ljudbaserade sanningskontrollen kan sägas vara ett specialfall av automatiska öron. Kanske morgondagens system för sanningskontroll blir riktigt kraftfulla genom att använda de tre metoderna tillsammans?

Låt oss börja med röstbaserad sanningskontroll. En intressant produkt har utvecklats av det israeliska företaget Nemesysco. Deras programvara analyserar frekvenser, vibrationer och andra variabler i rösten och känner med hjälp av detta av om personen talar sanning eller ljuger (liksom en del andra omständigheter).

Nemesyscos programvara fungerar även via telefon. Den gör sina bedömningar i realtid, alltså samtidigt som personen talar. Systemet uppnår inte full säkerhet i bedömningen, men leverantören hävdar att cirka 80 procents säkerhet kan påräknas.

Nemesysco vänder sig till stor del till polismyndigheter och underrättelsetjänster världen över, men finner även sina kunder på hela andra marknader. Exempelvis har flera försäkringsbolag i Storbritannien, Tyskland och Schweiz provat programvaran i sin kundtjänst. Det brittiska försäkringsbolaget Highway Insurance uppges ha kunnat minska sina utbetalningar med 15 procent efter att ha infört Nemesyscos lögnigenkänning på inkommande telefonsamtal till skaderegleringsavdelningen. Nemesysco provas också som ett led i säkerhetskontrollerna på Domodedovo-flygplatsen i Moskva.

”LVA känner av personens nivå av stress, avståndstagande, rädsla samt om han eller hon är generad eller försöker svara cyniskt eller bedrägligt. Den mäter också den avlyssnades grad av tänkande.”

*Företaget Nemesysco om sin programvara för automatisk analys av telefonsamtal*

En som forskar kring ordbaserad sanningskontroll är psykologen James Pennebaker vid University of Texas i Austin. Han säger i tidskriften National Geographic att automatisk lögnanalys kan basera sig på det faktum att personer som ljugar ofta använder ovanligt många ”skräpor” såsom pronomen, prepositioner och artiklar. Å andra sidan indikerar en frekvent användning av vad han kallar undantagsord (såsom ”men”, ”inte”, ”aldrig” och ”förutom”) att den som talar har en nyanserad bild av det som avhandlas och förmodligen talar sanning.

Lögner kan också avslöjas genom ovanligt många pauser och andra ”diskontinuiteter” i talat språk. En som forskar kring programvaror för detta är Tom Meservy, expert på informationssystem vid University of Arizona i Tucson. Hans forskningsgrupp arbetar också med att försöka utveckla programvaror som analyserar människors kroppsspråk i videoupptagningar för att dra slutsatser om sanningshalten i det som sägs. Bland annat handlar det om att analysera huvudets rörelser och placeringen av händerna.

Ett näraliggande område är automatisk detektering av vinklat skrivande, vilket är något som datorteknikern och textanalysexperten Paul Thompson vid Dartmouth College i New Hampshire forskar kring. ”De senaste åren har intresset varit stort för programvaror som automatiskt kan läsa av när en text inte är objektivt skriven”, säger han. Han berättar att datoriserad textanalys också kan användas för att dra slutsatser om vem som har skrivit en viss text.

I kapitlet om digitala dammsugare (sist i denna skrift) beskrivs en planerad amerikansk programvara som ska patrullera internet och registrera hur positivt eller negativt utländska medier och deras journalister skriver om USA. En enklare programvara (”News”) som har liknande funktionalitet tillhandahålls redan idag av företaget Corpora Software.

*Två andra initiativ på området:*

- Vid State University of New Jersey har man börjat utveckla ett system som ska kontrollera sanningshalten i tal genom au-

tomatisk analys av den talande personens kroppsspråk. Detta tas upp i kapitlet om automatisk ansiktsigenkänning tidigare i denna skrift.

- Den amerikanska militära forskningsmyndigheten Darpa har ett projekt kallat Misinformation Detection System (MDS), som syftar till utvecklandet av en programvara som automatiskt kan hitta lögnar och medvetet vilseledande information i skriven text.

#### 4.1 Avläsning av människors känslor via telefon

Det ovan nämnda företaget Nemesysco har inte bara programvaror för automatisk sanningskontroll. På sin webbplats berättar de om en serie programvaror avsedda för polis, underrättelsetjänst och privatdetektiver som automatiskt lyssnar på telefonsamtal (eller andra samtal) och läser av människors känslotillstånd. Det handlar bland annat om produkterna SCA1 och LVA 6.50. Analysen kan göras i realtid (under pågående samtal).

Systemen ska exempelvis via telefon kunna detektera en talande persons grad av spänning, rädsla, avståndstagande samt försök till cyniska svar och huruvida vederbörande är generad eller inte. Man använder en patenterad teknologi som enligt företaget ”detekterar spår av hjärnaktivitet” genom att göra en ”bred spektralanalys” av rösten och därigenom upptäcka ”minimale ofrivilliga förändringar i röstens vågform”.

Så här skriver Nemesysco på sin webbplats: ”LVA 6.50 uses Nemesysco’s Security Level Layer Voice Analysis technology (LVA) utilizing over 18 vocal parameters and thousands of mathematical processes to accurately analyze your subject’s state-of-mind in a professional and discreet manner. [...] LVA detects levels of tension, rejection, fear, embarrassment and attempts to outsmart or answer cynically. It also measures the subject’s level of thinking.”

Nemesysco har också olika specialversioner av sina analys-

programvaror, bland annat en för call centers och en för rekryteringsföretag och personalavdelningar. Den senare analyserar bland annat arbetssökandes hederlighet och lojalitet.

Det likaledes israeliska företaget Nice Systems, som har ett antal olika produkter inom området automatiska öron, har bland annat ett system som analyserar röster i telefon och automatiskt detekterar ilska. Tanken är exempelvis att företagsledningen på ett call center ska ingripa mot de telefonister som blir arga på sina kunder eller vars motparter (kunder) blir arga. Företaget har även automatisk ordigenkänning, så att ledningen kan specialhantera de samtal/telefonister som figurerar i samband med att vissa ord nämns. Datoriserad övervakning av samtalen i call centers är en bransch som enligt tidskriften Spectrum från standardiseringsorganisationen IEEE växer med 10-15 procent om året. Nice Systems har också produkter avsedda för polismyndigheter och underrättelsetjänster, exempelvis systemet NiceTrack avsett för totalintegration av övervakning med råvara från många slags informationskällor.

*Några länkar:*

Corpora Software: [www.corporasoftware.com](http://www.corporasoftware.com)

Darpa: [www.darpa.mil](http://www.darpa.mil)

Nemesysco: [www.nemesysco.com](http://www.nemesysco.com)

Nice Systems: [www.nice.com](http://www.nice.com)

## 5. Mobiltelefonen som diskret spion

På flera sätt kan mobiltelefonen förråda människor. Bland annat skickar den ständigt information som gör att mobiloperatören känner till mobiltelefonens geografiska position (vilket är nödvändigt för att nätet ska fungera). Nu märks en tendens att utomstående börjar använda dessa data för sina egna syften, en teknologi som kallas ”cell phone mining” (gruvdrift i mobilnät-loggfilernas stora ”gruva”).

### 5.1 Mobilen avlyssnar hela rummet

Mobiloperatörer kan installera programvara på mobiltelefoner som gör det möjligt att via mobilens mikrofon avlyssna omgivningen även när samtal inte pågår. Programvaran installeras på distans utan att mobilens ägare märker någonting. Därmed kan en helt vanlig mobiltelefon förvandlas till en närmast perfekt mobil buggningsenhet. Så här skriver den ansedda internationella affärstidningen Financial Times i sin internetupplaga:

*If ordered to do so, mobile telephone operators can also tap any calls, but more significantly they can also remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call, giving security services the perfect bugging device.*

Tidningen antyder att detta buggningsförfarande har kommit till användning vid spårandet och gripandet av Hamdi Adus Issac, en av de misstänkta gärningsmännen bakom terrorattentat i London.

”Utan att tänka på  
det har vi börjat bära  
med oss vårt egen  
pejlingsbara ID-kort i  
form av en mobil-  
telefon”

*Sandra Bell, chef för avdelningen  
Homeland Security på Royal United Services Institute.*

”Utan att tänka på det har vi börjat bära med oss vårt egen pejlingsbara ID-kort i form av en mobiltelefon”, säger i artikeln Sandra Bell, chef för avdelningen Homeland Security på Royal United Services Institute.

Det har också dykt upp spionprogramvaror för mobiltelefoner på den öppna marknaden. En sådan är FlexiSpy, som kan köpas via internet för några hundralappar. Programvaran skickar rapport till den nyfikne (den som har installerat spionprogramvaran) om vem telefonens ägare ringer och SMS-ar. SMS-meddelandena sänds i sin helhet till den nyfikne. Pro-versionen av FlexiSpy kan också användas för att avlyssna rummet där mobiltelefonen finns – hela tiden, oavsett om samtal pågår eller inte (förutsatt att telefonen är påslagen).

## 5.2 Osynlig närvarolista vid fotbollsmatch

Ett intressant exempel på innovativ ”cell phone mining” kan hämtas från Rotterdam i Nederländerna, där polisen ville ha hjälp av allmänheten med att identifiera ett antal huliganer som hade bråkat vid en fotbollsmatch. För att få kontakt med åskådarna vände sig polisen till mobiloperatörerna med en begäran att få ut en lista på de ca 17.000 mobiltelefonnummer som befunnit sig vid De Kuip-stadion vid tiden för matchen. Polisen skickade sedan ett SMS till alla dessa nummer med en begäran om assistans.

Det kontroversiella är att åskådarna i praktiken blev automatiskt uppsatta på en osynlig närvarolista när de kom till matchen, något som förmodligen ytterst få av dem var medvetna om. Att bli registrerad såsom fotbollsåskådare kan väl i och för sig i de flesta fall (om än inte alltid) avfärdas som ganska harmlöst, men tänk om det istället rört sig om en stor politisk demonstration? Eller Pride-festivalen?

Många tror att GSM-tekniken bara gör det möjligt att se vilken basstation som en mobilanvändare befinner sig närmast, något som ger en noggrannhet på som bäst ett par hundra me-

ter. Med så kallad triangulering, där flera basstationer mäter signalstyrkan från mobiltelefonen, kan dock positionen bestämmas på ungefär 10 meter när.

### 5.3 Övervakning av biltrafik

Ett annat exempel på ”cell phone mining” är övervakning av trafikflöden. På vägnätet runt staden Baltimore i USA, liksom i nederländska Antwerpen och israeliska Tel Aviv, har myndigheterna börjat övervaka trafikflödet genom att läsa av hur snabbt mobiltelefoner förflyttar sig. Innehavarna av mobilerna vet ingenting. Informationen köps från mobiloperatörer, som hittills bara lämnar kollektiv information. Steget vore inte långt till att börja läsa av sådan information på individuell nivå, något som skulle ge teknologins ägare Itis Holdings nya intäktsmöjligheter. Det vore exempelvis tekniskt möjligt att övervaka hur bilisterna håller fartgränserna.

### 5.4 Människokartor i Rom

I Rom pågår ett projekt där Italiens ledande teleoperatör, Telecom Italia, kontinuerligt skickar data om sina mobilkunders geografiska position till en programvara som framställer människokartor. Dessa uppdateras i realtid (hela tiden). Bakom det hela står ett forskningslaboratorium kallat Senseable City Laboratory vid det amerikanska universitetet Massachusetts Institute of Technology (MIT).

På människokartorna kan man med olika färger se hur människotätheten förändras minut för minut, inklusive information om vilken riktning människoströmmarna har. Exempelvis ska informationen enligt projektbeskrivningen kunna användas för att få reda på hur olika sociala grupper skiljer sig åt i sitt rörelsemönster, och hur turister från olika länder skiljer sig åt när det gäller val av platser att besöka. ”Man kan tänka sig att italienare vill vistas på de platser av staden som har högst koncentration

av skandinaviska turister”, säger projektets ledare Carlo Ratti till tidskriften *Technology Review*.

De data som presenteras på bildskärmarna är kollektiva och anonymiserade. Rent tekniskt skulle det dock gå att plocka fram vilka personer som döljer sig bakom de telefoner man följer, eftersom dessa data finns i teleoperatörens system.

Senseable City Laboratory driver eller har drivit liknande projekt i Florens, den österrikiska staden Graz och den spanska staden Zaragoza. Förhandlingar pågår med ytterligare ett antal städer.

*Några länkar:*

FlexiSpy: [www.flexispy.com](http://www.flexispy.com)

Itis Holdings: [www.itisholdings.com/cfvd.asp](http://www.itisholdings.com/cfvd.asp)

Senseable City Laboratory: <http://senseable.mit.edu>

## 6. Skrivare och kopiatorer som tjallar

Utan allmänhetens kännedom har myndigheter i många länder länge samarbetat med de stora tillverkarna av färgskrivare och färgkopiatorer om ett system med hemliga koder på utskrifterna. Koderna ger bland annat information om apparatens serienummer samt datum och tidpunkt för utskriften. Avsikten är att kunna spåra personen bakom papperet.

”Det är ett spår tillbaka till dig, som en bils nummerplåt”, säger Peter Crean, forskare på Xerox. ”Canon har utrustat alla sina färgmaskiner med kontrollteknologi för bekämpning av sedelförfalskning”, säger Anna McIntyre, som är PR-chef på Canon Europa.

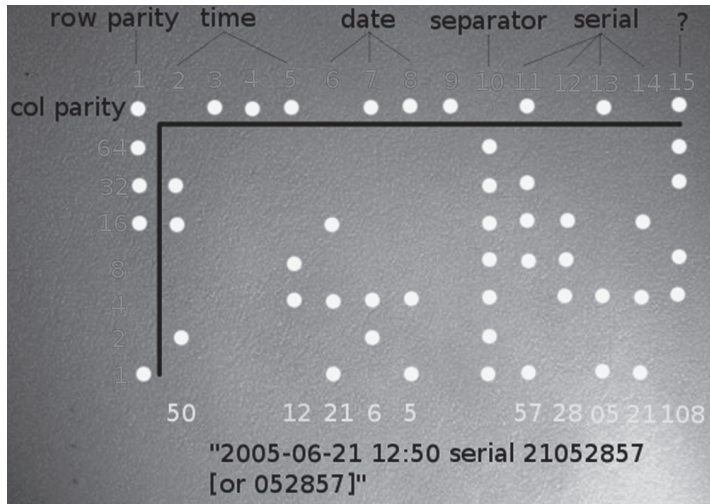
Just risken för att modern skrivar- och kopieringsutrustning används för sedelförfalskning uppges vara det ursprungliga skälet till att systemet med hemliga koder utvecklades. Dock har ändamålsglidningen sedan länge satt in, och koderna används nu regelmässigt av polisen mot all typ av brottslighet.

Integritetsombudsmannen har varit i kontakt med Statens Kriminaltekniska Laboratorium (SKL), som bekräftar att kodsystemet används även i Sverige. I övrigt är man ytterst ovillig att över huvud taget kommentera saken. ”Det är synd att det här har kommit ut”, var i stort sett det enda som SKL ville säga. Dock bekräftade sagesmannen att kodsystemet inte bara används för bekämpning av sedelförfalskning utan mot all typ av brottslighet.

När polisen begär information om ett pappers ursprung är skrivartillverkarna enligt samstämmiga källor mycket samarbetsvilliga. I en del fall har de själva detaljerad information om slutkunden – skrivarens ägare – i en kunddatabas, och läm-

nar då ut den informationen till polisen (sådan information kan tillverkare exempelvis bygga upp via registreringskort som köparna skickar in). Annars får polisen information om vilken återförsäljare skrivaren eller kopianer sålts till, och när. I många fall kan då polisen få information om konsumentens

Här visas de hemliga koder som många färgskrivare och färgkopiatorer förser utskriften med för att kunna identifiera personen bakom papperet. (Bild: Electronic Frontier Foundation)



identitet från butikens databas (som exempelvis upprätthålls för garantiändamål).

I en del fall kan koderna upptäckas med hjälp av ett förstoringsglas, gärna i kombination med blått ljus, exempelvis från en lysdiodsficklampa. En granskning som den amerikanska medborgarrättsorganisationen Electronic Frontier Foundation (EFF) har gjort visar att olika tillverkare har olika system. Hitills har man bara lyckats avkoda Xerox system.

Detta bygger på gula prickar som är arrangerade i en matris med 8 rader och 15 kolumner på en yta av ca 1,2 x 2,5 cm. Matrisen återkommer regelbundet på hela papperets yta, med ungefär 2,5 cm mellanrum, så att även en urklippt bit papper ska kunna spåras. På sin webbplats har EFF en programvara där allmänheten kan mata in värden från koderna på sina egna utskrifter, och få dem tolkade (se länk på nästa sida).

I Nederländerna har medierna uppmärksammat de hemliga skrivar- och kopiatorkoderna i samband med att det avslöjades att polisen använde dem för att nysta upp en härva av förfalskade tågbiljetter. Vid Purdue University i USA drivs forskning kring en metod för att förse även utskrifter från svartvita skrivare med osynliga koder (dock är det mycket som talar för att svartvita skrivare, likt svartvita TV-apparater, är på väg att försvinna från marknaden).

I Sverige har en produktchef på svenska Xerox, Jerker Larsson, uttalat sig för tidningen Computer Sweden om hemliga koder i skrivare och kopiatorer. Han säger att det ofta inte bara går att spåra vem som köpt en viss skrivare utan dessutom var den är uppställd. Det beror på att allt fler större skrivare har egen uppkoppling till internet och därmed eget IP-nummer (internetadress).

Oroande ur integritetsperspektiv är att det inte finns några lagar och regler som styr hur kodsystemet används eller vilka myndigheter som får ta del av spårningsinformationen och under vilka omständigheter. Det finns ingen insyn, ingen kontrollmekanism och inga rutiner för att informera dem som varit utsatta för spårning men visat sig vara oskyldiga. Risker är uppenbara att systemet exempelvis verkar hämmande på personer som vill tipsa media om missförhållanden, så kallade whistle blowers.

EFF om skrivarkoder: [www.eff.org/Privacy/printers](http://www.eff.org/Privacy/printers)

## 6.1 Programvaror får inbyggd polis

Efter att ovan ha studerat hur vissa apparater har börjat förse med en slags inbyggd polis kan vi konstatera att samma utveckling har inletts på programvarusidan. Det populära bildbehandlingsprogrammet Photoshop från Adobe har försetts med en funktion som gör det omöjligt att scanna in och redigera en bild på en sedel – åtminstone gäller det de viktigaste sedlarna, som känns igen av särskilda algoritmer i programvaran.

”Det är ett spår  
tillbaka till dig, som  
en bils nummerplåt”

*Peter Crean, seniorforskare på Xerox,  
om hemliga koder i utskrifter från kopiatorer och skrivare*

De polisiära funktionerna i Photoshop var till en början hemliga och förnekades av Adobe. Efter att ryktena blev allt intensivare bekräftade dock företaget slutligen existensen av dessa. Andra mjukvaruleverantörer har infört liknande funktionalitet. Exakt hur vanligt det är med polisiära funktioner i programvaror går inte att säga eftersom leverantörerna lägger locket på.

Man kan konstatera att det rent tekniskt vore möjligt att låta programvaran inte bara stoppa ett försök att bildbehandla en sedel utan även i det tysta rapportera det via internet till lämplig instans. Det har dock inte framkommit några indikationer på att ett sådant förfarande skulle förekomma.

Man kan tänka ytterligare ett steg framåt, och fundera över hur polisiära funktioner skulle kunna byggas in i helt andra programvaror. Ordbehandlingsprogram som Word skulle kunna spärra texter som beskriver tillverkning av bomber, och webbläsare som Internet Explorer skulle kunna spärra webbplatser som innehåller vissa ord.

Inte bara mjukvara, utan även hårdvara, har spärrar mot hantering av sedelbilder. Inte heller på detta område är omfattningen känd, men det har avslöjats att skrivartillverkaren Hewlett-Packard (H-P) i många av sina skrivare har byggt in en funktion som känner igen sedlar och spärrar utskrift. Enligt tidskriften Information Week har runt 90 procent av alla skrivare redan försetts med en sådan funktion, och enligt nyhetsbyrån AP är systemet också under införande i scannrar (så att dessa inte ska kunna scanna in sedlar).

Ett internationellt banksamarbete benämnt Central Bank Counterfeit Deterrence Group (CBCDG) har utvecklat de tekniska lösningar för hård- och mjukvara som förmodas utgöra grunden för åtminstone en del av de ovan beskrivna skyddsåtgärderna. Teknologin kallas Counterfeit Deterrence System (CDS), och erbjuds tillverkare av hård- och mjukvara på en basis som CBCDG kallar frivillig (se [www.rulesforuse.org](http://www.rulesforuse.org)).

## 7. Mönsterigenkänning

### – analys av totalt beteende

En människa som vandrar i skogen ser bara träd åt alla håll. Piloten i ett flygplan ovanför skogen, däremot, kan omedelbart få en överblick och enkelt se sådant som mönstret av vägar genom skogen.

Programvara för mönsterigenkänning fungerar enkelt uttryckt som flygplanet. I ena änden matar man in stora mängder data i ostrukturerad form, ofta från helt olika källor. Det är data som för en människa bara är ett virrvarr av ointressanta detaljer. I andra änden kommer det ut någon form av tydligt mönster, exempelvis i form av relationer mellan människor.

När personlig integritet i IT-samhället diskuteras hörs ofta kommentararen ”det gör väl ingenting att data om mig lagras någonstans, det är väl ändå ingen som orkar gå igenom det där informationsberget”. Nej, ingen människa orkar det, men programvaror för mönsterigenkänning är skapade för just detta.

Mönsterigenkänning används i många sammanhang, exempelvis i vetenskaplig forskning för att finna samband mellan olika provtagningar och i kommersiella sammanhang för att optimera marknadsföringen. Bland annat har teleoperatörer i många år använt mönsterigenkänning för att identifiera de kunder som man löper störst risk att förlora. Dessa får då särskilda förmåner för att förebygga avhopp.

På senare år, särskilt efter terrordåden den 11 september 2001, har användningen av mönsterigenkänning i brottsbekämpande och andra kontrollrelaterade syften ökat kraftigt.

”DecisionSite for Email Analysis kan hjälpa analytiker på myndigheter och i näringslivet med information om vem som pratar med vem via email och hur ofta”

*Ed Hart, tidigare ställföreträdande direktör  
på National Security Agency (NSA)*

Ledande i denna utveckling är som vanligt USA, där ”kri- get mot terrorismen” utgör murbräcka för en användning som egentligen är mycket bredare. Många satsningar finns, av varie- rande hemlighetsgrad, som syftar till att samla in människors elektroniska fotspår, tillämpa mönsterigenkänning och låta en programvara skriva ut en lista på suspekta personer.

Den ultimata mönsterigenkänningen planerades i USA efter attackerna mot World Trade Center under namnet Total Infor- mation Awareness. En särskild myndighet med namnet Infor- mation Awareness Office skapades, med uppgift att bygga upp det nämnda systemet som skulle gå igenom ”tusentals offentliga och kommersiella databaser” (även utanför USA). Information om sådant som inköp, ekonomiska transaktioner, resor, ring- ande, mejlande, surfande och mycket mer skulle gås igenom i jakt på människor med ett suspekt beteendemönster. Förenklat uttryckt: den som köper Koranen, reser till Afghanistan, köper dyra varor utan att få in någon regelbunden lön på banken och dessutom tar flygktioner är förmodligen en terrorist.

President Bush stödde projektet, men till slut blev det för kontroversiellt och kongressen ströp finansieringen. Mycket ty- der dock på att olika projekt i mindre skala syftar till att åstad- komma något liknande (se avsnittet om ADVISE i kapitel 10 om internetdammsugare).

Några andra exempel på tillämpning av mönsterigenkän- ning, utomlands och i Sverige:

- Det amerikanska Department of Homeland Security har uppdragit åt Pacific Northwest National Laboratory (PNNL) att utveckla en programvara som ska kunna ”nysta upp det komplexa nätet av relationer mellan människor, platser och händelser”. Bland annat ska data om e-mail, telefonsamtal, surfande och ekonomiska transaktioner användas som råvara. Forskningen ska resultera i en programvara kallad Starlight 3.0. ”I jakten på potentiella terrorister gäller det att hela tiden tolka innebörden i oräkneliga e-mail, webbsidor, finansiella transak- tioner och andra dokument”, säger Jim Thomas, som är direk-

tör på National Visualizations and Analytics Center (NVAC), den underavdelning till PNNL som utvecklar Starlight 3.0.

- Enligt den amerikanska tidskriften *Technology Review* kommer ovan nämnda Starlight 3.0 att användas på data som samlats in vid avlyssning av datornätverk och telefoner samt plöjande av offentliga databaser och privata finansiella transaktioner. Programvaran ska grafiskt visualisera relationer och samband mellan text, bilder, ljud och video. Samband ska sökas genom samtidig analys av upp till 40.000 dokument. Användaren av programvaran kommer inte bara att få sig grafiskt presenterat när varje händelse ägt rum, utan också var (rent geografiskt) och i närheten av vilka andra aktiviteter den ägt rum.

- PNNL utvecklar också en programvara kallad IN-SPIRE som ska tolka innebörden i stora mängder data, söka samtidigt i dokument på många språk och ”hitta det oväntade”.

- Det svenskägda företaget SpotFire, som faktiskt har den amerikanska underrättelsetjänsten CIA som delägare, har utvecklat en programvara vid namn ”DecisionSite for E-mail Analysis”. Den amerikanska avlyssningsmyndigheten National Security Agency (NSA) provar programvaran. En tidigare ställföreträdande direktör på NSA, Ed Hart, säger till amerikanska medier: ”DecisionSite for Email Analysis kan hjälpa analytiker på myndigheter och i näringslivet med information om vem som pratar med vem via email och hur ofta”.

- Det amerikanska Department of Homeland Security har införskaffat mönsterigenkänningsprogramvaran *Autonomy* för installation på 200.000 datorer hos 21 myndigheter, däribland FBI och CIA. På dessa myndigheter ska *Autonomy* analysera mycket stora mängder information, fördelad på ett stort antal databaser, och leta efter mönster, trender, nyckelpersoner och fraser som tyder på användning av kodord eller dolda budskap. Både text- video- och ljudfiler ska analyseras, och syftet är att producera en lista på misstänka personer (en så kallad ”watchlist”).

- Det svenska Skatteverket har införskaffat mönsterigenkännings- och visualiseringsprogramvaran ”Analyst’s Notebook” och databaslösningen ”iBase” från det brittiska företaget i2, som är en ledande leverantör till polis och underrättelsetjänst över hela världen. Syftet är att ”analysera komplexa samband mellan företag, människor, bankkonton och transaktioner”, enligt Stefan Danielsson på Skatteverket.

- Analyst’s Notebook används också av svensk polis, bland annat för att hitta samband mellan människor i stora mängder data från teleoperatörer om ringda samtal och för att lista ut verkliga namn på utländska gästarbetare som verkar i Sverige under olika identiteter.

- Det amerikanska skatteverket, Internal Revenue Service (IRS), tillämpar mönsterigenkänning på miljontals ansökningar om skatteåterbäring. Syftet är att hitta bedrägliga ansökningar. Här har svårigheterna med automatiska kontroller visat sig – amerikanska medier har avslöjat att två tredjedelar av de ansökningar som programvaran flaggat som suspekta har varit helt korrekta, vilket resulterat i att hundratusentals hederliga medborgare drabbats av frysta tillgångar.

- I Israel tillämpas mönsterigenkänning av polisen på hela befolkningen. Data om alla människor har lagts in i ett system, omfattande bland annat relationer släktingar emellan, födelse-data, bostadsadress och ägda bilar nu och förr. När ett brott har begåtts matar polisen in de ledtrådar man har, varpå programvaran levererar länkar, förbindelser och sådant som stämmer in på sökprofilen. Leverantör av systemet är svenska QlikTech.

- Den svenska varuhuskedjan Åhléns har införskaffat en programvara som med hjälp av mönsterigenkänning övervakar kassapersonalen. Syftet är att avslöja anställda som ägnar sig åt bedrägerier. Programvaran, som kommer från företaget Intel-liq, övervakar omständigheterna kring varje kassatransaktion, ”ser” helheten och slår larm när en kombination av vissa faktorer föreligger.

- Det amerikanska Department of Homeland Security an-

”[Syftet är att] analysera  
komplexa samband mellan  
företag, människor, bank-  
konton och transaktioner”

*Stefan Danielsson om Skatteverkets användning av  
mönsterigenkänningsprogramvara från brittiska i2*

vänder programvaran IxReveal från företaget Intelligenxia för att ”spåra meddelandetrådar online och ge svar på frågor som ännu inte blivit ställda”.

- Den amerikanska motsvarigheten till Riksrevisionen, General Accounting Office (GAO), skrev för en tid sedan i en rapport att av 128 undersökta myndigheter är det 52 som antingen använder eller planerar att använda mönsterigenkänning. Av de totalt 199 funna tillämpningarna ingår personuppgifter i 122. Enligt rapporten omfattas även ”utlänningar” (det vill säga icke-amerikaner) av mönsterigenkänningen.

## 7.1 Automatisk övervakning i Aten och EU-planer

Under de olympiska spelen i Aten 2004 provades ett mycket avancerat övervakningssystem, levererat av ett konsortium av internationella storföretag ledda av det San Diego-baserade företaget SAIC (Science Applications International Corp). Systemet inhämtade många typer av underlag, däribland

- Data om människors surfande, ringande och SMS-ande
- Innehåll i skickad epost (som automatlästes)
- Bilder från mer än 1.000 högupplösta övervakningskameror med infrarött mörkerseende
- Ljud som snappats upp från mikrofoner på övervakningskamerorna.

Bilder och ljud behandlades av programvaror som försökte tolka händelseförlopp. Sedan sammanställdes helheten av avancerade programvaror för mönsterigenkänning, huvudsakligen systemet Autonomy.

I ett så kallat green paper som EU-kommissionen presenterade i september 2006 uttrycker man intresse för data mining och automatisk texttolkning som verktyg för polis, tull och andra säkerhetsinstanser. Kommissionen skriver bland annat: ”Moderna verktyg för data mining och textanalys [”text mining”] existerar. Den teknologin kan vara behjälplig för att extrahera relevant information ur enorma mängder dokument”.

”Autonomy kommer att användas för att automatisera analys och leverans av meddelanden, oberoende av deras form och lagringsplats, och för att leta efter potentiellt suspekt aktivitet. Enorma mängder data, både på engelska och grekiska, kommer att analyseras automatiskt under de olympiska spelen”.

*Företaget Autonomy i ett uttalande inför Aten-OS enligt nyhetstjänsten CNET*

I EU-dokumentet nämns bland annat ”innehållsbaserad klassificering” och ”automatisk informationsanalys tvärs över olika datakällor” som intressanta metodiker, och ett resonemang förs där man konstaterar att om sådan teknik används på eposttrafik måste det ske i enlighet med lagen. Vidare presenteras tankar på möjligheten att skapa ett ”centre of excellence” på EU-nivå för data mining och automatisk textanalys, alternativt att skapa flera regionala centra. Dessa, så resoneras det, skulle kunna hjälpa polis och andra myndigheter tvärs över nationsgränserna med automatisk textanalys. EU-dokumentet heter ”Green paper on detection technologies in the work of law enforcement, customs and other security authorities.”

*Några länkar:*

Aungate: [www.aungate.com](http://www.aungate.com)

Autonomy: [www.autonomy.com](http://www.autonomy.com)

Basis Technology: [www.basistech.com](http://www.basistech.com)

i2: [www.i2.co.uk](http://www.i2.co.uk)

Intelligenxia: [www.intelligenxia.com](http://www.intelligenxia.com)

Intelliq: [www.intelliq.com](http://www.intelliq.com)

NSA: [www.nsa.gov](http://www.nsa.gov)

Qliktech: [www.qliktech.com](http://www.qliktech.com)

## 8. Umgängesanalys och automatisk kompisdetektering

Umgängeskretsanalys, på engelska kallat ”social network analysis”, är ett specialfall av mönsterigenkänning. Det innebär att programvaror analyserar kontakter mellan människor, ritar umgängeskartor och drar slutsatser om relationer och flöden. Som råvara kan i princip alla typer av data användas som säger något om människors umgänge, exempelvis telefon- och epost-data, ekonomiska transaktioner och data över resor/besök.

Två forskare vid namn David Krackhardt och Valdis Krebs har utvecklat en metodik för umgängesanalys där en programvara ritar en karta kallad ”kite network”. Tre faktorer i människors umgänge vägs därvid in:

- Aktivitet. Med hur många andra personer, och hur ofta, har den här personen kontakt?
- ”Mellanskap”. I vilken utsträckning utgör den här personen en brobyggare mellan olika grupperingar?
- Närhet. I vilken utsträckning befinner sig den här personen nära andra, i kontaktväg räknat?

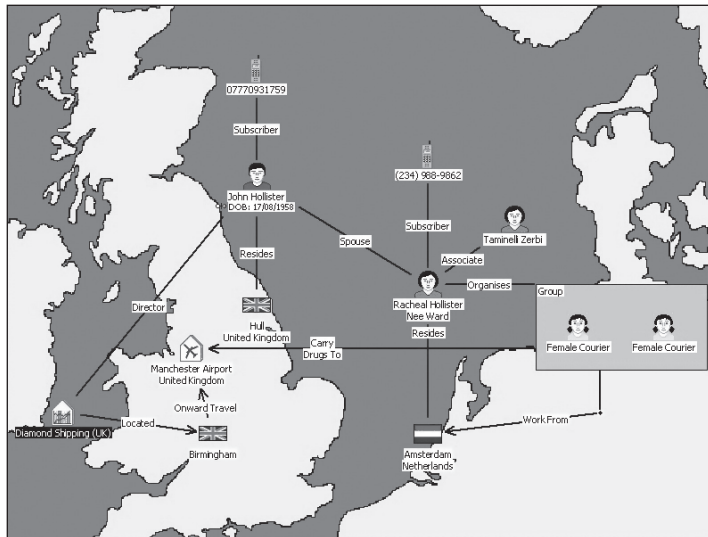
Existensen av faktorerna mellanskap och närhet antyder ett viktigt faktum: det är långtifrån säkert att den person som ser ut att sitta i centrum av ett nätverk för att han eller hon har kontakt med flest personer har den viktigaste rollen.

När de amerikanska styrkorna i Irak letade efter Saddam Hussein tillämpade de umgängesanalys. Med hjälp av ett ”länkdiagram” över den forne diktatorns släkt- och stamkon-

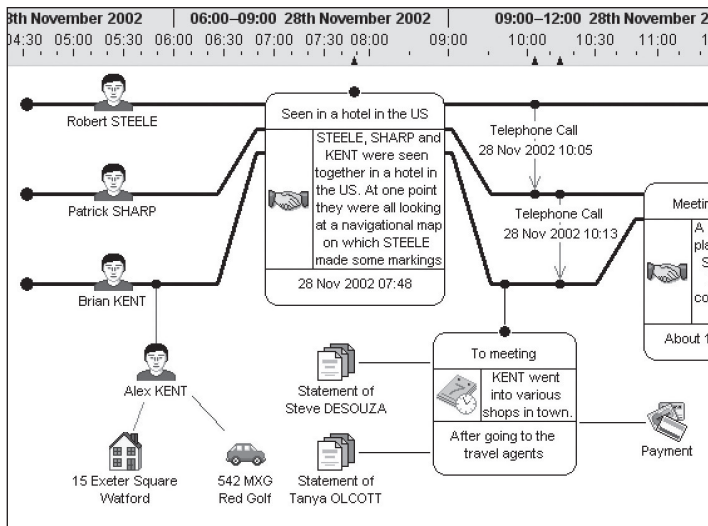
takter kunde de dra slutsatser om var någonstans det var mest ändamålsenligt att leta.

Se även kapitel 10 om internetdammsugare, där umgängesanalyser behandlas ur ett annat perspektiv.

Mönsterigenkänning med programvara från i2, där olika former av kontaktdata sätts samman till en relationskarta. (Bild: www.i2.co.uk)



Här har en programvara från i2 gjort en tidslinje av händelser upptäckta med mönsterigenkänning. (Bild: www.i2.co.uk)



”Att förstå samband mellan människor, organisationer, platser och föremål, genom att använda analys av socialt beteende och andra teknologier, är nödvändig för att gå från enkel data mining till omfattande kunskapsupp-täckt i databaser ”

*Dr. Joseph Kielman, chef, Threat and Vulnerability, Testing and Assessment Portfolio, Department of Homeland Security*

## 9. Automatisk övervakning av våra banktransaktioner

Ett annat specialfall av mönsterigenkänning är automatisk genomgång av banktransaktioner, så kallad Anti Money Laundering (AML), på jakt efter suspekt verksamhet. Programvaror för detta, så kallade AML-system, installeras i banker och andra finansiella institutioner där de går igenom samtliga transaktioner på jakt efter ett mönster av omständigheter som är programmerat som suspekt.

Amerikanska myndigheter driver på internationellt för ett brett införande av AML-system. Så här beskrivs tillvägagångssättet av en AML-leverantör i en artikel i tidskriften Wired:

*Programvaran kommer ihåg att en viss kund är en 30-årig ingenjör som avlönas den femte varje månad. Den studerar profilerna för andra ingenjörer i samma åldersgrupp och bygger ett mönster baserat på gemensamma drag som exempelvis lönens månatliga periodicitet. Om en annan kund säger att han är ingenjör och får insättningar på sitt konto varje vecka kommer programvaran att visa röd flagga. Han är suspekt.*

AML-system har också automatisk igenkänning av bedrägeriförsök, geografiskt betingade larm, larm baserat på ekonomiska relationer med svartlistade personer eller företag, automatisk upptäckt av dolda relationer mellan människor, analys av en kunds transaktionsmönster, profilering av bankens anställda för personalavdelningens räkning och en hel del annat. AML-systemsleverantören SDG Software skriver exempelvis att deras system gör det möjligt att ”kartlägga kundens liv och affärshändelser”.

”Det är mycket möjligt att systemet för det mesta inte kommer att fånga pengatvättare, eftersom dessa är försiktiga, utan vanliga människor.”

*En banktjänsteman uttalar sig om AML-systemet i tidskriften Wired.*

Det är inte säkert att de riktigt grova ekonomiska brottslingarna blir de som påverkas mest av AML-systemens införande. Suheim Sheikh på SDG Software säger:

*AML-system kommer att förändra banking för alltid. Myndigheter runt om i hela världen kommer att ha ögonen på bankkunder. Eftersom programvaran kan övervaka så många konton och så många transaktioner kommer alla slags människor att bli kontrollerade, även de som i teorin är helt vanliga människor. Per definition blir det så att inte bara pengatvätt utan allting som strider mot lagen, såsom undanhållande av skatt, blir svårt att dölja.*

Tidskriften Wired citerar en banktjänsteman som säger om AML-system: "Det är mycket möjligt att systemet för det mesta inte kommer att fånga pengatvättare, eftersom dessa är försiktiga, utan vanliga människor." Norge ligger i den internationella spjutspetsen när det gäller AML-system. Sedan den 1 januari 2005 är banker enligt lag skyldiga att ha ett sådant. Enligt en artikel på den norska webbplatsen N24.no i augusti 2006 hade då 130 norska banker och finansiella institutioner installerat AML-system. Sedan starten för drygt halvannat år sedan hade systemen i augusti 2006 resulterat i sammanlagt 28.500 larm, av vilka cirka 400 bedömdes ha tillräcklig substans för att överlämnas till den norska polisens ekobrottsrotel.

Användning av AML-system utgör ett steg på vägen mot "automated law enforcement" – automatisk polis – ett koncept som i vissa kretsar utmålas som framtidens melodi. Innebörden är att polisen låter programvaror ständigt gå igenom människors elektroniska fotspår på jakt efter lagöverträdelser.

*Exempel på leverantörer:*

EDB Business Partner: [www.edb.com](http://www.edb.com)

SAS Institute: [www.sas.com/industry/fsi/aml/](http://www.sas.com/industry/fsi/aml/)

SDG Software: [www.sdgsoftware.com](http://www.sdgsoftware.com)

## 10. Internetdammsugare patrullerar nätet – även i Sverige

Med internetdammsugare avses programvaror eller system som automatiskt ”patrullerar” internet, samlar in information samt i många fall även analyserar denna och drar slutsatser. Det som ”dammsugs” kan vara allt ifrån människors personliga intressen till journalisters syn på USA. Internetdammsugare utvecklas nu i bland annat USA och Sverige.

Ett exempel är det amerikanska säkerhetsdepartementets (Department of Homeland Security) system för övervakning av befolkningen genom insamling av elektroniska fotspår, som nu är under uppbyggnad. Programvaror ska samla in sådant som information från webbplatser, inlägg på bloggar och epost-meddelanden. Sedan ska mönsterigenkänning sättas in för att automatiskt hitta människor med ett suspekt beteende. Systemet kallas ADVISE (Analysis, Dissemination, Visualization, Insight and Semantic Enhancement).

ADVISE ska samla in mängder med elektroniskt tillgänglig information, samköra den med polisdatabaser och information från underrättelsetjänster, och sedan lagra ”samband” i form av vad som kallas ”entities” (ungefär ”begrepp”). Informationen från systemet ska få en omfattande spridning inom USA – alla säkerhetsfunktioner på federal nivå, delstatsnivå, lokal nivå och i den privata sektorn kommer att få ta del av informationen i realtid.

”Att förstå samband mellan människor, organisationer, platser och föremål, genom att använda analys av socialt beteende

och andra teknologier, är nödvändig”, skriver dr Joseph Kielman från Department of Homeland Security i en rapport.

Den amerikanska avlyssningsmyndigheten National Security Agency (NSA) ser ut att hysa planer på utveckla internetdammsugare som automatiskt ska masskartlägga människor genom att gå igenom personlig information som de har lagt ut om sig själva på sajter för socialt nätverkande. Den vetenskapliga tidskriften *New Scientist* rapporterar att NSA finansierar forskning om just detta.

På sajter som exempelvis MySpace (internationell) och Lunarstorm (svensk, för ungdomar) lägger människor frivilligt ut stora mängder information om sig själva, information som ofta kan vara både ingående och känslig. Denna kan ibland användas för att dra slutsatser om sådant som umgängeskrets, intressen, politiska åsikter, intentioner, hälsotillstånd och mycket mer. Precis detta ska göras av NSA:s internetdammsugare, genom så kallad ”profilering” (människoprofilering), om myndigheten förverkligar det man nu forskar om.

En grupp forskare från University of Georgia och University of Maryland i USA har publicerat en rapport med titeln ”Semantic Analytics on Social Networks”. Den beskriver hur personlig information från communities och andra webbplatser för socialt nätverkande ska kunna användas för att automatiskt kartlägga människor. I rapporten står det att forskningen delfinansierats av Advanced Research Development Activity (ARDA). Denna organisation har som roll att kanalisera pengar från NSA till forskning som ”kan lösa amerikansk underättelsetjänsts mest kritiska problem”. ARDA bytte för övrigt nyligen namn till Disruptive Technology Office (DTO).

Den automatiska masskartläggning av människor som NSA ser ut att planera underlättas av en teknisk förändring av internet som genomförs om några år. Det handlar om ”Semantic Web”, ett nytt sätt att strukturera informationen på nätet så att den kan tolkas maskinellt på ett enhetligt sätt. Så här beskrivs innebörden av Semantic Web av tidskriften *New Sci-*

entist: ”Det betyder att [en dator] kan fråga en webbplats saker som den inte kunde fråga förut, eller genomföra beräkningar på data som webbplatsen innehåller. I en hälsodeklaration, till exempel, kommer en hjärtattack att ha samma semantiska etikett som dess mera tekniska beskrivning ’myocardial infarkt’. Tidigare hade de två termerna sett ut som olika sjukdomar. Varje slags numerisk information, som inflationstakten eller antalet trafikdödade människor, får också sina etiketter.”

Amerikansk masskartläggning av människor via webbsajter passar in i ett sedan länge tydligt mönster. Det har exempelvis relativt nyligen avslöjats att NSA har övervakat 200.000.000 (200 miljoner) människors ringande, förmodligen för att kartlägga deras sociala nätverk. Den informationen skulle väsentligt kunna kompletteras och fördjupas med den kunskap om människors livsstil och personliga förhållanden som finns att hämta på webbplatser för socialt nätverkande. Som stöd i analysen används redan teknologier som exempelvis mönsterigenkänning för att hitta intressanta detaljer i enorma informationsberg och för att identifiera mönster och sammanhang.

Ett annat exempel på internetdammsugare är en programvara som ska utvecklas av forskare vid Rensselaer Polytechnic Institute i USA. Programvaran ska automatiskt övervaka så kallade chatrum på internet, det vill säga webbplatser där människor kommunicerar med varandra i realtid. Målet är automatisk kartläggning av relationer och grupperingar – alltså svar på frågan ”vem känner vem?”. Projektet finansieras av National Science Foundation, som är underställt den amerikanska regeringen.

I oktober 2006 avslöjades det att amerikanska Department of Homeland Security tillsammans med ett konsortium av framstående amerikanska universitet ska utveckla en programvara som automatiskt ska övervaka omvärldens syn på USA. En internetdammsugare ska kontinuerligt gå igenom webbplatser runtom i världen och automatläsa det som skrivs om USA. Sedan ska programvaror med texttolkning ta vid och bedöma vilken grundläggande USA-syn som kommer fram i respektive

artikel. Resultatet ska sedan automatiskt föras in i en databas där inte bara olika medier (exempelvis tidningar) får varsin profil beroende på sin USA-syn utan även enskilda journalister.

## 10.1 Svenska skatteverket skaffar dammsugare

Det svenska Skatteverket kommer förmodligen att skaffa internetdammsugare. Dessa ska självständigt leta efter webbplatser där varor bjuds ut till försäljning av privatpersoner, såsom Blocket. Annonserna ska hämtas från webbplatserna, och sedan ska en annan programvara analysera dem på jakt efter personer som bedriver yrkesmässig handel med varor under täckmantel som privatpersoner. Det berättar Dag Hardyson, Skatteverkets rikssamordnare för internethandel, för integritetsombudsmannen.

Utvecklingen av internetdammsugare avsedda för jakt på skattebrottslingar samordnas med andra EU-länder inom ett samarbete som kallas "Internet monitoring and search tools". Det handlar om två typer av programvaror, dels sådana som står för själva dammsugandet av webbplatser, dels sådana som därefter genomför texttolkning och mönsterigenkänning.

Dag Hardyson uppger att den holländska spindelprogramvaran Xenon är intressant och kan komma att köpas in av Skatteverket. Beträffande textanalys nämner han att företaget Zylab har en mycket kraftfull produkt. Skatteverket har också utvecklat en egen programvara som heter ECyes (ska uttalas "easy eyes").

Se även kapitlet om mönsterigenkänning.

*Länkar för vidare läsning:*

ARDA (länk till en speglad kopia av webbplatsen nedtagen 2005):

<http://web.archive.org/web/20050305225739/www.ic-arda.org/main.htm>

Lunarstorm: [www.lunarstorm.se](http://www.lunarstorm.se)

MySpace: [www.myspace.com](http://www.myspace.com)

NSA: [www.nsa.gov](http://www.nsa.gov)

Rapport: [www2006.org/programme/files/pdf/4068.pdf](http://www2006.org/programme/files/pdf/4068.pdf)

Zylab: [www.zylab.com](http://www.zylab.com)

”Amerikanska myndigheter utvecklar ett väldigt data-system som kan samla in enorma mängder information och, genom att länka samman helt olika typer av information från bloggar och e-post till statliga register och underrättelserapporter, söka efter mönster som tyder på terroristaktivitet”

*The Christian Science Monitor*  
*om övervakningssystemet ADVISE*

# 11. Andra kreativa metoder för kontroll och övervakning

## 11.1 Kommunikationsdammsugare

Svensk polis föreslås få tillgång till ett hemligt verktyg, hittills bara använt av Säpo, för att registrera samtliga elektroniska kommunikationsapparater som används inom ett visst fysiskt område (som exempelvis ett kvarter). Verktöget ger en helhetsbild av vilka fasta telefoner, mobiltelefoner, internetanslutna datorer och andra ”teleadresser” som för stunden är i bruk i området. Detta föreslås av den statliga utredningen Beredningen för rättsväsendets utveckling (BRU).

## 11.2 Flygande övervakningskameror

I USA har man börjat testa övervakningskameror monterade i obemannade flygplan, så kallade droner eller UAV (Unmanned Aerial Vehicle). Dessa har använts i stor skala i kriget i Afghanistan och Irak, och nu övervägs civil användning. Pionjär är Los Angeles county, som överväger att inhandla 20 kameradroner. Flygplanen väger ungefär 2,5 kg, kan sända videobilder upp till 80 meter och betingar ett styckpris på 20-30.000 dollar. Även polisen i Storbritannien överväger att införskaffa övervakningskameror i obemannade flygplan, som är tänkta att flyga över problemområden och ”identifiera antisocialt beteende”.

### 11.3 Nakenscanner - med eller utan fikonlöv

Både i USA och Storbritannien har en ny apparat testats i flygplatsers säkerhetskontroll – en nakenscanner. Apparaten mäter reflekterade röntgenstrålar, vilket får till följd att kläderna i praktiken skalas bort. På bildskärmen visas människokroppen naken. Fördelen är att eventuella dolda vapen syns mycket tydligt. Av integritetsskäl har nakenscannern ännu inte tagits i skarp drift. Tillverkarna försöker utveckla elektroniska fikonlöv, det vill säga en funktion för att på bildskärmen maskera känsliga kroppsdelar.

### 11.4 Myndigheterna fjärrstyr våra bilar

Storebror verkar inte vara helt nöjd med att via satellitpositionering (GPS) kunna hålla reda på varje bils läge och fart, sekund för sekund. Undersåtarna kan ju faktiskt trotsa övervakningen och köra för fort i alla fall. Medlet mot detta är Automatic Speed Adaption, som utgör den mest avancerade formen av Intelligent Speed Adaption (ISA).

Så här fungerar det: En svart låda i bilen innehåller en GPS-navigatör, och skickar via mobiltelefonnätet hela tiden information till en övervakningscentral om var bilen befinner sig och hur fort den kör. I centralen matchas den informationen mot en databas med en digital karta, där fartgränsen för varje vägsträcka är inlagd. Om gällande fartgräns överskrids skickas en signal via mobiltelefonnätet tillbaka till bilen, där en ventil stryper motorns bränsletillförsel.

I London har Transport for London, som kollektivtrafiken kallas, inlett förberedelser för ett pilotprojekt där sådan fjärrstyrning ska provas i ett tiotal fordon. Enligt BBC har den brittiska regeringen uttalat sig i positiva ordalag om att på sikt införa teknologin på bred front, även för privatbilar. Inom EU har ett utvecklingsprojekt kallat ATESSST som innehåller denna teknologi dragits igång.

Mera information om bilövervakning finns i Den Nya Valfärdens skrift "Med storebror i baksätet" (2006).

### 11.5 Kreativa sätt att bekämpa anonymiteten

Det utvecklas olika kreativa teknologier för att råda bot på det "problem" som består i att människor ännu så länge har vissa möjligheter att utföra handlingar i vardagen utan att identifiera sig. Här är några av dem.

*Datorklockan som fingeravtryck.* Tadayoshi Kohno, doktorand vid University of California, har utvecklat ett sätt att på distans känna igen en dator på internet. Metoden utnyttjar det faktum att varje dator har mycket små avvikelser i den inbyggda klocka som styr mikroprocessorn, och denna information blir i praktiken ett osynligt "fingeravtryck". Indirekt kan det gå att identifiera människor genom att känna igen datorn, eftersom "fingeravtrycket" vars användare man vill identifiera kan förekomma i ett helt annat sammanhang där personen har valt att identifiera sig (såsom en webbplats för socialt nätverkande). Klockinformationen som innehåller datorns "fingeravtryck" skickas rutinmässigt med vid all datakommunikation över internet.

*TV-vanor.* En forskare vid University of Birmingham, Martin Russell, har utvecklat en metod för att identifiera människor via deras TV-tittande. Om en persons TV-vanor är kända kan han eller hon med 82 procents sannolikhet identifieras via tittandet.

*Tangentbordsrytm.* Det är också möjligt att använda rytmen i skrivandet på ett tangentbord för att identifiera en person, under förutsättning att man har en sedan tidigare känd rytm att jämföra med.

*SMS-språkanalys.* Varje människa har sin egen stil och sitt eget karakteristiska mönster när de skriver SMS-meddelanden. Detta gäller inte minst valet av förkortningar. Dessa skillnader kan användas för att identifiera människan bakom ett SMS-meddelande, tror forskare från universitetet i Leicester i Storbritannien.

*Lukt.* Vid det amerikanska University of Buffalo försöker man forska fram en teknologi för att med hjälp av “elektroniska näsor” identifiera förbipasserande människor med hjälp av deras unika kroppslukt. Forskningen befinner sig i ett tidigt skede och teknologin har långt kvar till sitt eventuella genombrott.

*Mönsterigenkänning.* Det kan också gå att identifiera en person genom mönsterigenkänning. En upphittad mobiltelefon, exempelvis, är många gånger inte så anonym som man kan tro även om SIM-kortet är ett anonymt kontaktkort. Om loggfilen med tidigare uppringda nummer ligger kvar i telefonen kan det gå att matcha ringprofilen med teleoperatörens data om namngivna kunder. En matchning i ringprofilen (i huvudsak att samma nummer är uppringda enligt ett liknande mönster vad gäller dag och tid) visar att det med mycket stor sannolikhet är samma person som står bakom. Om loggfilen i telefonen inte finns kvar kan samma matchning göras ändå, eftersom ringandet och SMS-andet har registrerats och lagrats hos teleoperatören enligt de nya reglerna om obligatorisk trafikdatalagring.

*Geografisk spårning 1.* Den amerikanska avlyssningsmyndigheten National Security Agency (NSA) har fått patent på en teknologi som via människors internetanvändning ska kunna spåra deras geografiska position. Teknologin bygger på mätning på många ställen av de fördröjningar som uppstår när information transporteras genom routrar och switchar på internet.

*Geografisk spårning 2.* Företag som IBM och MetaCarta har utvecklat system som söker genom textdokument, såsom epost-meddelanden, på jakt efter ord som kan ge ledtrådar om var meddelandets avsändare och/eller mottagare befinner sig geografiskt.

*Länkar:*

MetaCarta: [www.metacarta.com](http://www.metacarta.com)

NSA: [www.nsa.gov](http://www.nsa.gov)

## 12. Övervakning – bra eller dåligt?

*Efter att ha gått igenom denna kakafoni av högteknologiska övervakningsinitiativ kanske många läsare känner oro över utvecklingen och upprördhet över samhällets ägarattityd gentemot medborgarna. Andra läsare, däremot, kanske välkomnar ökad övervakning mot bakgrund av den verklighet av våldsbrott, terrorism och organiserad brottslighet som så hotfull tornar upp sig alldeles utanför ytterdörren.*

Integritetsombudsmannen och Den Nya Valfärden intar inte någon överslätande attityd gentemot brottslighet. Vi säger heller inte generellt nej till övervakning. Självklart behövs en viss övervakning i ett civiliserat samhälle. Problemet är balansen.

Det har alltid funnits, och kommer alltid att finnas, en motsättning mellan personlig integritet å ena sidan och bekämpning av brott och fusk å den andra sidan. Personlig integritet kan aldrig bli total så länge vi människor ska leva tillsammans i ett samhälle. Ett land helt utan övervakning skulle snart urarta i anarki, och det vore förmodligen farligt att över huvud taget gå utanför dörren. Noll övervakning är alltså definitivt inte något bra alternativ.

Den motsatta ändpunkten på skalan, det totala övervakningssamhället à la 1984, har på motsvarande sätt länge betraktats som en skräckvision. Alltså har demokratier legat ungefär på mitten av skalan, och om vi skulle nöja oss med det skulle den här varningsrapporten inte behövas. Problemet är att vi har satt oss i rörelse åt övervakningshället till. En kombination av drivkrafter gör att gränserna för hur långtgående övervakning som anses nödvändig, liksom gränserna för vad allmänheten

accepterar, förflyttar sig. Och det handlar inte om någon engångsförflyttning, utan om en kontinuerlig rörelse längs skalan utan tecken till uppbromsning.

Resultatet blir att den känsliga maktbalansen mellan stat och medborgare i rask takt förskjuts till statens fördel. Medborgarna förvandlas alltmer från ägare av staten till undersåtar. Och DET är något som integritetsombudsmannen och Den Nya Valfärden opponerar sig mot.

Det är inte lätt att formulera en exakt definition på hur långtgående övervakning som är lämplig i ett angenämt samhälle. En grundprincip enligt integritetsombudsmannens sätt att se saken är dock att dra en rågång mellan övervakning av brottsmisstänkta personer och övervakning av alla medborgare i förebyggande syfte. Självklart ska polis och andra rättsvårdande instanser ägna sig åt ingående övervakning av personer som misstänks för exempelvis terrorism, mord och grov organiserad brottslighet. Men en medborgare som inte är misstänkt för något brott måste å andra sidan slippa få sitt privatliv övervakat och analyserat av myndighetsrepresentanter.

Riskerna för medborgarna med insamling av elektroniska fotspår och annan övervakning är högst reella:

- Känslig information om privatlivet kan hamna i orätta händer, eftersom alla databaser läcker (inklusive polisens). De läcker ganska ofta, ganska mycket och på olika vis. Det kan åsamka individer stor skada.

- Medvetenhet om att elektroniska fotspår samlas in och används för profilering och svartlistning kan göra att människor drar sig för att köpa vissa saker, kontakta vissa personer, besöka vissa platser eller surfa till vissa sajter (för att ta några exempel). Det försämrar livskvaliteten och utgör ytterst en fara för demokratin eftersom informationsinhämtning utgör demokratin livsnerv.

- Ändamålsglidning kan göra att insamlade personuppgifter med tiden börjar användas på ännu mera påträngande sätt

än vad som utlovats från början (betänk den ändamålsglidning som drabbat PKU-registret).

- Staten får en hållhake på varje medborgare, vilket inte är önskvärt även om den svenska staten fortsätter att vara god och demokratisk (vilket inte är säkert).

När medborgarna försöker skydda sig mot övervakning och dess skadeeffekter står en företeelse i centrum: Anonymiteten. Berövade vår möjlighet att agera anonymt i vardagen står vi nakna och utlämnade inför överheten. Anonymiteten utgör ett oerhört viktigt socialt skydd som vi länge har tagit för givet och därför inte värderar. I IT-åldern står anonymiteten inför hot om utrotning, och är det en enda sak vi medborgare bör stå upp för så är det möjligheten och rätten att agera anonymt i vardagen.

Vi måste inse att den digitala revolutionen under lång tid kommer att erbjuda alltmer avancerade och påträngande övervakningsmetoder. Antingen säger vi förr eller senare nej till att fortsätta glidningen längs skalan mot ett 1984-samhälle, även om det innebär att brottsbekämpningen inte är riktigt lika maximalt supereffektiv som den skulle kunna vara, eller också accepterar vi att 1984 är oundvikligt.

I debatten får man ibland intrycket att samhällets nyttokalkyl är det enda som ska styra graden av övervakning av medborgarna. Men det handlar inte bara om en nyttokalkyl. Man kan, och bör, också närma sig saken från ett helt annat perspektiv. Vi är människor och har därmed mänskliga rättigheter. Dessa är inskrivna i bland annat FN:s deklaration om mänskliga rättigheter. Där stadgas det, i artikel 12, att vi har rätt att ha vårt privatliv för oss själva. Utan att behöva motivera det.

Personlig integritet är som syre – vi värderar den först när den saknas.



**Går vi mot en värld där automatiska öron** massavlyssnar telefonsamtal, översätter dem vid behov och producerar skriftliga sammanfattningar? Där alla människor blir automatiskt identifierade i gathörnen (och loggade i databaser) av övervakningskameror med digital ansiktsigenkänning? Där internetdammsugare automatiskt gör personlighetsprofiler på oss alla utgående från information som vi i förtroende har lämnat om oss själva på olika internetsajter? Där myndigheterna minut för minut vet var varje medborgare befinner sig?

Den som studerar vad övervaknings- och säkerhetsbranscherna håller på med upptäcker snabbt att svaret är – förmodligen! Om vi inte protesterar!

Pär Ström är integritetsombudsman vid Den Nya Valfärden.

den  
nya  
välfärden

Box 5625, 114 86 Stockholm | tel 08-545 038 10  
[www.dnv.se](http://www.dnv.se) | [integritetsombudsmannen@dnv.se](mailto:integritetsombudsmannen@dnv.se)