LUND UNIVERSITY

Kameraövervakningens effekter – vad vet vi och vad vet vi inte?

Weaver, Benjamin; Lahtinen, Markus

2015

Document Version:
Förlagets slutgiltiga version

Link to publication

Citation for published version (APA):
Weaver, B., & Lahtinen, M. (2015). *Kameraövervakningens effekter – vad vet vi och vad vet vi inte?* (Övervakning och integritet – en antologi). Myndigheten för samhällsskydd och beredskap.
https://www.svet.lu.se/tobbe-petterson/publication/c2fe5be0-e7e4-4201-93e5-107633a5a758

Total number of authors:
2

Creative Commons License:
Annan

General rights
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

Övervakning och integritet
- en antologi

Innehåll

Introduktion *Tobbe Petterson* **5**

Ett svenskt perspektiv på contextual integrity *Julia Branting* **7**
Inledning 7
Privacy – ett rörigt och komplext ämne 7
Personlig integritet – ett begrepp utan definition 9
En fråga om balans? 9
Helen Nissenbaum och contextual integrity 11
Contextual integrity i svenskt perspektiv – två fallstudier 13
ITS27 – automatiserad utlämning av trafikuppgifter 14
Analys av ITS27-dokumentet 16
Hemlig dataavläsning – legala spiontrojaner 20
Analys av förslaget om hemlig dataavläsning 21
Inte bara balans 25
Referenser 28

Övervakning av metadata som spelplan för rättsliga principkonflikter *Markus Naarttijärvi* **35**
Metadata i rätten 35
Bakgrund *35*
Tre tendenser *36*
Mer framåtblickande myndighet, mindre återblickande domstol *39*
Den individualiserade misstankens generalisering – du är ditt mönster *42*
En rättslig reaktion 44
Nya förutsättningar för den rättsliga analysen *44*
Digital Rights Ireland – ett rättsligt trendbrott? *45*
Utveckling på FN-nivå *46*
Kommande fall *47*
Slutsatser och analys 48
En principiell kollision *48*
Ett kommande vägskäl *50*
Referenser 51

Nya aktörer och ny teknik i kontrollandskapet *Janne Flyghed* **55**
Några exempel på teknikens expansion 55
Radio Frequency Identification (RFID) 57
Vad ska övervakas och kontrolleras? 58
Varför denna expansion? 59
Privata brottsutredningar 61
Effektiv diskretion 63
Staten tappar kontroll? 65
Integriteten och den rena mjölpåsens dilemma 66
Referenser 68

En virtuell kompis *Petrus Bolin* **70**
Syfte, payback och positiva rånförebyggande effekter 72
Övriga effekter av CCTV installation i butik 77
En virtuell kompis 78

Säkerhetskultur och kollektiv acceptans - en säkerhetschefs betraktelse över hur samhället kan förhålla sig till kameraövervakning inför behovet av en ökad trygghet *Per Gustafson* **80**
Tidigare tillståndsbedömningar enligt lag om allmän kameraövervakning 80
Kameror och dess eventuella bevisvärde 81
Kan det finnas en acceptans? 82
Skyltar, kameror och dess effekter för säkerhetskultur 83
Hur ska en god säkerhetskultur uppnås? 84
Hur ska en positiv acceptans uppnås? 86
En modell för sekuritetsacceptans *86*
Slutsats 87
Referenser 88

Kameraövervakningens effekter – vad vet vi och vad vet vi inte? *Benjamin Weaver och Markus Lahtinen* **89**
Inledning 89
En övertro på kameraövervakningens effekter? 90
Stort mediegenomslag 90
Forskning om kameraövervakning 91
Storbritannien är en unik kontext för allmän kameraövervakning 92
De brittiska CCTV-programmen *92*
Storbritannien och analog videoteknologi *93*
Problemet med att använda den brittiska forskningen på kameraövervakning som mall 94
Övervakning av stadskärnor är ett specialfall *94*
De flesta kamerasystem som övervakar allmän plats är privata *94*
Få likheter mellan situationen Sverige och Storbritannien *95*
Forskning saknas på effekterna på brottsuppklarning 95
Erfarenheter från Storbritannien när det gäller brottsuppklaring *95*
Brottsuppklaring och bristande rutiner och processer *96*
Erfarenhet av brottsuppklaring med hjälp av kameraövervakning i Sverige *97*
Integritetsaspekten vid kameraövervakning 98
Integritetsrisker vid kameraövervakning *98*
Skillnader mellan rättspraxis i Sverige och på EU-nivå *99*
Kameraövervakningslagen och Ipred- och FRA-lagstiftningen *99*
Allmänhetens inställning till kameraövervakning 100
Slutsatser 101
Ny forskning behövs *102*
Referenser 103

Måste vi ta det onda med det goda eller går det att välja? Om övervakning som samhällsproblem *Håkan Hydén och Marcin de Kaminski* **106**
Det senmoderna samhällets regleringsproblem 106
Intersystemkonflikter – dubbla normativa budskap 109
Övervakning som samhällsfenomen 111
Övervakning som postindustriellt problem 114
Referenser 118

Demokratins skydd eller självmål? En sammanfattande diskussion
Wilhelm Agrell **119**
Rent mjöl i fel påse? Kontroversen kring metadata 121
Att förhålla sig till teknikens potential och konsekvenser 122
Självcensur och demokratins självmål 124
Referenser 125

Om författarna **126**

Introduktion

Tobbe Petterson

En googling på ordet övervakning ger över en halv miljon träffar[1]. En snabb analys av sökresultatet pekar på att de allra flesta träffarna avser någon form av övervakning av individer; endast en liten del avser övervakning av t ex läkemedel eller miljö. De av träffarna som är taggade som nyheter, dryga 5.000 stycken, tyder på samma fördelning - att begreppet även i mer aktuellt hänseende främst handlar om övervakning av enskilda. Likaså är de bilder som söks fram nästan enbart med motiv på samma tema. Särskilt tydligt är där att övervakning ofta förknippas med kameror av olika slag.

Görs en sökning på ”övervakning och integritet” halveras antalet träffar, och det inte särskilt förvånande dominerande temat är hur begreppen på något sätt står i motsats till varandra. Ökad övervakning anses nagga integriteten i kanten, ibland tros till och med stora tuggor tas. Återigen handlar många av träffarna om kameraövervakning. Endast en mindre del handlar om andra sätt som individer övervakas, vilket är intressant att notera eftersom den enskilde idag kartläggs via ett stort antal sensorer; telefonen, bilen, aktivitetsarmbandet, inpasseringskortet, tvättstugebokningen, internetbanken och gymkortet för att nämna några. Hade ”någon” tillgång till alla sensorer skulle sannolikt vissa individer kunna kartläggas dygnet runt med avseende på geografisk plats, fysisk status, personlig ekonomi, trafikuppträdande och vardagliga aktiviteter. De tekniska möjligheterna att övervaka på ett sätt som de flesta troligtvis skulle uppleva som negativt för integriteten finns redan.

Det är om det möjliga motsatsförhållandet som den här antologin handlar. I ett antal texter diskuterar en stor bredd av författare olika aspekter av fenomenet. Startskottet för antologin var den workshop i ämnet som MSB initierade och som 2014 genomfördes vid Lunds universitet. Utfallet visade på ett behov av att ytterligare kartlägga den svenska debatten och att peka ut framtida viktig forskning. Uppdraget gick återigen från MSB till Lunds universitet och resultatet blev således denna skrift.

Det har varit en utmaning att föra allt i hamn – ämnet är i allra högsta grad aktuellt och nya fakta och infallsvinklar kommer hela tiden fram (som i form av nya avslöjanden från den tidigare NSA-medarbetaren Edward Snowden, vilka ofta har visat sig röra även svenska förhållanden). Händelserna har tvingat författarna att återkommande uppdatera och komplettera sitt underlag; att sätta punkt har liksom aldrig varit aktuellt. Antologin kan därför ses som en lägesrapport som sannolikt inte är helt aktuell när den läses, men som ändå pekar på ett antal möjliga spår av debatten att undersöka närmare.

I antologin kommer kamerorna återigen att dyka upp, men diskussionerna som förs är mer generella och tillämpbara även för andra övervakningsinstrument; kameran kan ses som en tydlig och lättförståelig symbol för en mängd sensorer, vilka alla har förmågan att inverka på integriteten. Att övervakningen kan ha både positiva och negativa sidor kommer också att beskrivas i skriften, liksom att integriteten är svårdefinierbar och individuell. Lagstiftning kommer att beröras och tekniska möjligheter (eller hot) att belysas. Sammantaget visar

[1] Sökningen gjordes i februari 2015 på de svenska orden och filtrerades till att enbart omfatta resultat från Sverige.

antologin på den stora bredd som ämnet omfattar och några av de olika ståndpunkter som kan antas; gemensamt för alla texterna är att de tydligt visar på behovet att följa utvecklingen på området närmare och över tiden.

I ett första kapitel går Malmö stads förre chefsstrateg Julia Branting på djupet med begreppet integritet och därefter diskuterar juristen Markus Naarttijärvi de konflikter som utvecklingen av olika rättsliga principer kan ge upphov till. Därpå följer en redogörelse av Janne Flyghed, professor i kriminologi, för nya kontrollmetoder och för nya aktörer på området. Nästa två kapitel är skrivna av två säkerhetschefer, Petrus Bolin på Handelsbanken och Per Gustafson på Lunds universitet, vilka båda ger en erfaren praktikers syn på det studerade fenomenet. Benjamin Weaver och Markus Lahtinen, båda forskare med inriktning på ämnet, ger sedan en internationell utblick och förslag på framtida svensk forskning. Nästa kapitel ringar in ämnet i en rättslig kontext och är skrivet av seniorprofessorn i rättssociologi Håkan Hydén och Marcin de Kaminski, nätforskare vid Lunds universitets Internetinstitut. Till slut knyter professorn i underrättelseanalys, Wilhelm Agrell, ihop säcken med ett sammanfattande kapitel.

Ett stort tack till alla författare som med kort varsel prioriterat denna antologi och som med hänsyn till den korta tid som tilldelats uppdraget hållit ett högt tempo i sitt skrivande – vilket engagemang och vilken discliplin ni visat!

Ett svenskt perspektiv på contextual integrity

Julia Branting

Inledning

Tiden och teknikutvecklingen har en tendens att ställa allt på ända. Den legendariske brittiske människorättsjuristen Paul Sieghart skrev 1976 i boken *Privacy och computers*:

> *"A computer, after all, is an assembly of elegant boxes sitting peacefully in someone else's building, and seems quite unsuited to intrude on anyone, or to conduct a surveillance operation."*

Idag tycks hans text både komisk och naiv. De senaste decennierna har ställt den personliga integriteten inför ständigt nya utmaningar. Efter den 11 september 2001 råder en ny säkerhetspolitisk doktrin som anger att nationalstaternas säkerhetsorganisationer för att hitta fienden måste rikta sökarljuset och avlyssningsutrustningen inåt, mot den egna befolkningen. Samtidigt gör teknikutvecklingen, där allt mindre lådlika men utomordentligt eleganta datorer spelar en framträdande roll, det möjligt att avlyssna och lagra fler och fler data i större och större mängder, vilket inte minst visas av Snowden-avslöjandena.

Skyddet av den personliga integriteten i lagstiftningen har dock inte utvecklats på ett sätt som möter upp samhällsutvecklingen. Forskaren Markus Naarttijärvi har i sin avhandling *För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, framlagd vid Umeå universitet i november 2013, undersökt hur den svenska staten väger säkerhet och integritet mot varandra i lagstiftningsarbetet och om dessa överväganden förändrats över tid, inte minst i ljuset av den tekniska utvecklingen. Naarttijärvi visar att någon proportionalitetsbedömning, som är det traditionella sättet att balansera säkerhet och integritet, numera i princip inte sker i lagstiftningsarbetet "utan snarare en prioritering mellan två intressen där det ena helt enkelt får företräde framför det andra" (Naarttijärvi 2013:523).

Ytterligare ett exempel på att skyddet av den personliga integriteten inte följer teknikutvecklingen är hanteringen av det som kallas "metadata". Trafikuppgifter och annan automatiskt genererad information betraktas fortfarande som mindre integritetskänslig än till exempel innehållet i e-postbrev och samtal, trots att, som professorn i underrättelseanalys och författaren Wilhelm Agrell påpekar, den tvärtom är "i viktiga avseenden […] mer exakt och mer avslöjande" (Agrell 2014:23).

Sammanfattningsvis tycks det angeläget att hitta metoder som gör det möjligt att på ett tillfredsställande sätt göra avvägningar mellan integritet och övervakning i dagens verklighet, men även när förändringar sker över tid.

Privacy – ett rörigt och komplext ämne

Privacy, som är den engelska motsvarigheten till *personlig integritet*, har en relativt kort historia som juridiskt och filosofiskt begrepp. Juridikprofessorn Serge Gutwirth daterar dess födelse till 1890 i en artikel av Bostonadvokaterna Samuel D. Warren och Louis D. Brandeis i

Harvard Law Review (2002).[2] Det sägs ha varit den tekniska utvecklingen – inte minst Eastman Kodaks billiga kameror – tillsammans med flera skvallertidningsreportage om Warrens fester, som utgjorde inspirationen (Wacks 2010).

Warren och Brandeis går igenom samtida domar kring förtroendebrott, äganderätt, copyright och förtal. Deras tes är att dessa utgör tillämpningen av en, redan existerande, generell rätt till *privacy* – "the right to be let alone" – och därmed att den befintliga lagen även kan skydda individen mot nyfikna medier (Warren och Brandeis 1890).[3] Det tog femton år för deras lagtolkning att få genomslag (Wacks 2010). Men efterhand har den blivit inflytelserik i den amerikanska juridiken och så småningom även i den allmänna debatten (A.a.; Solove 2002).[4]

Först under 1950- och 60-talet blev *privacy* en brännande fråga hos allmänheten. Beate Rössler, professor i etik vid universitetet i Amsterdam, kopplar detta till att datateknikens framväxt ökade de statliga byråkratiernas intresse för att samla in och behandla information (Rössler 2005). Alan Westin, som då var professor i offentlig rätt vid Columbia University, publicerade 1967 boken *Privacy and Freedom*. Den blev en viktig grund för de dataskyddslagar som stiftades i olika länder under 1970- och 80-talet (Bylund, 2013).

Westin beskriver *privacy* som ett rörigt och komplext ämne: "Few values so fundamental to society as privacy have been left so undefined in social theory or have been subject to such vague and confused writings by social scientists", inleder han sin bok (Westin 1967:7). Ännu idag ställer sig forskarvärlden med stor samstämmighet bakom denna beskrivning. Innebörden av *privacy* bedöms vara utomordentligt svårfångad, vilket också för med sig att begreppet saknar en enhetlig definition. Daniel J. Solove, professor vid George Washington University Law School och en auktoritet inom privacyforskningen, skriver till exempel lakoniskt att "Privacy is a concept in disarray. Nobody can articulate what it means" (Solove 2006a:477).

Ett skäl till otydligheten kan vara begreppets kontextuella karaktär. Redan 1967 skrev Westin att olika historiska och politiska traditioner tycks skapa olika förhållningssätt. Och i den samtida privacyforskningen råder, trots att man alltså inte är överens om begreppets omfattning och innebörd, samstämmighet om att dessa på ett eller annat sätt är beroende av sammanhanget.

Det kontextuella synsättet har även fått genomslag i policy. Professorerna i statsvetenskap Colin J. Bennet och Charles Raab framhåller till exempel att den policyutveckling rörande dataskydd som skedde under 1980-talet utgick ifrån att *privacy* är subjektivt och därför baserades på proceduriella snarare än innehållsmässiga kriterier (Bennet och Raab 2007).

Efter noga övervägande väljer Solove att se *privacy* som ett paraplybegrepp (Solove 2006a). Kanske är det så man bäst hanterar det. Och för att inte bli alltför nedslagen av begreppsdiskussionen kan man vända sig till den israeliska juridikprofessorn Ruth Gavison, som påpekar att de flesta människor trots allt ser *privacy* som ett användbart begrepp och

[2] Se även Glancy (1979); Solove (2004); Wacks (2010); Stone (2010).

[3] Domaren och forskaren Thomas Cooley är upphovsman till uttrycket "right to be let alone". Warren och Brandeis (1890).

[4] Den amerikanske juridikprofessorn Geoffrey R. Stone (2010) påpekar att Warren och Brandeis mediekritik är slående lik dagens kritik av publicering på internet.

använder det som om det vore det – vilket faktiskt innebär att det är det (Gavison 1980). För forskarna är begreppsdiskussionen nödvändig men i vardagligt tal eller i allmänna sammanhang spelar det ingen roll om individer lägger något olika innebörd i ordet.

Personlig integritet – ett begrepp utan definition

Även det svenska begreppet *integritet*, (i betydelsen *personlig integritet*), är otydligt till sin karaktär. Enligt den legendariske professorn emeritus i civilrätt Stig Strömholm kan man spåra dess bredare introduktion till år 1966 då den första integritetsskyddskommittén tillsattes och fick i uppgift att undersöka möjligheterna för ett förstärkt skydd av privatlivet (Strömholm 1978).

I samband med den Internationella juristkommissionens nordiska konferens om privatlivets rättsskydd 1967 gjordes ett försök att definiera *integritet* genom att upprätta en katalog över integritetskränkningar (SOU 2007:22; SOU 2008:3). Inom ramen för detta sätt att hantera begreppet stod dock Stig Strömholm själv för det mest inflytelserika bidraget (Strömholm 1971).

Det finns än idag ingen definition av begreppet i den svenska lagstiftningen (Ds 2014:23).[5] I sitt delbetänkande *SOU 2007:22* skriver 2004 års integritetsskyddskommitté att det ”är svårt för att inte säga omöjligt att komma fram till en entydig och allmänt accepterad definition av begreppet personlig integritet” (SOU 2007:22:53f). I samma betänkande finns en redogörelse för hur tidigare utredningar och kommittéer inom integritetsområdet förhållit sig till frågan – de flesta använder egna definitioner, eller ingen definition alls. Integritetsskyddskommittén väljer själv att förlita sig på ”intryck” på ett sätt som återknyter till Gavisons resonemang ovan (SOU 2007:22:63):[6]

> *”Det sammantagna intrycket av direktiven, tidigare utredningsarbete och den allmänna diskussion som förts genom åren ger trots allt en ganska bra bild av vad det är som kommittén förväntas undersöka och analysera.”*

Liksom *privacy* anses även *personlig integritet* ha kontextuell karaktär. Ledamoten i Högsta förvaltningsdomstolen (då Regeringsrätten) Annika Brickman skrev till exempel i Svensk Juristtidning 2007 att ”yttre omständigheter, som ekonomi, kultur och sociala förhållanden, är helt avgörande för att en människa över huvud taget skall kunna hävda sin rätt till en privat sfär” (Brickman 2007:174). Ett ytterligare exempel är Datainspektionens svar på frågan ”Vad menas med en kränkning av den personliga integriteten?” på myndighetens hemsida: ”vad som kan vara en kränkning för en viss person eller i ett visst sammanhang […] behöver [inte] vara det för en annan person eller i ett annat sammanhang”.

En fråga om balans?

Den traditionella metoden att presentera problematiken kring integritetsfrågor som en avvägning innebär en tillämpning av proportionalitetsprincipen i regeringsformen (SOU 1998:46). Oftast beskrivs avvägningen som att den står mellan två befogade intressen: den

[5] Se även SOU 1984:54; SOU 2002:18; SOU 2005:38; SOU 2008:3; Dir. 2004:51.

[6] Ett liknande förhållningssätt kan även iakttas i SOU 2002:18.

enskildes integritet å den ena sidan och exempelvis effektivitet eller säkerhet å den andra (SOU 2007:22).[7]

Integritetsskyddskommittén visade i sitt betänkande att det finns betydande brister i redovisning och analys av lagstiftarens proportionalitetsöverväganden, ”i vissa fall närmast av den karaktären att de måste betecknas som systemfel” (SOU 2007:22:449). De positiva effekter som väntas av ett nytt lagförslag redovisas dåligt, och de skador som kan åsamkas den personliga integriteten ännu sämre och ofta inte alls. Även i de fall där beredningsunderlaget är tillräckligt för att göra en proportionalitetsbedömning, görs denna ofta ”på ett alltför knapphändigt och klichéartat sätt” (SOU 2007:22:451):

> *”Många gånger sägs egentligen bara att integritetsintrånget visserligen är betydande men att det jämfört med fördelarna med den föreslagna åtgärden ändå inte är så stort att det vore försvarligt att avstå från lagstiftning.”*

Integritetsskyddskommitténs slutsatser bekräftas även i Markus Naarttijärvis avhandling. ”En bristfällig avvägningsprocess i kombination med risktänkande och en preventiv utgångspunkt […] tycks leda till en ensidig och subjektiv bedömning utan hänsyn till de mer långsiktiga värden som de konstitutionella rättigheterna söker upprätthålla”, skriver Naarttijärvi (2013:523).

Efter att ha tagit del av Integritetsskyddskommitténs betänkanden, beslutade regeringen att lägga till en bestämmelse i Regeringsformen (RF) 2 kap 6 § (Regeringens proposition 2009/10:80).[8] Även RF 2 kap 20§ och 21§, som utgör grundvalen för proportionalitetsprincipen, reviderades och regeringen skrev (Lag 2010:1408; Regeringens proposition 2009/10:80:176f.):

> *”[E]n följd av denna reglering [är] bl.a. att lagstiftaren tvingas att tydligt redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen. Detta kan förväntas öka förutsättningarna för att avvägningarna i fråga om integritetsintrånget blir mer ingående belysta och att de presenteras på ett sådant sätt att kvaliteten i lagstiftningen höjs ytterligare.”*

Har man därmed vidtagit de åtgärder som krävs för att en väl genomförd bedömning av integritetsaspekterna ska ske? Naarttijärvi har även undersökt direktiv, betänkanden och propositioner som skrivits fram efter att grundlagsändringen trätt i kraft den 1 januari 2011 och kommer ändå till slutsatsen att proportionalitetsbedömningen är undermålig (2013).[9] Av detta kan man dra slutsatsen att grundlagsändringen, i alla fall under åren 2011 och 2012 som granskats av Naarttijärvi, inte har fått den önskade effekten.

---

[7] Se även SOU 2008:3. I praktiken ska man dock, om proportionalitetsprincipen ska kunna anses vara rätt tillämpad, ta med många fler variabler än två, och även beakta vilka alternativa och mindre ingripande metoder som skulle kunna användas istället.

[8] Tillägget i Regeringsformen lyder: ”var och en [är] gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.” Lag (2010:1408).

[9] Han finner till exempel en ”avsaknad av egentliga analyser [---] i det beredningsunderlag som låg till grund för regelverket i 2012 års inhämtningslag” (Naarttijärvi 2013:515).

Helen Nissenbaum och contextual integrity

Helen Nissenbaum, professor vid Institutionen för media, kultur och kommunikation vid New York University, har under ett par decenniers tid arbetat fram en teori och metod som hon föreslår ska ersätta metoden att presentera problematiken kring integritetsfrågor som en avvägning mellan *personlig integritet* och andra befogade intressen.[10]

Nissenbaum är en auktoritet i USA, och inte bara inom akademin. Hennes sätt att se på *privacy* har påverkat den amerikanska motsvarigheten till Konsumentverket, Federal Trade Commission (Madrigal 2012). Hon var även aktiv i remissförfarandet när Obamas administration skrev fram en rapport som innehåller förslag till en ny lagstiftning för att stärka konsumenternas rättigheter på Internet – i rapporten citeras både hennes bok *Privacy in context* från 2010 och remissvaret (Weinstein 2012; The White House, Office of the Press Secretary 2012).

Nissenbaum (2010) iakttar att människors oro för integriteten hänger samman med teknikutvecklingen, men att inte alla nya övervakningssystem hälsas med samma misstro.[11] En teori måste kunna förklara dessa olikheter och lösningen, menar hon, är inte att kontrollera eller begränsa tillgången till information, utan att reglera informationsflödet så att det sker på ett i varje sammanhang passande sätt. Sammanhangen kallar hon för *kontexter*. Som exempel på olika kontexter anges sjukvård, utbildning, arbetsliv, religion, familj och affärsliv.

Nissenbaum beskriver – tämligen raljant – hur i stort sett alla som skrivit om *privacy* och informationsteknologi har gett sig på att försöka reda ut begreppsdefinitionen, men att detta är en återvändsgränd. Med den motiveringen avstår hon ifrån att alls ge någon definition av *privacy* och talar istället om *personuppgiftsflöden*. Definitionen av vad som är en personuppgift hämtar hon från EU:s Dataskyddsdirektiv.[12] Nissenbaum menar att människor har olika förväntningar på flödet av *personuppgifter* utifrån karaktäristika i respektive *kontext*, som hon kallar *kontextrelaterade informationsnormer*. Dessa är en funktion av:

1. informationsslaget,
2. den person som är informationens objekt,
3. sändaren (kan vara samma person som i punkt 2.) och mottagaren, samt
4. sändnings-/överföringsprinciperna.

När normerna respekteras bevaras *contextual integrity*, men när de trotsas upplever vi det som en kränkning. Observera att det räcker att en – vilken som helst – av de fyra parametrarna förändras för att kränkningen ska uppstå.

[10] Detta beskrivs mest utförligt i Nissenbaum (2010).

[11] Som exempel på övervakningssystem som tagits emot med stor entusiasm nämner hon de apparater som registrerar patienternas hjärtrytm m.m. på sjukhus.

[12] I sin svenska version lyder den: ”personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”. Direktiv 95/46/EG, Artikel 2 a.

Nissenbaum gör alltså upp med föreställningen att information som man en gång delat med sig av ovillkorligt kan spridas vidare. Likaså är hon kritisk till alla idéer om att viss teknik per definition är kränkande och bör mötas av motstånd.[13]

Nissenbaum identifierar och bemöter två problem, som är inbyggda i *contextual integrity*-ramverket. Det första är att all förändring vid första anblicken, i och med att måttstocken är de existerande normerna, kommer att klassificeras som en kränkning av *contextual integrity*. Det andra kallar hon andra sidan av samma mynt: det finns i ramverket inget skydd mot "normalitetens tyranni".

Mot det första problemet invänder Nissenbaum att det att man noterar att en praxis eller ett system bryter mot normen inte är analysens slutpunkt utan endast ett påstående som ligger till grund för fortsatt analys. Hon anser också att bägge problemen vederläggs genom att en moralisk komponent inkorporeras i teorin. Genom att undersöka vilka moraliska och politiska faktorer som påverkas och därefter om de nya normerna stödjer *kontextens* relevanta *värden* på ett bättre eller sämre sätt än de gamla, kan man avgöra om systemet eller praxisen de facto kränker *contextual integrity*, vilket ger skäl för motstånd och protest.[14]

Nissenbaums redogörelse för teorin kring *contextual integrity* landar i vad hon kallar för en *utvidgad beslutsheuristik*. Begreppet *heuristik* betyder enligt Nationalencyklopedin "dels metod för att upptäcka eller bilda ny relevant kunskap, dels läran om sådana metoder".[15] En heuristik används för att göra antaganden eller formulera hypoteser som man sedan kan pröva empiriskt.

Enligt Nissenbaum är *beslutsheuristiken* ett verktyg för att förstå konflikten när till exempel ett tekniskt system eller en praxis kritiseras med integritetsargument, och den *utvidgade beslutsheuristiken* ett sätt att utvärdera systemet eller praxisen ifråga ur moralisk och politisk synvinkel. Hennes *beslutsheuristik* består av punkterna 1-6 nedan och den *utvidgade beslutsheuristiken* av punkterna 1-9 [16]:

1. "Describe the new practice in terms of information flows.
2. Identify the prevailing context. [---]
3. Identify information subjects, senders, and recipients.
4. Identify transmission principles.
5. Locate applicable entrenched informational norms and identify significant points of departure.
6. Prima facie assessment: [---] A breach of informational norms yields a prima facie judgment that contextual integrity has been violated because presumptions favors the entrenched practice.
7. Evaluation I: Consider moral and political factors affected by the practice in question. [---]

[13] Ett liknande resonemang finns i SOU 2007:22.

[14] I sina tidigare verk talar Nissenbaum även om en andra uppsättning normer - norms of appropriateness. Se till exempel Nissenbaum (2004). I Nissenbaum (2010) använder hon dock inte längre detta begrepp.

[15] Adjektivformen heuristisk förklaras av Nationalencyklopedin "som innebär självständigt sökande efter lösning (på ett problem)". Se Heuristik respektive Heuristisk (utan år).

[16] Observera att Nissenbaum endast använder sig av numrerade punkter för att tydliggöra resonemanget. När hon gör sina analyser sker det i löpande text.

8. Evaluation II: Ask how the system or practices directly impinge on values, goals, and ends of the context. In addition, consider the meaning or significance of moral and political factors in light of contextual values, ends, purposes, and goals. [---]
9. On the basis of these findings, contextual integrity recommends in favor of or against systems or practices under study. [---]"

Denna metod kan enligt Nissenbaum användas i alla situationer där farhågor finns för att ny teknik eller teknikanvändning ska påverka den personliga integriteten. Den begränsas alltså inte till exempelvis bedömning av lagförslag.

Nissenbaum är filosof och hennes *beslutsheuristik* hämtar tydlig inspiration från filosofisk metod. Det är inte frågan om att empiriskt försöka bevisa att en eller annan föreslagen teknikanvändning kränker *contextual integrity*, utan att lägga fram argument, som kan granskas. Analysen blir med nödvändighet subjektiv utifrån forskarens eller analytikerns bakgrund och perspektiv. Detta gäller dock för alla analyser, oavsett metod, och en fördel här är att metoden så tydligt redovisas och analysen därmed är lätt att följa och utvärdera.

Contextual integrity i svenskt perspektiv – två fallstudier

Nissenbaum utformar sin teori i USA, för amerikanska förhållanden och utifrån amerikanska exempel.[17] Hon menar dock att den ska vara möjlig att tillämpa överallt. Detta ska inte tolkas som att hon är ovillig att erkänna kulturella skillnader, utan som att dessa skillnader inte spelar någon roll. Varje kontext bedöms ju för sig.

Begreppet *contextual integrity* förtjänar en kommentar när man funderar över hur teorin kan överföras till svenska förhållanden. Till skillnad från det svenska *integritet*, som ingår i begreppet *personlig integritet* och ofta används som en kortform för detta, har i USA *integrity* eller någon sammansättning med detta ord inte använts i betydelsen *personlig integritet*. Varför väljer Nissenbaum då att bygga på det? Det finns ingen förklaring i hennes bok, men jag gissar att Nissenbaum försöker etablera ett avstånd till *privacy* genom att välja ett annat begrepp.

För att reproducera detta avstånd skulle man i Sverige behöva översätta *contextual integrity* till något annat än *kontextintegritet* eller *kontextuell integritet*, exempelvis *kontextuell personsfär* eller *kontextuell normanalys*. Jag säger inte att dessa förslag är bra, eller ens bättre än andra, men de tydliggör mitt resonemang genom att ge läsaren möjlighet att själv känna hur språket fungerar. Tills vidare har jag dock valt att behålla *contextual integrity* oöversatt.

I syfte att illustrera hur tillämpningen av *contextual integrity*-ramverket skulle kunna te sig i praktiken går jag nu över till två konkreta, svenska, fallstudier. De förslag jag analyserar har i denna form redan avfärdats. Men eftersom syftet med övningen inte är att avgöra om förslagen bör genomföras eller ens att bedöma faktiska integritetskränkningar utan enbart att visa fram en teori och metod, kan det till och med vara en fördel att förslagen är överspelade. Det ger nämligen möjlighet att upprepa analysen och studera hur slutsatserna påverkas när förändrade förslag läggs fram.

[17] Nissenbaum är född och uppväxt i Sydafrika, där hon också tog sin kandidatexamen. Hon avlade mastersexamen vid Stanford University, doktorerade där i filosofi och har sedan dess varit verksam i USA. Hon är dock mycket tydlig med att teorin om *contextual integrity* utgår ifrån USA och amerikanska förhållanden. Krattenmaker 1994; Nissenbaum, 2014.

ITS27 – automatiserad utlämning av trafikuppgifter

Mitt första undersökningsobjekt är standardiseringsdokumentet ReportITS27 - Tillämpningsanvisning/Application guide, utgåva 1.1.1 daterad den 1 augusti 2012, ett standardiseringsdokument som bland annat ”[b]eskriver gränssnitt och procedurer som kan användas mellan tjänsteleverantörer och brottsbekämpande myndigheter för utlämnande av trafikuppgifter i enlighet med det legala regelverket” (Report ITS27:5).[18]

Bakgrunden är att tjänsteleverantörerna enligt *lagen om elektronisk kommunikation*, sedan en lagändring med syfte att implementera EU:s datalagringsdirektiv trädde ikraft den 1 juli 2012, är skyldiga att lämna ut trafikuppgifter ”utan dröjsmål”, ”så att verkställandet av utlämnandet inte röjs”, och ”på ett sådant sätt att informationen enkelt kan tas om hand” (Lag (2012:127), 6 kap, 16f§). Enligt *lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*, 1§, får Säkerhetspolisen i underrättelseverksamhet i hemlighet hämta in trafikuppgifterna.[19] Beslut om inhämtning fattas av myndighetschefen eller på dennes delegation, varefter Säkerhets- och integritetsskyddsnämnden ska underrättas, senast en månad i efterhand (Lag (2012:278) 4§ och 6§).

Tanken med ITS27 är att automatisera och förenkla begäran och utlämnande av trafikuppgifter. De tjänsteleverantörer som vill genomföra automatiseringen ska ingå bilaterala avtal om den tekniska implementationen (Report ITS27:5; Kleja 2013a). Den är inte tvingande. Men enligt en artikel i Ny Teknik anser Säpos signalstrategiske rådgivare, kriminalkommissarie Kurt Alavaara, att operatörerna måste använda standarden om de ska klara kraven i lagen om elektronisk kommunikation (Kleja 2013a). Han uppger även att ITS27 medför att polisen får direktkontakt med databaser med trafikdata.

När ITS27 kom till mediernas kännedom hösten 2013 uttryckte flera teleoperatörer, med Bahnhof och Tele2 i spetsen, stark kritik (A.a.; Eriksson, 2013; Tele2 Sverige, 2013).[20] Trots att ITS27 omfattade samtliga brottsbekämpande myndigheter låg fokus i debatten helt på Säkerhetspolisen.

Den 27 november spelade Bahnhofs VD Jon Karlung in fyra timmar av ett möte med flera personer från Säpo (bland annat Alavaara) samt Rikskriminalpolisen på band och lämnade över inspelningen till Ekot, som sände delar av den i december (Djelevic och Gagliano 2013a; Kleja 2013c).

På bandet framkom att Säpo ville teckna säkerhetsskyddsavtal, så kallade SUA-avtal klass 2, med samtliga cirka 570 svenska tjänsteleverantörer (Gagliano och Djelevic 2013; Svenska stadsnätföreningen, utan år; Kleja 2013c). Enligt Ekot innebar detta inte bara ett förbud att berätta om samarbete med Säpo utan även att de tjänsteleverantörer som valt att stå utanför systemet inte skulle kunna berätta att de *inte* samarbetar med Säpo. Dessutom framkom att Säpo varken informerat Säkerhets- och integritetskyddsnämnden eller Datainspektionen om

[18] ITS27 är en svensk tillämpning av ETSI TS 102 657 som fastställts av det europeiska telekommunikationstandardiseringsorganet European Telecommunications Standards Institute (ETSI).

[19] Detta gäller även övriga polismyndigheter samt Tullverket.

[20] Även TeliaSonera och Tre var skeptiska. Kleja 2013b.

att man planerade att införa ett helautomatiskt system för utlämnande av trafikuppgifter (Djelevic och Gagliano 2013b).

I december sammanträdde AG-15, den arbetsgrupp vid Informationstekniska standardiseringen (ITS) som har tagit fram ITS27-standarden. Arbetsgruppens ordförande sade i samband med mötet att man ansåg att operatörerna måste få göra manuella kontroller innan uppgifter lämnas ut, även om överföringen sker automatiskt, för att de ska kunna uppfylla reglerna om tystnadsplikt (Kleja 2013c). Han sade också att arbetsgruppen avsåg att ägna den närmaste tiden bland annat åt frågan om ”grad av automatik” och åt att tydligare skilja på olika uppgiftskategorier i utlämningsformuläret.

Den 8 april 2014 förklarade EU-domstolen EU:s datalagringsdirektiv ogiltigt varpå Bahnhof avbröt all datalagring och raderade sina sparade trafikuppgifter (Europeiska unionens domstol 2014; Bahnhof 2014a). Enligt ett pressmeddelande från ITS samma dag avvaktade man där ”regeringens, Post- och telestyrelsens (PTS) och ETSIs konsekvensanalys” (Informationstekniska Standardiseringen 2014).

Den 10 april uttalade PTS generaldirektör Göran Marby i ett pressmeddelande att man ”ser […] stora svårigheter att vidta åtgärder utifrån de särskilda reglerna om datalagring som utgör undantag från de integritetsskyddande reglerna” (Post- och telestyrelsen 2014). Branschtidningen Computer Sweden tolkade detta i en rubrik som ”PTS: okej att sluta lagra” (2014).

Den 14 april avbröt även Tele2 sin datalagring och raderade de uppgifter som tidigare lagrats, efter att ha meddelat att man fortsättningsvis endast skulle lämna ut information om abonnentfakturering och nätövervakning (Wretman 2014a; Carlsson 2014).[21] Dagen efter anmälde Rikspolisstyrelsen (RPS) Tele2 till PTS (Wretman 2014a).

Regeringen tillsatte den 29 april den förre ordföranden i Högsta förvaltningsdomstolen Sten Heckscher som utredare för att analysera EU-domens konsekvenser för svensk rätt (Ju2014/3010/P2). Heckscher uttalade i sin promemoria i juni att det i och för sig ”kan finnas skäl att närmare överväga några frågor”, men att ”det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK samt övriga bestämmelser om tillgång och behandling av sådana uppgifter, även utan sådana åtgärder och med beaktande av EU-domstolens uttalanden, inte strider mot unionsrätten eller europarätten” (Ds 2014:23:101).[22]

PTS skickade den 16 juni ut ett brev till operatörerna i vilket man skriver att ”myndigheten kommer nu [det vill säga efter att regeringens utredare lämnat sin rapport] att utgå från att de svenska reglerna om datalagring ska tillämpas” (Bergman 2014). Tele 2 svarade samma dag att man stod fast vid sitt beslut att upphöra med datalagring, bland annat menade man att

[21] Även Comhem meddelade att man avsåg att avbryta sin datalagring från den 14 juni ”så till vida att PTS inte kommer med andra besked." (Åhlin 2014).

[22] De frågor som utredningen anser att det kan finnas skäl att överväga är ”dels lagringsskyldigheten avseende ett par uppgiftskategorier, dels reglerna om tillsyn såvitt avser inhämtning av abonnemangsuppgifter och reglerna om en oberoende kontroll såvitt gäller inhämtning av uppgifter i underrättelseskedet. Vidare kan övervägas om ett uttryckligt förbud mot lagring utanför EU/EES bör införas.” (Ds 2014:23). Vad jag har kunnat se är England och Sverige de enda EU-länder som har kommit till slutsatsen att det egna regelverket kan fortsätta användas trots domen (Hern 2014).

Heckschers slutsatser byggde på en felaktig tolkning av domen i EU-domstolen (Wretman 2014a).

Den 19 juni skickade PTS en underrättelse till företaget där man under rubriken ”PTS bedömning” skriver att man ”vid en sammantagen bedömning mot bakgrund av vad Tele2 anfört, EU-domstolens dom samt slutsatserna i Ds 2014:23, [finner] att det saknas skäl att underlåta att tillämpa de svenska reglerna om lagring av trafikuppgifter m.m.” (A.a.).

Den 27 juni meddelade PTS i ett föreläggande att Tele2 från och med den 25 juli 2014 skulle vara skyldiga att åter lagra trafikuppgifter (Wretman 2014b). Tele2 påbörjade då, enligt uppgift från chefsjuristen Stefan Backman, datalagringen igen.[23]

Bahnhof lämnade den 8 juli in en anmälan mot sig själv till PTS för brott mot lagen om elektronisk kommunikation (Bahnhof 2014b). Man skrev att ”Bahnhof vill få prövat om den svenska lagstiftningen om datalagring är förenliga med EU-rätten […]. Som tillsynsmyndighet med uppgift att övervaka att reglerna i LEK efterföljs utgår Bahnhof från att PTS kommer att vidta åtgärder med anledning av denna anmälan.”[24] PTS beslut kom den 27 oktober och hotade Bahnhof med fem miljoner kronor i vite om företaget inte börjat lagra trafikuppgifter inom fyra veckor (Bahnhof 2014e). Bahnhof svarade i ett pressmeddelande att lagringen kommer återupptas, men att alla kunder kommer erbjudas kostandsfri anonymiseringstjänst "som gör datalagringen meningslös” (Bahnhof 2014f).

Bahnhof har under året, med bistånd av yttrandefrihetsexperten och journalisten Nils Funcke, försökt att få tillgång till den rättsutredning som PTS tog fram efter EU-domstolens utslag och som låg till grunden för generaldirektören Göran Marbys pressmeddelande den 10 april (Funcke 2014a; Bahnhof 1 oktober 2014c och 2014d). Det besked man fått är att rättsutredningen inte utgör en allmän handling. I slutet av oktober framkom dock att Marby i en skrivelse till riksdagens justitieutskott den 23 maj angivit att myndigheten har möjlighet att lämna ut rättsutredningen men att man anser att ”det i dagsläget vore olämpligt” (Funcke 2014a). Detta brev registrerades inte i PTS diarium utan hålls ordnat på rättssekretariatet, vilket är tillåtet enligt lag men kritiseras skarpt av Nils Funcke som skriver att det ”i princip [är] nödvändigt att veta att dokumentet finns för att få del av det” och att liknande fall har klandrats av JO. Funcke meddelade också på sin blogg att han den 14 november på Bahnhofs uppdrag anmält PTS till JO (Funcke 2014b och 2014c).

Analys av ITS27-dokumentet

Jag ämnar nu att, med hjälp av Nissenbaums *utvidgade beslutsheuristik*, analysera en situation där en fiktiv mobilleverantör överväger att ansluta sig till ITS27-standarden och teckna avtal med Säpo om utlämning av trafikuppgifter. För att göra analysen så grundläggande som möjligt kommer jag att bortse från vad företaget skulle kunna skriva i sin sekretesspolicy och

[23] ”Vi begärde inhibition av PTS föreläggande men förvaltningsrätten avslog detta så vi är därmed skyldiga att efterleva PTS föreläggande och börja datalagra ånyo”, skriver Backman i ett mail (Backman 2014a). Tele2 förlorade även själva datalagringsmålet i förvaltningsrätten i slutet av oktober men har överklagat domen till kammarrätten. (Backman 2014b).

[24] Pressmeddelandet är ordagrant citerat med bibehållna korrekturfel.

även från den detaljerade lagregleringen av olika omständigheter, exempelvis vad inhämtat material får och inte får användas till.[25]

Sändaren och *mottagaren* är i det här fallet avtalsparterna i form av kund och leverantör, *objekten* är kunden och de personer som denne har kontakt med via sin mobiltelefon, *informationsslaget* trafikuppgifterna och *sändnings-/överföringsprinciperna* utgörs av de system som finns för hantering av trafikuppgifter.

Information om trafikuppgifter som lagras av tjänsteleverantören och eventuella underleverantörer ska enligt lag vara tillgänglig för brottsbekämpande myndigheter, inklusive Säpo. De existerande normerna i kontexten innefattar alltså att information kan komma att lämnas ut. Men de innefattar dessutom förväntningar på hur utlämningen ska gå till: enligt min uppfattning bland annat att Säpo ska kunna producera ett beslut med stöd i lag, att operatören endast lämnar ut den nödvändiga informationen och inte en mängd överskottsinformation, samt att granskning och kontroll äger rum. Vidare finns det förväntningar om att så få personer som möjligt får ta del av informationen, och att tjänsteleverantören har ett intresse av att värna tystnadsplikten bland annat genom att se till att informationen inte läcker.

Hur påverkas de *kontextrelaterade informationsnormerna* om företaget beslutar sig för att använda sig av ITS27?

I och med att brottsbekämpande myndigheter har tillgång till informationen oavsett om överlämnandet sker manuellt eller automatiserat, påverkas inte *sändare* eller *mottagare* av automatiseringen.

Påverkas de personer som är informationens *objekt*? Ja, både genom att formatet standardiseras och om Säpo får direktkontakt med den databas där en stor mängd information förvaras.

Informationsslaget påverkas definitivt. Avtalen omfattar både de trafikuppgifter som det är obligatoriskt att lämna ut enligt lag och uppgifter som man därutöver beslutar sig för att inkludera, exempelvis PUK-koder och betalningsuppgifter inklusive kontonummer (Report ITS27 2012:8; Kleja och Anrell 2013).

Slutligen påverkas *sändnings-/överföringsprinciperna*, i och med att manuell överföring med vidhängande granskning ersätts av automatisk överföring där granskning endast kan ske i efterhand.

Sammanfattningsvis innebär ITS27 alltså förändringar av både *objekt*, *informationsslag* och *sändnings-/överföringsprinciper* – det vill säga en prima facie kränkning av *contextual integrity*. När detta står klart fortsätter utvärderingen i enlighet med den *utvidgade beslutsheuristiken* som undersöker de moraliska och politiska faktorer som påverkas:

Solove beskriver hur inte bara vetskap om att övervakning sker utan i lika hög grad medvetenhet om att övervakning skulle kunna äga rum kan göra en person obekväm, hämmad och få honom eller henne att ändra sitt beteende, vilket bland annat innebär att övervakning

[25] Så gör även Helen Nissenbaum i motsvarande analyser (2010).

(även) på detta sätt är ett verktyg för social kontroll (Solove 2006a).[26] Positiva konsekvenser saknas inte, bland annat kan man hindra vissa typer av brott. Men samtidigt hämmas den intellektuella friheten och individualiteten. Solove beskriver det som att övervakning slipar av kanterna i våra åsikter och vårt beteende, så att de blir mer konventionella.

Oavsett automatiseringen sker lagring och utlämning av trafikuppgifter. Men någonting inträffar i och med att maskiner tar över delar av processen från människor. Den inflytelserike amerikanske juristen Richard Posner har argumenterat för att automatisk hantering är mindre integritetskränkande: ”This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer" (Solove, (2008b:192). På samma sätt är datorn i detta perspektiv att föredra framför telefonbolagets anställda.

Robert S. Litt, chefsjurist vid amerikanska Office of the Director of National Intelligence (ODNI), reflekterade i ett tal i juli 2013 kring varför människor som gärna lämnar personlig information till privata företag inte är beredda att ge samma information till staten:[27] ”This does not seem to me to be a difficult question”, skriver han i den publicerade versionen av talet, ”we care because of what the Government could do with the information”. Staten har makt och det finns alltid en farhåga att makten kan missbrukas. Men blir det någon skillnad med automatisk hantering? Jag vill påstå det. Beakta denna mening från Solove: ”If a government computer decides that you are a likely threat, then you might find yourself on a watch list […]” (Solove 2008a:57). Känslan som väcks i oss vid tanken på att en dator skulle ges makt över våra liv är starkt negativ. Metaforen ”storebror” är mycket kraftfull, och djupt inbäddad i det västerländska tänkandet kring personlig integritet (se till exempel Solove 2008a och Solove 2006b). Även när sanningen är den motsatta, känner vi att automatisk hantering ökar risken för integritetskränkande misstag. När detta förhållande ställs vid sidan av texten i föregående stycke syns en paradox: Känslan är både att automatisk övervakning är mindre integritetskränkande och samtidigt att det ger en ökad risk för integritetskränkning.

Det finns argument för att standardiseringen enligt ITS27 inför nya, förstärkta, normer om ordning och reda i utlämnandet. Erik Hörnfeldt, dåvarande presschefen på mobiloperatören Tre, säger i en intervju att ”[d]et blir tydligt att det är Säpo som är vår kontaktpunkt […]. Nu kan enskilda polismän ringa till oss och begära data, då måste vi hänvisa dem till de korrekta kanalerna” (Eriksson 2013). Med ITS27 blir rutinen tydlig och lätt att följa. Varje beställning ska ha ett unikt referensnummer och äktheten i beställning och leverans verifieras med kodnycklar (ReportITS27 2012). En tilläggsspecifikation som Säpo vill teckna med leverantörerna kommer att göra det möjligt för dessa att verifiera att IP-adressen som beställningen kommer ifrån är behörig (Kleja 2013a).

Men samtidigt kan, i och med automatiseringen, beställningens laglighet och beslutsenlighet inte kontrolleras innan utlämnandet äger rum. Genom referensnumret kan man få fram en hänvisning till beslut hos den myndighet som auktoriserat beställningen – men först i efterhand (Kleja 2013b).[28] En referens till rättslig grund för beställningen kan uppges – men

[26] Detta kallas för den panoptiska effekten, efter Jeremy Benthams tänkta fängelsebyggnad Panopticon med tårtbitsformade celler som gränsar till övervakarens utrymme i mitten (Solove 2006a).

[27] Litts exempel rör faktiskt just telefonbolagens möjligheter att överföra information till NSA:s servrar.

[28] Enligt Tele2:s chefsjurist Stefan Backman, som intervjuas i artikeln.

det är frivilligt att avtala om detta (ReportITS27 2012). Det tycks som att tjänsteleverantörerna idag kontrollerar beslut och laglighet. Bahnhofs VD Jon Karlung säger till exempel till Ny Teknik att ”vi kan få mejl att [sic] polisen med begäran om utlämning där det inte ens finns med någon laglig grund” (Kleja 2013c). Och Tele2:s chefsjurist Stefan Backman säger enligt tidningsreferat att det hänt att polisen velat ha ut trafikdata i utredningar kring ”lindrigare brott eller brott som har lägre straffvärde än två år, vilket Tele2:s personal i dag stoppar” (Kleja 2013b). Automatiseringen medför därmed att en granskningsfunktion försvinner.

Standardiseringen gör risken mindre för att överskottsinformation lämnas ut, men om Säpo får direktkontakt med databaser där operatören lägger in uppgifter, finns samtidigt en icke försumbar risk att man kan få ut mer eller annan information än den beslutet gäller. Även möjligheten att sluta separata avtal med varje leverantör, med sinsemellan olika ”tillval”, ger samma känsla. Man kan beskriva detta som skillnaden mellan vad myndigheten *kan* respektive *får* göra. Vid manuell hantering kan man inte komma över mer information än vad det finns lagstöd för, men vid automatisk hantering kan man komma över all information i databasen om man har tillgång till denna.[29]

Ledamoten i dåvarande Regeringsrätten Annika Brickman skriver om vikten att myndigheterna hanterar insamlad information ”professionellt och under ansvar” (Brickman 2007).[30] Den viktigaste faktorn för att så ska ske, menar hon, är kontinuerlig utvärdering. I fallet med ITS27 är det oklart hur utvärdering ska ske. Underrättelseorganisationer kan inte underställas öppen kontroll på samma sätt som statliga myndigheter i allmänhet. Och datastandardiseringsorganet ITS är inte något kontrollorgan. Det tycks som att allmänheten saknar möjlighet att avgöra om reglerna följs.

Det sista steget i utvärderingen enligt Nissenbaums *utvidgade beslutsheuristik* är att undersöka om den gamla eller nya praxisen samlat bättre stödjer relevanta *värden* i *kontexten* – i detta fall mobil kommunikation (Nissenbaum 2010). De existerande normerna innefattar känslan av något som skulle kunna kallas för ett moraliskt avtal mellan tjänsteleverantör och kund. I det ingår att kontrollerad utlämning av nödvändig information till Säpo kan komma ifråga, men att tystnadsplikten i övrigt gäller, och att tjänsteleverantören är beredd att ta strid för denna om den ifrågasätts. Känslan av att tystnadsplikten är essentiell inte bara för kunden utan också för operatören, och uppfattningen om detta gemensamma intresse, är en viktig förutsättning för att människor utan hämningar ska kunna utöva sin informationsfrihet och utveckla sin individualitet.[31] Såväl automatisering som anonymisering, tillval och hemliga föreskrifter är steg bort från detta. Den nya praxisen och dess normer stödjer alltså kontextens värden sämre än de existerande, och det finns enligt *contextual integrity*-ramverket skäl att avstå från att teckna avtal om automatiserad utlämning enligt tillämpningsanvisningens utgåva 1.1.1 från augusti 2012. Jag anser dock att det är möjligt att ta fram en tillämpningsanvisning som tvärtom bättre skulle stödja kontextens relevanta värden, inte

[29] I oktober 2013 skrev tidningarna om att den manuella hanteringen är dyr för de brottsbekämpande myndigheterna. Särskilt Tele2 fick kritik för att man tog ut höga avgifter. Operatörerna framförde att prissättningen bland annat skett av integritetsskäl, dels då ett dyrare pris förväntades medföra en automatisk avhållsamhet från myndigheternas sida och dels då det gav teleföretagen möjlighet att granska varje begäran för sig. Se till exempel Carlsson (2014).

[30] Brickman skriver om polisen, men givetvis gäller samma resonemang även för Säpo.

[31] Tele2:s agerande är ett exempel på en konkret manifestation av känslan av ett gemensamt intresse, se Kleja 2013c.

minst då en standardisering kan främja ordning och reda i utlämnandet. Detta förutsätter att man inkluderar betryggande kontrollfunktioner och avstår från att automatisera processen fullt ut.

Hemlig dataavläsning – legala spiontrojaner

Den 24 april 2014 rapporterade Dagens Juridik att ”Säkerhetspolisen och Åklagarkammaren för säkerhetsmål vill införa ett nytt hemligt tvångsmedel i Sverige – hemlig dataavläsning där en ’spiontrojan’ planteras i en dator så att myndigheterna kan följa vad datoranvändaren gör” (Wahlberg 2014). Artikeln var ett referat från en debatt i regi av Svenska kriminalistföreningen. Bland paneldeltagarna fanns Tomas Lindstrand, Chefsåklagare vid Åklagarkammaren för säkerhetsmål, och biträdande säkerhetspolischefen Johan Sjöö. Bägge ansåg att Säpo borde få lov att använda sig av hemlig dataavläsning.

Förslaget är inte nytt. Det nämns också i artikeln att det har avvisats av lagstiftaren. Hemlig dataavläsning föreslogs som ett nytt tvångsmedel av Beredningen för rättsväsendets utveckling, under ledning av förre Säpochefen Anders Eriksson, i *SOU 2005:38*. Beredningen ansåg att en ny lag, till att börja med temporär under fem år, borde införas. Den skulle innebära att myndigheterna, efter domstolsbeslut, i huvudsak vid förundersökning angående brott som kunde ge två års fängelse men även vid till exempel dataintrång, kunde ”i hemlighet sänd[a] en viss mjukvara till en dator”, alternativt placera ”hård- eller mjukvara med liknande funktion […] i den informationsbärande utrustningen genom ett fysiskt ingrepp, t.ex. vid ett hemligt intrång i en persons bostad eller på dennes arbetsplats” (SOU 2005:38:50). Genom denna utrustning skulle myndigheterna sedan kunna få ”uppgifter om vilken information som finns i datorn och hur datorn används, med andra ord såväl historiska uppgifter som uppgifter som genereras under verkställigheten” (A. a.). Hemlig dataavläsning skulle få äga rum även om det inte fanns någon person som var skäligen misstänkt för brottet, om den syftade till att fastställa vem som skäligen kunde misstänkas.

Vad gällde den personliga integriteten skrev man i utredningens sammanfattning att ”[o]mfattningen av det integritetsintrång som skulle bli följden om dataavläsning användes kan vara svår att uppskatta generellt och blir naturligtvis beroende av omständigheterna i det enskilda fallet. I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte kommer att bli större än vid tvångsmedlen hemlig teleavlyssning och hemlig kameraövervakning” (SOU 2005:38:54).

Denna bedömning delades dock inte av Advokatsamfundet. I sitt remissvar kritiserade man att inte bara elektronisk kommunikation utan även allt innehåll i datorn, som kunde vara mycket omfattande, skulle kunna avläsas, samt att samtal mellan personer i de rum där utrustningen förvarades skulle kunna avlyssnas i realtid – så kallad buggning (Ramberg 2005; Ramberg 2007). Advokatsamfundet pekade även på problemen med att de datorer som kom ifråga för hemlig dataavläsning skulle kunna finnas hos affärsdrivande företag, att åtgärden skulle innebära ett intrång i det främmande rikets suveränitet om informationssystemet helt eller delvis befann sig utomlands, samt att andra aktörer skulle kunna uppmärksammas på och utnyttja samma säkerhetsluckor som myndigheterna.

Även Datainspektionen var starkt negativ i sitt remissvar (Datainspektionen; Kleja 2005). Liksom Advokatsamfundet kritiserade man att all information som lagrats i datorn skulle kunna avläsas. Man uttryckte även skarp tveksamhet till att hemlig dataavläsning skulle

kunna riktas emot andra än skäligen misstänkta, och anmärkte på att begreppet *informationssystem*, som används i lagförslaget, inte var närmare definierat. Datainspektionen påpekade att myndigheterna därmed skulle ha rätt att skicka in trojaner även i portabel utrustning som mobiltelefoner och gps-mottagare (Kleja 2005).

Att förslaget om hemlig dataavläsning aldrig genomfördes betyder inte att det är överspelat. Tvärtom är det levande i debatten, vilket exemplet från Dagens Juridik visar. Utredningen om vissa hemliga tvångsmedel valde också att i *SOU 2012:44* kommentera hemlig dataavläsning trots att förslaget föll utanför dess uppdrag. Man ansåg sig ha ”stöd för att tvångsmedlet hemlig dataavläsning skulle kunna medföra beaktansvärd nytta för de brottsbekämpande myndigheterna”, samtidigt som integritetsintrången som det skulle kunna medföra ”i vissa fall skulle kunna vara berättigade” och föreslog att frågan utreds (SOU 2012:44:767 och 768).

Analys av förslaget om hemlig dataavläsning

Den information som kan avläsas med till exempel en trojan ingår i ett flertal olika *informationsflödeskontexter* som var och en styrs av sina normer. Om avläsningen, som Datainspektionen befarar, dessutom kan vidgas till att omfatta mobiltelefoner och annan handhållen utrustning blir kontexterna än fler.

Det kan finnas ett stort antal olika *sändare*. Datorägaren förstås, men denne kan ju även vara *mottagare* av den information som avläses (vid tillfället för avläsningen eller tidigare). *Mottagarna* är också många: avläsningen kan fånga olika typer av elektronisk kommunikation, samtal i rummet där datorn står, information som inte är ämnad att skickas alls (som dikter för skrivbordslådan, eller gps-koordinaterna till svampstället), och dessutom datorägarens informationssökningar på webben. *Objekten* är alla personer som informationen handlar om, det kan vara en eller en oöverskådlig mängd. *Informationsslagen* kan också vara få eller oändligt många. Och *sändnings/överföringsprinciperna* skiljer sig mellan kontexterna.

De normer som styr *informationsflödena* i kontexterna är olika, och därmed människors förväntningar. Elektronisk kommunikation brukar ofta liknas vid vykort – meddelanden som man måste utgå ifrån att andra läser. E-postmeddelanden och annan elektronisk kommunikation räknas dessutom i lagstiftningen som telemeddelanden och kan avläsas genom hemlig teleavlyssning (SOU 2005:38). I kontexten av förtroliga samtal finns däremot normer om stark sekretess, i synnerhet om informationen rör privatlivet. För det man skriver men aldrig visar är hemligstämpeln norm. Och informationssökning på nätet liknas av Nissenbaum vid besök på ett bibliotek, som ska respekteras som en del av informationsfriheten (Nissenbaum 2010).

Jag har här ingen möjlighet att analysera alla olika *informationsflödeskontexter* var för sig, utan väljer att röra mig på ett övergripande plan och ser på kontexten ”datoranvändande”. Bland de generella normer som formar denna finns förväntningen att datorer kan skyddas med personliga lösenord, och så även e-postprogram, sociala medier och dylikt. Man kan dessutom välja att lösenordskydda enstaka filer, eller att spara dem i format som inte tillåter ändringar.

Få av oss tvekar inför att lämna ut lösenord till personer som ska hjälpa oss att få datorn att fungera – kanske oftast släktingar eller vänner, men jag har även bevittnat hur lösenord lämnats per telefon till kundtjänstanställda. Vi tvekar inte heller inför att låta supportfunktion på vår arbetsplats ”ta över” datorn. Ändå är det nog inte många som har tänkt tanken att

avlyssning/filmning kan ske via datorn i realtid. Om vi trots allt tänker den, så ser vi detta som en annan och allvarligare typ av intrång än informationsavläsningen.

Det finns en medvetenhet om att alla datorer som är anslutna till internet potentiellt kan smittas med virus och trojaner som kullkastar alla försök till lösenordsskydd. På liknande sätt följer med installationen av brandväggar, kryptering och dylikt känslan att det finns möjlighet till skydd, men att detta är aldrig komplett. Man är hela tiden är ett steg efter hackarna.[32] Dessa är ute efter att stjäla det som är värdefullt: konto- och kortuppgifter, lösenord, kontaktlistor som kan användas för spamutskick, och porrbilder. De förväntas inte kopiera hela hårddisken.

Våra datorer rymmer en närmast oöverskådlig mängd information, med bäring på varje livssituation vi befunnit oss i, och sparad enligt svårbegripliga privata katalogsystem. Vi förväntar oss inte att någonsin behöva visa eller förklara vårt informationsinnehav för någon annan person. Ställda inför tanken om hemlig dataavläsning vill vi att Säpo, på motsvarande sätt som hackarna, inte avläser annat än det väsentliga. Även den som författar bombrecept ska kunna ha sina kärleksdikter i fred.

Hur påverkas de olika faktorer som styr *informationsnormerna* av att man inför hemlig dataavläsning?

En *mottagare* läggs till. *Sändaren* påverkas av vetskapen om att hemlig dataavläsning skulle kunna äga rum (i och med att riksdagen så beslutat). Informationens *objekt*, liksom *informationsslagen* förändras genom att annan slags information (mer, till exempel utkast och anteckningar för eget bruk) kan nå tredje person. Och *sändnings/överföringsprinciperna* påverkas såtillvida att det som skulle förbli osänt blir ”sänt”.

Sammanfattningsvis medför hemlig dataavläsning alltså en förändring av *mottagare*, *sändare*, *objekt*, *informationsslag* samt *sändnings/överföringsprinciper* – och därmed en *prima facie* kränkning av *contextual integrity*.

Nästa steg i analysen är att undersöka de moraliska och politiska faktorer som påverkas. I *SOU 2005:38* likställs hemlig dataavläsning genomgående med hemlig teleavlyssning och hemlig kameraövervakning. Utan att någon djupare jämförelse sker etableras en föreställning om likhet som ligger till grund för förslag om att kopiera existerande lagstiftning när de lagar som reglerar hemlig dataavläsning ska skrivas fram. Man skriver att integritetsintrånget inte kommer att bli större och att hemlig teleavlyssning och kameraövervakning till och med ”i de flesta fall anses innefatta en mer total kontroll av och insyn i en persons förehavanden än vad dataavläsning innebär” och dessutom ”typiskt sett […] en större risk för att personer som är ovidkommande för en brottsutredning drabbas av ett integritetsintrång” (SOU 2005:38:368).[33]

Frågan är dock om det inte i många fall förhåller sig tvärtom. Även i samband med telefonavlyssning och kameraövervakning registreras irrelevant information. Men här kan mängden öka något så ofantligt. Inte minst rymmer den mobila tekniken detaljerad

[32] Bennet (1997) påtalar att människors tillgång till ”integritetsskyddsteknik” (Privacy Enhancing Technologies), dessutom är mycket ojämn, av flera olika skäl. Bland annat finns ett underskattat behov av utbildning.

[33] Naarttijärvi påpekar för övrigt att den tekniska utvecklingen ”motiverar […] utvidgningar av inhämtningsmöjligheterna, men […] sällan [tycks] göra lagstiftaren benägen att införa inskränkningar utifrån att tidigare existerande inhämtningsmöjligheter kommit att innebära större integritetsintrång.” (2013:517).

information om mängder av privata vardagsförhållanden. Utredningen skriver att det är ”möjligt att i viss utsträckning precisera och begränsa vilken information man vill ha uppgift om” genom utformning av mjukvaran (SOU 2005:38:361). Man gör dock inga försök att reglera detta, vilket gör att påståendet framstår som naivt.

Vidare argumenterar man för att det, liksom för hemlig teleavlyssning men till skillnad från vad som gäller för hemlig kameraövervakning, inte ska finnas en regel som anger att upptagningar som saknar betydelse från brottsutredningssynpunkt ska förstöras omedelbart efter det att de har granskats. Motiveringen är att det är svårt att ”vid varje särskild tidpunkt” veta vad som har eller saknar betydelse. Det är uppenbart att denna regel öppnar för att mycket stora mängder av information kommer att sparas.

Om utrustningen för den hemliga dataavläsningen kommer i form av hårdvara krävs för installationen ett fysiskt intrång. I utredningen föreslås att utrustningen tas bort eller görs obrukbar så snart som möjligt efter att avläsningen avslutats. Man påtalar i detta sammanhang skillnader jämfört med hemlig teleavlyssning: Dels att inget intrång krävs vid hemlig teleavlyssning, men också att ”[o]peratörernas nödvändiga medverkan vid den verkställigheten innebär bl.a. att polisen kan värja sig mot obefogade anklagelser om omfattande eller otillbörlig avlyssning” (SOU 2005:38:390). Utredningens slutsats blir att det även vid hemlig dataavläsning finns behov av ”en [sic] slags yttre kontroll av att verkställighet inte fortgår t.ex. efter det att tillståndet har upphört” (SOU 2005:38:391). Man föreslår därför att åklagaren ska underrätta domstolen när det tekniska hjälpmedlet har tagits bort eller gjorts obrukbart. Här finns dock en skillnad. I fallet hemlig teleavlyssning är det operatörerna som äger den tekniska åtkomsten och helt sonika kan strypa tillgången. När det gäller hemlig dataavläsning kan man behöva operatörernas medverkan för installationen (genom ett aktivt försämrat virusskydd), men den kan också ske via en existerande sårbarhet. Då blir det frågan om att till domstolen lämna ett besked om att Säpo själv stängt av utrustningen. Om intrånget sker genom att man utnyttjar sårbarheter som man därmed inte rapporterar försämras datasäkerheten generellt, vilket kan utnyttjas av exempelvis kriminella eller främmande makt. Och om man istället skulle tvinga operatörerna att aktivt försämra virusskyddet förändras relationen mellan företag och kund på ett sätt som strider emot de förväntningar som finns i den existerande praxisen.

Hemlig dataavläsning beskrivs som en riktad åtgärd som ska användas vid utredning av grova brott och organiserad brottslighet. Intrycket är att den riktas mot små grupper av personer. Men i själva verket kan de personer som övervakas vara få eller oändligt många – förutom den som får trojanen skickad till sin dator, även alla som han eller hon har kontakt med på elektronisk väg eller samtalar med på platser där datorn (eller eventuellt mobiltelefonen) befinner sig. Dessutom vill man att hemlig dataavläsning ska kunna ske av informationssystem i ”någon annans stadigvarande bostad”, om det finns synnerlig anledning att tro den misstänkte ”har använt eller kommer att använda sig av detta” (SOU 2005:38:384ff). Förutom vid grova brott, hets mot folkgrupp och barnpornografibrott som inte är att anse som ringa, föreslås hemlig dataavläsning få äga rum vid förundersökning angående dataintrång, ett brott där straffskalan börjar med böter. Detta är konsistent med att hemlig teleövervakning sedan 1 oktober 2004 får genomföras vid förundersökning om dataintrång.

I utredningen understryks vikten av att hemlig dataavläsning omgärdas av ”tydliga och strikta ramar”, med ”rättssäkerhetsgarantier som säkerställer att bestämmelserna inte kan missriktas” (SOU 2005:38:369). Detta anser man tillgodoses genom att beslutsrätten inte i något fall kan

delegeras till de verkställande myndigheterna eller åklagare utan ligger hos domstolen, att åtgärden används i utredningar av grova brott, och med ett ”starkt skydd för den personliga integriteten” (SOU 2005:38:369). Det sistnämnda uppnås genom att ”rätten får föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när”[34], samt att ett offentligt ombud utses för att vara motpart till åklagaren i domstolen i syfte att bevaka enskildas integritetsintressen (både den person som tvångsmedelsanvändningen riktas mot, som förstås inte kan underrättas om detta, och tredje mans integritetsintressen), och att de grundläggande principerna för tvångsmedelsanvändningen följs. Dessutom ska en årlig redovisning av tillämpningen lämnas till riksdagen.

Självklart är det positivt med denna form av regleringar och kontroll. Iain Cameron, professor i folkrätt vid Uppsala universitet, påpekar dock i en artikel i Svensk Juristtidning 2007 att allvarlig problematik följer av att man låter domstolar besluta om tvångsmedelsanvändning utifrån underrättelsematerial. Hans resonemang förtjänar att citeras i sin helhet (Cameron 2007:93):

> *”Sådant material består i regel av olika typer av riskbedömningar. Domstolar har förhållandevis lite erfarenhet av sådana. Domstolsprövning är inget skydd mot maktmissbruk om domarna, i praktiken, saknar tillräckligt intresse eller självförtroende att ingripa och förbjuda en åtgärd, när den nationella säkerheten påstås vara i fara. Detta illustrerades av de extremt långvariga avlyssningarna av vänstergrupper för påstådd olagligt kårverksamhet under 1960 och 1970-talet. Man kan säga att det också idag finns få incitament för en domstol att inte godkänna telefonavlyssning, men många incitament för att godkänna densamma.”*

Ytterligare en aspekt på rättssäkerheten är myndighetens eventuella underrättelseskyldighet gentemot den enskilde. En ledamot i den referensgrupp som knöts till utredningen ansåg att en sådan skulle införas och att de personer som utsatts för hemlig dataavläsning vid icke fällande dom skulle ha möjlighet att få skadestånd, på samma sätt som i Danmark. Utredningen bedömde dock att det ”inte är aktuellt att överväga frågan nu, utan att det får ske i ett annat sammanhang än i detta betänkande” (SOU 2005:38:371). Detta är i mina ögon ett mycket märkligt sätt att hantera frågan. Vilket sammanhang är bättre lämpat än det betänkande som lägger fram ett lagförslag om hemlig dataavläsning?

Det framgår tydligt av utredningen att hemlig dataavläsning står högt på önskelistan hos både Säpo och den öppna polisen (SOU 2005:38).[35] Samtidigt finns det skäl att tro att implementeringen kommer att vara förenad med svårigheter. Utredningen beskriver de tekniska komplikationer som möter polisen. Förmodligen måste man använda sig av mycket avancerad datateknik och det är rimligt att anta att det endast finns ett fåtal personer som har tillräcklig expertis. Man beskriver även hur kriminella anpassar sig till polisens arbetsmetoder. Samma slags anpassning måste även antas komma ske till hemlig dataavläsning. Frågan är då hur användbart verktyget egentligen blir.

Stödjer den gamla eller nya praxisen bäst kontextens relevanta *värden*? Enligt utredningen ska hemlig dataavläsning kunna användas vid brott som kan ge minst två års fängelse men även till exempel dataintrång. Detta innebär att man tänker sig att samhällsskyddet mot dataintrång sker genom dataintrång. De flesta av oss tvekar inte att ge ut våra lösenord till ”goda krafter”

---

[34] Man diskuterar inte hur dessa villkor skulle se ut eller när de ska användas.

[35] Detta iakttar även Utredningen om vissa hemliga tvångsmedel som i SOU 2012:44:765 skriver att ”de brottsbekämpande myndigheterna […]med viss emfas framhållit att det finns ett behov av tvångsmedlet och att det bör införas”.

som kan hjälpa oss att få våra informationssystem att fungera och radera skadlig programvara. Här finns alltså pudelns kärna – ser vi Säpo som en sådan ”god kraft”, som jagar hackare och yrkeskriminella inifrån deras datorer men aldrig tar med sig någon oväsentlig information om enskildas privatliv? Tror vi att integritetsskyddet är tillräckligt omfattande och att reglerna är tillräckligt strikta? Jag ser tydliga brister i den kontroll och de ramar som beskrivs i utredningens förslag och anser därmed att *contextual integrity*-ramverket inte stödjer införandet av hemlig dataavläsning enligt det förslag som läggs fram i *SOU 2005:38*.

Inte bara balans

Naarttijärvi har kunnat visa att lagstiftarens proportionalitetsavvägningar kring integritetsfrågorna är behäftade med stora brister. Det saknas inte förslag till förbättringar. Integritetsskyddskommitténs ordförande Olle Abrahamsson förordar till exempel en metod med tre rangskalor där olika integritetsbegränsande åtgärder bedöms i förhållande till varandra (Abrahamsson 2009). Den första ska ställas upp utifrån de faktiska värderingar som är rådande i samhället, utan hänsyn till syftet. Den andra ska enbart ta hänsyn till åtgärdernas effektivitet. Och den tredje ska ställas upp utifrån ”graden av acceptans hos befolkningen”, med hänsyn till sammanhanget, då acceptansen varierar utifrån syftet. Abrahamssons arbete är lovvärt, men frågan är i vilken utsträckning ett sådant system skulle förändra dagens situation. De olika åtgärderna relateras uteslutande till varandra och den analys som blir resultatet kan därför misstänkas likna resonemanget i SOU 2005:38 kring integritetsaspekterna på hemlig dataavläsning i förhållande till hemlig teleavlyssning och hemlig kameraövervakning.

Marie Demker, professor i statsvetenskap vid Göteborgs universitet, förespråkar å sin sida att den personliga integriteten på internet blir föremål för transnationella överenskommelser eller avtal på EU- eller FN-nivå, på motsvarande sätt som de mänskliga rättigheterna hanteras idag, även om hon bedömer utsikterna att få till sådana avtal som små så länge frågorna inte ”politiseras på en övernationell nivå” (det vill säga formuleras som en konflikt mellan två motstående intressen eller politiska partier) (Demker 2014:48). Demkers idé är god och det är väl värt för den svenska regeringen att lyfta den i lämpliga internationella samarbetsorgan. Men de svårigheter som hon pekar på är en krass realitet och den personliga integriteten kan inte sättas på undantag tills internationella avtal kommer till stånd. Dessutom sträcker sig behovet mycket längre än enbart till integriteten på internet – i takt med att nya tekniska landvinningar sker krävs integritetsbedömningar på allt fler områden.

Naarttijärvi skriver att ”[n]ågon form av intresseavvägningar är oundvikliga utifrån den rättsliga konstruktionen av skyddet för den personliga integriteten […]” (2013:523). Det är onekligen sant. Det finns därför klara poänger med att strukturera och formalisera proportionalitetsövervägandena, men jag menar att det dessutom skulle vara gynnsamt att ha tillgång till fler verktyg för bedömningen.

Kan Nissenbaums ramverk för *contextual integrity* utgöra ett sådant? Ja, sannolikt kan det komplettera de bedömningar som idag sker i lagstiftningsarbete som till exempel rör underrättelseverksamhet, men även i situationer när man överväger att förändra Säpos teknikanvändning inom ramen för vad som är tillåtet enligt lag, eller i en diskussion där säkerhets- och underrättelsetjänsten ställs inför anklagelser om kränkningar av den personliga integriteten.

En proportionalitetsbedömning sker med nödvändighet i form av en juridisk värdering. I det fält som utgörs av lagstiftarens offentliga utredningar med direktiv, förarbeten och departementspromemorior är praxis dessutom att man ser tillbaka på hur andra gjort. Nissenbaum tar istället sin utgångspunkt i filosofisk metod och introducerar ett sätt att tänka som inte ställer värden mot varandra och inte drar paralleller till andra sammanhang eller tidigare bedömningar.

Genom att introducera Nissenbaums teori i ett bredare perspektiv kan man dessutom förvänta sig att förändra diskussionen om *personlig integritet* så att denna blir mer mångsidig och lättillgänglig. Detta är inte minst viktigt.

Fred Schreier, som är seniorkonsult vid Geneva Centre for the Democratic Control of Armed Forces och som engagerat sig i frågan om styrning och kontroll av underrättelse- och säkerhetstjänster har, på en generell nivå, påpekat att det hemlighetsmakeri som omgärdar underrättelseverksamheten medför att den av allmänheten inte bara ses som mystisk, utan dessutom som tygellös och utanför lagen (Schreier 2007).

Agrell har iakttagit precis den här typen av mekanismer i debatten om den personliga integriteten efter 2001. Han skriver att det inte bara rått skilda uppfattningar om vilken balans mellan integritet och övervakning som är rimlig i förhållande till de hot som kan iakttas, utan att även ”historiskt grundade misstankar” kommit till ytan ”om att övervakningen beskrivs på ett sätt offentligt, men i hemlighet ser helt annorlunda ut; medborgarna är utsatta för övervakning som de inte är informerade om och än mindre fått godkänna” (Agrell 2014:8).

Även i de fall som jag har undersökt finns åtskilligt som riskerar att (rätt eller orätt) skapa och underhålla den här typen av misstankar:

Standardiseringsdokumentet ReportITS27 är daterat den 1. augusti 2012 men kom till allmänhetens kännedom först ett år senare (ReportITS27 2012; Kleja 2013a). Det framkom då också att Säpo utövade påtryckningar på teleoperatörerna vid hemliga möten och att varken Säkerhets- och integritetsskyddsnämnden eller Datainspektionen informerats om avsikten att införa ett helautomatiserat system (Djelevic och Gagliano 2013a och 2013b; Kleja 2013c). Ytterligare frågor har väckts av PTS hantering av sin rättsutredning, där man i det längsta försökt att dölja dess existens (Funcke 2014a, 2014b och 2014c; Bahnhof 2014c och 2014d).

Av kapitlet om hemlig dataavläsning i SOU 2005:38 framgår att polisen inte alltid velat lämna utredningen detaljerad information. Beredningen skriver dessutom att man av sekretesskäl inte kan redogöra för uppgifter man fått om åtgärdens effektivitet. För läsaren framstår det som märkligt att det ens föreligger sådana uppgifter för en åtgärd som inte är tillåten. Är det frågan om bedömningar eller internationella erfarenheter, borde de kunna omtalas åtminstone i allmänna ordalag. Vidare avfärdar utredningen frågan om myndighetens eventuella underrättelseskyldighet gentemot den enskilde med att denna borde hanteras i ett annat sammanhang - oklart vilket. Någon proportionalitetsbedömning genomförs inte och på det hela taget upplevs resonemanget kring förslagets konsekvenser för integriteten som ofullgånget.

Det är svårt för domstolar, politiska aktörer och medborgare att sätta sig in i, utvärdera och i förekommande fall argumentera emot åtgärder som motiveras med att hot föreligger mot den nationella säkerheten, inte minst som de saknar insyn i och kunskaper om underrättelseorganisationernas arbete (Cameron 2007; Demker 2014). När processerna sköts

på detta sätt blir komplikationerna än fler. Den misstänksamhet som skapas påverkar inte bara förtroendet för underrättelse- och säkerhetstjänsten utan riskerar i förlängningen att urholka själva samhällstilliten.

I diskussioner som rör förhållandet mellan övervakning och integritet finns därmed, kanske mer än i andra politiska frågor, allt att vinna på att ”komma överens och tänka efter före”, för att låna ett uttryck som Olof Ruin, professor emeritus i statsvetenskap vid Stockholms universitet, använt för att beteckna de historiska särdragen i svensk politik. Vid utvärderingen av integritetsaspekter på lagförslag och åtgärder som berör underrättelseverksamhet bör man eftersträva en så bred och öppen diskussion som möjligt. Här kan *contextual integrity*-ramverket spela en viktig roll.

Referenser

Agrell, Wilhelm (2014) i Wilhelm Agrell och Marie Demker, ”Världen efter Snowden. Övervakning till vilket pris?”, *Världspolitikens Dagsfrågor 2014/7-8,* Stockholm: Utrikespolitiska institutet.

Abrahamsson, Olle (2009) ”Integritetsskydd med eller utan förnuft”, *Svensk Juristtidning,* nr. 1, 421-434.

Backman, Stefan (2014a) mailkonversation 18 augusti, *RE: fråga om PTS föreläggande.*

Backman, Stefan (2014b) mailkonversation 4 november, *RE: fråga om PTS föreläggande.*

Bahnhof (2014a), ”Efter EU-domen: Bahnhof upphör med all datalagring omedelbart”, *Bahnhof.se,* pressmeddelande 8 april, läst 1 augusti: https://www.bahnhof.se/press/press-releases/2014/04/08/efter-eu-domen-bahnhof-upphor-med-all-datalagring-omedelbart.

Bahnhof (2014b) ”Anmäler sig själv för utebliven datalagring”, *Bahnhof.se,* pressmeddelande 8 juli, läst 18 augusti: https://www.bahnhof.se/press/press-releases/2014/07/08/anmaler-sig-sjalv-for-utebliven-datalagring.

Bahnhof (2014c) ”Vad försöker ni dölja, PTS?”, *Bahnhof.se,* pressmeddelande 1 oktober, läst 3 november: https://www.bahnhof.se/press/press-releases/2014/10/01/vad-forsoker-ni-dolja-pts.

Bahnhof (2014d) ”Brevet som PTS inte vill att du ska läsa”, *Bahnhof.se,* pressmeddelande 24 oktober, läst 3 november: https://www.bahnhof.se/press/press-releases/2014/10/24/brevet-som-pts-inte-vill-att-du-ska-lasa.

Bahnhof (2014e) ”Bråket om datalagringen: PTS hotar Bahnhof med miljonbelopp”, *Bahnhof.se,* pressmeddelande 27 oktober, läst 3 november: https://www.bahnhof.se/press/press-releases/2014/10/27/braket-om-datalagringen-pts-hotar-bahnhof-med-miljonbelopp.

Bahnhof (2014f) ”Bahnhof aktiverar ”plan B”: erbjuder fri anonymisering”, *Bahnhof.se,* pressmeddelande16 november, läst 17 december: https://www.bahnhof.se/press/press-releases/2014/11/16/bahnhof-aktiverar-plan-b-erbjuder-fri-anonymisering.

Bennet, Colin J. (1997) ”Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?”, i Philip E. Agre och Marc Rotenberg, *Technology and Privacy: The New Landscape,* Cambridge Massachusetts och London: The MIT Press.

Bennet, Colin och Charles Raab (2007) ”The Privacy Paradigm” i Sean P. Hier & Joshua Greenberg (red.) *The Surveillance Studies Reader,* Maidenhead och New York: Open University Press.

Bergman, Annika (2014) Brev 16 juni: ”Angående lagring av trafikuppgifter m.m. för brottsbekämpande ändamål”, *Post- och telestyrelsen.*

Brickman, Annika (2007) ”Vad får man tåla?”, *Svensk Juristtidning,* nr. 1.

Bylund, Markus (2013) *Personlig Integritet på nätet*, Stockholm: Fores.

Cameron, Iain (2007) ”Brottsbekämpning, rättssäkerhet och integritet – vissa internationella trender”, Svensk Juristtidning, nr. 1, 83-98.

Carlsson, Ulf (2014) ”Tele2 slutar att hjälpa polisen lösa brott, *Östran* 16 april, läst 16 augusti 2014: http://www.ostran.se/layout/set/popup/NYHETER/Kalmar/Tele2-slutar-att-hjaelpa-polisen-loesa-brott.

Computer Sweden, 10 april 2014, ”PTS: okej att sluta lagra” http://www.idg.se/2.1085/1.556263/pts--okej-att-sluta-lagra.

Datainspektionen, ”Vad menas med en kränkning av den personliga integriteten?”, *Frågor och svar*, läst 1 juli 2014: http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-menas-med-en-krankning-av-den-personliga-integriteten1/.

Demker, Marie (2014) i Wilhelm Agrell och Marie Demker, ”Världen efter Snowden. Övervakning till vilket pris?”, *Världspolitikens Dagsfrågor 2014/7-8*, Stockholm: Utrikespolitiska institutet.

Dir. 2004:51, *Skyddet för den personliga integriteten*, Justitiedepartementets kommittédirektiv.

Djelevic, Milan och Alexander Gagliano (2013a) ”Så pressar Säpo operatörerna. Abonnenterna behöver aldrig få veta”, *Ekot* 17 december, Sveriges Radio, läst 1 augusti 2014: http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5735453

Djelevic, Milan och Alexander Gagliano (2013b) "’Därför informerade inte Säpo kontrollmyndigheterna.’ Ska träffa Säpo i dag”, *Ekot* 19 december, läst 1 augusti: https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5738020.

Ds 2014:23, *Datalagring, EU-rätten och svensk rätt*, Justitiedepartementet.

Eriksson, Gustaf (2013) ”Kritiken: Operatörerna struntar i integriteten”, *Metro* 21 november, läst 1 augusti 2014 http://touch.metro.se/teknik/kritiken-operatorerna-struntar-i-integriteten/EVHmku!7JtuyAoKLMHa/.

European Telecommunications Standards Institute (2010) ”Interception (LI);
Retained data handling; Handover interface for the request and delivery of retained data”, *ETSI TS 102 657*, V1.6.1 (2010-09), läst 31 juli 2014: http://www.etsi.org/deliver/etsi_ts/102600_102699/102657/01.06.01_60/ts_102657v010601p.pdf.

“Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter”, *Europeiska gemenskapernas officiella tidning* nummer L 281, 23/11/1995, 31-50.

Europeiska unionens domstol (2014) *Dom i de förenade målen C-293/12 och C-594/12 Digital Rights Ireland och Seitlinger m.fl.*, pressmeddelande 8 april nr 54/14.

Funcke, Nils (2014a) "När det gäller rättsutredningen om datalagring vill PTS både ha kakan och äta den", *Dagens Juridik* 24 oktober, läst 3 november: http://www.dagensjuridik.se/2014/10/nar-det-galler-rattsutredningen-om-datalagring.

Funcke, Nils (2014b) ”Anmälan”, *www.nilsfuncke.se* 14 november, läst 17 december 2014: http://www.nilsfuncke.se/wp-content/uploads/2014/11/JO-anmälan-PTS-inklusive-bil.pdf.

Funcke, Nils (2014c) ”PTS anmält till JO”, *www.nilsfuncke.se* 17 november, läst 17 december: http://www.nilsfuncke.se/tag/bahnhof/.

Gagliano, Alexander och Milan Djelevic (2013) ”Säpo vill hemligstämpla allt samarbete med teleoperatörer. ’Vi håller truten om det’", *Ekot* 18 december, läst 1 augusti 2014: https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5736819.

Gavison, Ruth (1980) ”Privacy and the Limits of Law”, *The Yale Law Journal*, Vol. 89, No. 3.

Glancy, Dorothy J. (1979) ”The Invention of the Right to Privacy”, *Arizona Law Review*, vol. 21, nr. 1.

Gutwirth, Serge for the Rathenau Institute (2002[2001]), *Privacy and the Information Age*, översättning Raf Casert, Lanham, Boulder, New York, Oxford: Rowman & Littlefield Publishers, Inc.

Hern, Alex (2014) ” British government 'breaking law' in forcing data retention by companies. EU directive overturned in April but UK continues to make telecoms and internet firms comply with legislation”, *The Guardian* 24 juni, läst 17 augusti 2014: http://www.theguardian.com/technology/2014/jun/24/british-government-breaking-law-in-forcing-data-retention-by-companies.

Informationstekniska Standardiseringen (2014) “EU:s datalagringsdirektiv* har ogiltigförklarats av EU-domstolen”, *Its.se*, nyheter 8 april, läst 25 juli 2014: http://www.its.se/eus-datalagringsdirektiv-har-ogiltigforklarats-av-eu-domstolen/.

Ju2014/3010/P, *Uppdrag med anledning av EU-domstolens dom om datalagringsdirektivet*, Justitiedepartementet.

Kleja, Monica (2005) “Datarådet säger nej till polisens hemliga trojaner”, *Ny Teknik* 19 december, läst 1 augusti 2014: http://www.nyteknik.se/nyheter/it_telekom/allmant/article246145.ece.

Kleja, Monica (2013a) ”Säpos krav: Flöden från operatörerna”, *Ny Teknik* 6 november, läst 20 juli 2014: http://www.nyteknik.se/nyheter/it_telekom/allmant/article3784822.ece.

Kleja, Monica (2013b) “Vi vill göra en manuell granskning i varje fall”, *Ny Teknik* 6 november, läst 20 juli 2014: http://www.nyteknik.se/nyheter/it_telekom/allmant/article3784825.ece.

Kleja, Monica (2013c) ”PTS tar strid mot Säpos trafikdatakrav”, *Ny Teknik* 17 december, läst 20 juli 2014: http://www.nyteknik.se/nyheter/it_telekom/allmant/article3794376.ece.

Kleja, Monica och Kalle Anrell (2013) ”Säpos krav: Direkttillgång till pukkoder”, *Ny Teknik* 19 november, läst 20 juli 2014: http://www.nyteknik.se/nyheter/it_telekom/allmant/article3788288.ece.

Krattenmaker, Tom (1994) “Privacy in the Computer Age”, *Princeton Alumni Weekly* 26 oktober, vol. 95.

Lag (2010:1408) om ändring i Regeringsformen, Justitiedepartementet.

Lag (2012:127) om ändring i lagen (2003:389) om elektronisk kommunikation, Näringsdepartementet.

Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, Justitiedepartementet.

Litt, Robert S. (2013) *PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection*, tal vid Brookings Institution 19 juli, Washington DC.

Madrigal, Alexis C. (2012) ”The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy”, *The Atlantic* 29 mars, läst 3 juli 2014: http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/.

Naarttijärvi Markus (2013) *För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, Skrifter från Juridiska institutionen vid Umeå universitet, Uppsala: Iustus förlag.

Nationalencyklopedin, Heuristik, läst 16 augusti 2014: http://www.ne.se.ludwig.lub.lu.se/lang/heuristik.

Nationalencyklopedin, Heuristisk, läst 16 augusti 2014: http://www.ne.se.ludwig.lub.lu.se/sve/heuristisk.

Nissenbaum, Helen (2004) ”Privacy as Contextual Integrity”, *Washington Law Review*, vol. 79, nr. 1.

Nissenbaum, Helen (2010) *Privacy in context*, Stanford: Stanford University Press.

Nissenbaum Helen (CV), New York University, läst 16 augusti 2014: http://www.nyu.edu/projects/nissenbaum/main_cv.html.

Post- och telestyrelsen (2014) *PTS kommer inte i nuläget att vidta åtgärder utifrån datalagringsreglerna*, pressmeddelande 10 april, läst 17 augusti 2014: http://www.pts.se/sv/Nyheter/Telefoni/2014/PTS-kommer-inte-i-nulaget-att-vidta-atgarder-utifran-datalagringsreglerna/.

Ramberg, Anne (2005), remissvar, Sveriges Advokatsamfund, diarienummer 2005R-2005/1309.

Ramberg, Anne (2007) ”Tvångsmedel, rättssäkerhet och integritet — går det att förena?”, *Svensk Juristtidning*, nr. 1.

Regeringens proposition 2009/10:80, *En reformerad grundlag*, Justitiedepartementet.

ReportITS27 (2012) - Tillämpningsanvisning/ Application guide, utgåva 1.1.1 2012-08-01, ITS Information Technology Standardization, hämtad 15 maj från: http://www.its.se/standards/ss6363x/Report-ITS27-Ed1.pdf.

Rössler, Beate (2005[2001]) *The Value of Privacy*, översättning R. D. V. Glasgow, Cambridge: Polity Press.

Schreier, Fred (2007) “The Need for Efficient and Legitimate Intelligence” i Hans Born & Marina Caparini (red.) *Democratic Control of Intelligence Services. Containing Rogue Elephants*, , Aldershot UK och Burlington USA: Ashgate.

Sieghart, Paul (1976) *Privacy and Computers*, London: Latimer New Dimensions Limited.

Solove, Daniel J. (2002) ”Conceptualizing Privacy”, *California Law Review*, vol. 90, nr. 4, 1087-1155.

Solove, Daniel J. (2004) *The digital person. Technology and Privacy in the Information Age*, New York och London: New York University Press.

Solove, Daniel J. (2006a) “A Taxonomy of Privacy”, *University of Pennsylvania Law Review* vol. 154, nr. 3.

Solove, Daniel J. (2006b) ”The Digital Person and the Future Of Privacy”, i Katherine J. Strandburg och Daniela Stan Raicu (red.), *Privacy And Technologies Of Identity: A Cross-disciplinary Conversation*, New York: Springer Science+Business Media, Inc.

Solove, Daniel J. (2008a) ”Data Mining and the Security-Liberty Debate”, *The University of Chicago Law Review*, Vol. 75, 343-362.

Solove, Daniel J. (2008b) *Understanding Privacy*, Cambridge Massachusetts och London: Harvard University Press.

SOU 1984:54, *Tvångsmedel - Anonymitet – Integritet*, Justitiedepartementet, Betänkande av Tvångsmedelskommittén.

SOU 1998:46, *Om buggning och andra hemliga tvångsmedel*, Justitiedepartementet, Buggningsutredningen.

SOU 2002:18, *Personlig integritet i arbetslivet*, Näringsdepartementet, Betänkande från Integritetsutredningen.

SOU 2005:38, *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*, Justitiedepartementet, Beredningen för rättsväsendets utveckling.

SOU 2007:22, *Skyddet för den personliga integriteten*, Justitiedepartementet, Delbetänkande av Integritetsskyddskommittén, Del 1.

SOU 2008:3, *Skyddet för den personliga integriteten - Bedömningar och förslag*, Justitiedepartementet, Integritetsskyddskommittén, slutbetänkande.

SOU 2012:44, *Hemliga tvångsmedel mot allvarliga brott*, Justitiedepartementet, Betänkande av Utredningen om vissa hemliga tvångsmedel.

Stone, Geoffrey R. (2010) "Privacy, the First Amendment, and the Internet" i Saul Levmore & Martha C. Nussbaum (red.) *The Offensive Internet: Speech, Privacy and Reputation*, Cambridge och London: Harvard University Press.

Strömholm, Stig (1971) "Integritetsskyddet – Ett försök till internationell lägesbestämning", *Svensk Juristtidning*, nr. 1, 695-736.

Strömholm, Stig (1978) "Integritetsskydd i massmedia", *Nordiskt juristmöte 1978*, bilaga 7.

Svenska stadsnätsföreningen, "FAQ Datalagringstjänsten", *ssnf.org*, läst 12 augusti 2014: http://ssnf.org/informationsbank/Lagar/Datalagring/FAQ-Datalagringsdirektivet/.

Tele2 Sverige (2013) "Tele2 kommenterar medierapporteringen kring automatiserat flöde till myndigheter", *Tele2 Newsroom* 19 november, läst 1 augusti 2014: http://newsroom.tele2.se/nyheter/tele2-kommenterar-medierapporteringen-kring-automatiserat-flode-till-myndigheter/.

The White House, Office of the Press Secretary, 23 februari 2012, *We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online,* , läst 6 juli 2014: http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

Wacks, Raymond (2010) *Privacy. A Very Short Introduction*, Oxford, New York, m.fl.: Oxford University Press.

Wahlberg, Stefan (2014) "Åklagare och Säpo vill införa nytt tvångsmedel – hemliga 'spiontrojaner' i datorer", *Dagens Juridik* 24 april, läst 20 juli 2014: http://www.dagensjuridik.se/2014/04/aklagare-och-sapo-vill-infora-nytt-tvangsmedel.

Warren, Samuel D. och Louis D. Brandeis (1890) "The Right to Privacy", *Harvard Law Review*, vol. 4, nr. 5, 193-220.

Weinstein, Debra (2012) "Inside NYU Steinhardt: Helen Nissenbaum on the White House Bill to Protect Consumers Online", *Privacy, At a Glance, News from the NYU Steinhardt Community* 24 februari, läst 3 juli 2014: http://steinhardt.nyu.edu/site/ataglance/2012/02/inside-nyu-steinhardt-helen-nissenbaum-on-the-white-house-bill-to-protect-consumers-online.html.

Westin, Alan (1967) *Privacy and Freedom*, New York: Atheneum.

Wretman, Catarina (2014a) Brev 19 juni: Underrättelse om bristande uppfyllelse av bestämmelser om lagring av samt ersättning vid utlämnande av trafikuppgifter m.m. för brottsbekämpande ändamål, Post- och Telestyrelsen, Dnr: 14-4175.

Wretman, Catarina (2014b) Brev 27 juni: Föreläggande om efterlevnad av skyldighet att lagra trafikuppgifter m.m. för brottsbekämpande ändamål, Post- och Telestyrelsen, Dnr: 14-4175.

Åhlin, Daniel (2014) ”Comhem slutar också med datalagring”, *Computer Sweden* 11 april, läst 17 augusti 2014: http://www.idg.se/2.1085/1.556460/comhem-slutar-ocksa-med-datalagring.

Övervakning av metadata som spelplan för rättsliga principkonflikter

Markus Naarttijärvi

De senaste tio åren har fört med sig en dramatisk utveckling av de tekniska möjligheterna till övervakning av enskilda och gruppers kommunikationer, liksom en förhållandevis långtgående utvidgning av de rättsliga mandaten till att bedriva sådan övervakning. Utvecklingen i Sverige är på många sätt symptomatisk för en internationell utveckling, där även EU delvis varit drivande genom bland annat skapandet av datalagringsdirektivet. I detta bidrag presenteras utifrån ett konstitutionellt perspektiv tre utvecklingstendenser som präglat framväxten av moderna former av elektronisk övervakning. Därefter presenteras den kollision med grundläggande rättsliga principer som denna utveckling lett fram till, illustrerad av bl.a. EU-domstolens dom i Digital Rights Ireland, och vissa tecken på vad denna kollision kan föra med sig diskuteras. Till sist diskuteras det vägskäl som moderna rättsstater står inför i frågan om synen på, och tillämpningen av övervakningsmöjligheterna i det moderna informationssamhället.

Metadata i rätten

Bakgrund

Så kallad metadata rörande elektronisk kommunikation har på senare tid kommit att hamna i fokus för den allmänna och rättsliga debatten rörande övervakning och den personliga integriteten. Metadata kan i det här sammanhanget kortfattat beskrivas som data om vem som kommunicerat med vem, när, hur, och var. Det kan också röra sig om information om vem som besökt vilken hemsida, eller var en person befunnit sig med sin mobiltelefon. Metadata kan enklast uttryckas som att det innefattar data rörande kommunikation undantaget kommunikationens innehåll (jfr. Prop. 2010/11:46).[36] Det finns sannolikt flera anledningar till det intresse som kommit att riktas mot denna typ av information, men två händelser har särskilt bidragit till att sätta ljuset på metadata. För det första avslöjandena från systemanalytikern Edward Snowden rörande NSA:s massiva övervakning av sådan metadata (Greenwald 2013a; Greenwald 2013b; MacAskill 2013). För det andra debatten kring EU:s datalagringsdirektiv (2006/24/EG) vars syfte var att lagra metadata rörande elektronisk kommunikation i syfte att hjälpa brottsbekämpande myndigheter utreda och förebygga allvarliga brott. Även om metadata således kommit att bli föremål för en mer omfattande diskussion, så är inte tillgången till metadata, eller rättsliga frågor rörande formerna för denna tillgång, någonting nytt i sig. Metadata har redan tidigare varit en spelplan för rättsliga principkonflikter. Däremot så har av olika skäl förutsättningarna för en mer djuplodande diskussion kommit att förändras. I det följande kommer tre tendenser för utvecklingen av myndigheters tillgång till metadata att analyseras, varefter förutsättningarna för denna nya diskussion kommer att beröras utifrån den principiella kollision mot grundläggande rättigheter som metadataövervakning medför.

[36] Det bör dock framhållas att gränsdragningen mellan metadata och innehåll inte alltid är självklar eller given på förhand.

Tre tendenser

Mer data till nya verktyg

Det är på många sätt naturligt att när frågan om inhämtning av kommunikationsmetadata ursprungligen diskuterades i svenska förarbeten på 1950-talet, i samband med införandet av möjligheten till telefonkontroll i vissa säkerhetsmål, så framstod metoden inte som särskilt problematisk. Begreppet metadata användes inte och det rörde sig vid den tiden framför allt om uppgifter rörande vem som ringt vem från fasta telefoner och en möjlighet att förhindra samtal från att nå fram (SOU 1975:95). I fråga om integritetsintrånget vid sådan inhämtning kretsade analysen, såsom den gjort ända sedan dess, främst kring att åtgärden inte kan anses lika känslig som avlyssning av kommunikationens innehåll (SOU 2012:44). Samtidigt kan man konstatera att lagstiftaren trots detta konstanterande tycktes ovillig att släppa allt för mycket på tyglarna. Inhämtning av metadata fick ursprungligen ske endast efter beslut om s.k. *hemlig teleövervakning*, vilket således krävde en tillståndsprövning av domstol. Det krävdes också skälig misstanke mot den person som övervakningen skulle inrikta sig mot, något som lagstiftaren inte ansåg det möjligt att göra undantag ifrån så sent som på slutet av 80-talet.

> *”När det gäller frågan vilken grad av misstanke som skall krävas är jag – av motsvarande skäl som jag redovisat i avsnittet om hemlig teleavlyssning – inte beredd att godta kommitténs förslag om att det skall räcka med att den som skall övervakas kan misstänkas för brottet. jag kan tillägga att det inte ens vid misstanke om de allvarligaste högmålsbrotten och brotten mot rikets säkerhet i 1952 års lag gjorts undantag från kravet på skälig misstanke för att telefonövervakning skall få användas. jag förordar alltså samma misstankenivå som vid hemlig teleavlyssning nämligen skälig misstanke.” (Prop. 1988/89:124:49)*

Under början av 90-talet öppnades dock, närmast av lagtekniska skäl, ett separat spår för tillgång till kommunikationsmetadata. När telemarknaden privatiserades kom vissa undantag i sekretessbestämmelser som Televerket tidigare omfattades av att flyttas över till regelverket för den privata marknaden i telelagen och sedermera till lagen (2003:389) om elektronisk kommunikation (LEK). Innebörden av dessa undantag kom att bli att brottsbekämpande myndigheter kunde få del av historisk metadata från privata operatörer utan föregående beslut av domstol, om den brottsbekämpande myndigheten själv ansåg att förutsättningarna i 6 kap. 22 § 3 p. var uppfyllda (misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år) och om uppgifterna fanns tillgängliga hos operatörerna. Då tolkningen av detta lagrum skedde internt hos den brottsbekämpande myndigheten, och inte prövades i domstol, skulle regelverket i LEK komma att bli föremål för en i sammahanget synnerligen extensiv tolkning. Kravet på misstanke om brott ansågs nämligen inte hindra att uppgifter lämnades ut även inom ramen för underrättelseverksamheten, trots att misstanke om brott samtidigt skulle föranleda att en förundersökning skulle inledas och rättegångsbalkens regler således skulle bli tillämpliga. Inte heller ansågs det krävas att uppgifterna skulle röra någon särskild person, vilket innebar att s.k. basstationstömning ansågs tillåten under bestämmelsens tillämpningsområde.[37] Denna myndighetspraxis fick också stöd i förarbeten, utan att någon rättslig analys presenterades för att underbygga tolkningen och trots att denna typ av ingripanden i den personliga integriteten innebär att lagtolkning ska ske synnerligen restriktivt (se allmänt Naarttijärvi 2013).

[37] Basstationstömning eller ”masttömning” innebär att polisen inhämtar uppgifter om vilka mobiltelefoner som varit anslutna till en viss basstation för mobiltelefoni under ett visst tidsintervall, och kan bl.a. ge ledning till vilka individer som befunnit sig i närheten av denna basstation.

Det går att konstatera att brottsbekämpande myndigheter även drev på för att få tillgång till kommunikationsmetadata under mindre restriktiva former än tidigare. Lagstiftaren kom i detta sammanhang att acceptera de brottsbekämpande myndigheternas beskrivning av den ökade nyttan av denna typ av uppgifter i verksamheten, men tycktes samtidigt ovillig att se över sina tidigare bedömningar av det integritetsintrång som uppgifternas utlämnande innebar (Naarttijärvi 2013). Något motsägelsefullt sågs därför uppgifterna i lagstiftningen som förhållandevis harmlösa ur integritetssynpunkt men på samma gång som centrala för kartläggningen av individer och grupper.

Med tiden kom de tekniska verktygen att möjliggöra en övergång från riktad inhämtning till en mer storskalig sådan. Dels utvecklades möjligheter att inte bara avlyssna och övervaka en bestämd teleadress, så som ett telefonnummer eller IP-nummer, utan att även kunna placera avlyssningsutrustning vid centrala kommunikationsvägar och i praktiken övervaka och avlyssna all den kommunikation som passerar genom dessa. Därutöver utvecklades möjligheten att lagra enorma mängder av denna kommunikation vilket möjliggjorde och underbyggde krav på att sådan lagring skulle äga rum. Än mer relevant i sammanhanget så utvecklades de tekniska verktygen i form av analysmjukvara för att på ett snabbt, billigt och enkelt sätt söka igenom dessa enorma mängder information för att hitta relevanta mönster och kopplingar mellan individer och organisationer. Denna tekniska utveckling skedde parallellt med att vi började generera enorma mängder spårbar elektronisk information genom ett omfattande bruk av elektroniska kommunikationstjänster (UNGA 2014a). Därutöver blev ständigt närvarande mobila kommunikationsverktyg som mobiltelefoner vardagsmat.[38] Såväl mängden tillgänglig data som möjligheterna att analysera den ökade således parallellt.

Ett stort antal reformer rörande metadata kom i slutet av 00-talet att ske under kort tid. År 2007 kom efter en långdragen lagstiftningsprocess, den första uttryckligt preventiva tvångsmedelslagstiftningen som möjliggjorde bl.a. avlyssning och övervakning av kommunikation; lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (hädanefter 2007 års preventivlag). Lagen innebär att rättegångsbalkens hemliga tvångsmedel får tillämpas i ett stadium innan förundersöknings inledande för att förhindra vissa särskilt uppräknade allvarliga brott som faller under Säkerhetspolisens ansvarsområde.

Genom den s.k. FRA-lagen, lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, som trädde i kraft 1 januari 2009, gavs Försvarets radioanstalt möjlighet att avskilja trådbunden kommunikation över Sveriges gränser för analys av metadata och innehåll i syfte att kartlägga fenomen av intresse för rikets säkerhet. Lagen blev föremål för stark debatt och skulle bli föremål för ett antal justeringar över tid, men innebar i sig ett principiellt avsteg från dittills gällande normer för övervakning av kommunikation som får ses som mycket långtgående. Regeringen fick också steg för steg backa från påståendet om att den automatiska genomsökningen av metadata i sig inte innebar något integritetsintrång (jfr. Ds 2005:30; Prop. 2006/07:63).

[38] Intressant att notera är att mobiltelefonernas ständiga närvaro är så påtaglig att det faktum att någon lämnar mobiltelefonen hemma kan ses som ett konspiratoriskt beteende. Det var fallet när en tysk sociolog vid Humboldt universitetet i Berlin greps som misstänkt för terroristbrott med hänvisning till att han träffat intervjupersoner i radikala rörelser utan att ha tagit med sig sin mobil, liksom författat vetenskapliga artiklar innehållande ord som “gentrification” och “inequality” (Sennett & Sassen, 2007; Connolly 2007). Tyska domstolar kom sedermera att bedöma gripandet som baserat på otillräcklig bevisning, men beskrev kontakterna som ”konspiratoriska” (Deutsche Welle 2007)

En ytterligare förändring skedde 2012 genom lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (hädanefter 2012 års inhämtningslag). Lagen var ett resultat av att det regelverk i LEK som beskrivits ovan såvitt avsåg polisens tillgång till uppgifter under förundersökning skulle flytta in under rättegångsbalkens paraply. I samband med detta ansåg regeringen att behovet av tillgång till elektroniska uppgifter i underrättelseverksamhet skulle regleras i särskild ordning (prop. 2011/12:55). 2012 års inhämtningslag ger i underrättelseverksamhet hos Polisen, Säkerhetspolisen och Tullverket tillgång till i huvudsak samma uppgifter som tidigare givits genom rättegångsbalken och 2007 års preventivlag, med den skillnaden att uppgifter om elektroniska meddelanden med vissa undantag endast får avse historiska uppgifter och inte inhämtning i realtid.[39] Förutsättningarna för inhämtning skiljer sig däremot åt på vissa avgörande sätt. För det första finns inget krav på extern tillståndsgivning för inhämtning enligt 2012 års inhämtningslag, istället är det myndigheten själv som avgör om förutsättningarna för inhämtning är uppfyllda. För det andra saknas den typ av rekvisit som kräver att det finns konkreta omständigheter rörande en viss person som leder till en misstanke eller en anledning att anta att denne kan komma att begå brott. Istället tar rekvisiten för inhämtning enligt 2012 års inhämtningslag sin utgångspunkt i nyttan som den inhämtande åtgärden kan tänkas ha i den preventiva verksamheten. Detta är i lagstiftningen formulerat som att uppgifter enligt 2 § i lagen får hämtas in om ”omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet för vilket inte är föreskrivet lindrigare straff än fängelse i två år”. Ett ytterligare krav enligt 2 § 2 p. i lagen är att en proportionalitetsbedömning ägt rum där ”skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse”.

Vid sidan av inhämtningslagarnas förändring genomfördes datalagringsdirektivet (2006/24/EG) i svensk rätt. Därigenom föreskrevs i LEK en allmän lagring på sex månader av ett antal kategorier av metadata, vilket gjorde att mängden historisk metadata som lagras, och därigenom finns tillgänglig för inhämtning, ökade markant. Denna ökning beror på att denna typ av uppgifter tidigare omfattades av ett omvänt krav där operatörerna istället skulle se till att metadata raderades så snart uppgifterna inte behövdes för exempelvis fakturering. Till sist kan i sammanhanget också nämnas den möjlighet som infördes för Säkerhetspolisen att inrikta den strategiska signalspaning i trådbunden kommunikation som införts genom den ovan nämnda s.k. FRA-lagen (SOU 2009:66; Ds 2011:44; prop. 2011/12:179).

Separat från de traditionella hemliga tvångsmedlen diskuterades även andra metoder för inhämtning. Av Polismetodutredningen framgick att svenska polisen utan lagstöd använt s.k. IMSI-catchers,[40] en teknisk utrustning för att bl.a. spåra och kartlägga vilka personer som är närvarande vid vissa platser genom att gentemot mobila enheter framstå som en mobilmast och således locka mobiltelefoner att ansluta till IMSI-catchern och därigenom lämna ifrån sig identifierande information. Bruket av sådana metoder i brist på uttryckligt lagstöd får ses som stridande mot såväl regeringsformens som Europakonventionens krav. Utredningen föreslog följaktligen att lagstiftningen skulle förtydligas (SOU 2010:103). Metoden kan utifrån flera aspekter ses som problematisk, den kan exempelvis identifiera samtliga personer som varit

[39] Såvitt avser lokaliseringsuppgifter, dvs. uppgifter om var en viss teknisk utrustning befunnit sig eller befinner sig, samt vilka tekniska utrustningar som finns i ett visst område, är de uppgifter som tillgodogörs underrättelsemyndigheten likvärdiga och inhämtning får rörande sådana uppgifter ske i realtid.

[40] Ibland benämnda ”Stingrays”, se Pell & Soghoian (2014).

närvarande vid en viss demonstration och därigenom hypotetiskt sett ligga till grund för åsiktsregistrering. IMSI-catchers kan också, rent tekniskt, möjliggöra såväl avlyssning som övervakning av innehållet i kommunikation (Pell & Soghoian 2014). Trots detta så fördes förhållandevis få resonemang i utredningen rörande metodens risker (SOU 2010:103). Internationellt har dock samma metod varit föremål för förhållandevis stark debatt (Jfr. Pell & Soghoian 2014).

Trots att kritiska röster hördes rörande dessa utökade befogenheter för brottsbekämpande myndigheter (exempelvis Flyghed 2007; Ramberg 2007; Träskman 2007), så var de politiska och rättsliga bromsklossarna för denna utveckling få. Europadomstolen hade förvisso slagit fast att inhämtning av metadata innebär ett intrång i den personliga integriteten vilket förutsätter lagstöd, ett legitimt ändamål, och proportionalitet i förhållande till ändamålet (*Malone mot Förenade Konungariket* 1984; *Copland mot Förenade Konungariket* 2007). Likaså kräver lagring av uppgifter att samma krav ska vara uppfyllda (*Leander mot Sverige* 1987; *Amann mot Schweiz* 2000). men i de rättsfall som rört storskalig och strategisk inhämtning av sådan metadata tycktes domstolen inte se denna som oproportionerlig förutsatt att kraven på ett tydligt och förutsägbart lagstöd varit uppfyllda (*Weber & Saravia mot Tyskland* 2006; *m.fl. mot Förenade Konungariket* 2008). Samtidigt drev EU på för datalagringsdirektivets genomförande. Även om varnande röster kring riskerna med en tillåtande inställning till metadata hördes från tekniskt inriktade forskare och civilsamhället (Escudero-Pascual & Hosein 2004; Opsahl, 2013) så fick dessa röster inte särskilt stort normativt genomslag.

Mer framåtblickande myndighet, mindre återblickande domstol

Om det funnits något som sedan första början präglat svenska myndigheters tillgång till övervakning av telefon och (det som utgjorde förstadierna till) dagens internettrafik så har det varit domstolens roll. Tvångsmedlet "hemlig teleövervakning" som sedermera kom att byta namn till "hemlig övervakning av elektronisk kommunikation" utgör en del av den straffrättsliga processen som syftar till att inom ramen för en förundersökning inhämta bevis i utredningen av ett brott, vilket också illustreras av dess placering i rättegångsbalken.[41] När ett (förhållandevis allvarligt) brott begåtts,[42] och konkreta omständigheter gjort att en viss (skälig) grad av misstanke mot en viss person uppstått, samt om åtgärden varit av synnerlig vikt för utredningen, har åklagaren enligt bestämmelser i 27 kap. rättegångsbalken haft möjlighet att be rätten om tillstånd att i hemlighet övervaka denne misstänktes kommunikationer och ta reda på exempelvis vilka telefonnummer denne ringt. Det har således varit upp till domstolen att sedan bedöma huruvida åklagarens redan existerande bevisning räckte för att tillstånd skulle meddelas, samt om skälen för intrånget uppvägde de nackdelar

[41] Ett kompletterande regelverk som etablerades i 1952 års tvångsmedelslag, numera överfört till lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott, har öppnat för teleövervakning (samt avlyssning och hemlig kameraövervakning) vid utredning av vissa allvarliga brott som huvudsakligen faller under Säkerhetspolisens verksamhetsområde även om förutsättningarna i rättegångsbalken i övrigt inte är uppfyllda. Även under detta regelverk syftar dock åtgärderna till utredning av brott, och tillstånd meddelas av domstol efter ansökan av åklagare. En möjlighet till interimistiskt beslut av åklagare i brådskande fall finns dock, sådana beslut ska dock underställas domstol så snart som möjligt.

[42] I rättegångsbalkens nuvarande lydelse definierat som ett brott (inklusive försök, förberedelse eller stämpling till sådant brott) för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader, där vissa särskilda brott också kan föranleda övervakning även i övrigt (datorintrång, barnpornografibrott, narkotikabrott som inte är att anse som ringa, samt narkotikasmuggling). (RB 27 kap. 18-19 §§)

som åtgärden förde med sig för den enskilde eller annat intresse. Detta system har förvisso haft sina brister, exempelvis har det visat sig att domstolar har en tendens att förhållandevis okritiskt acceptera vissa påståenden från åklagare, särskilt i säkerhetsmål (SOU 2002:87). Samtidigt har systemet inneburit att åtminstone fyra ur rättslig synvinkel principiellt viktiga aspekter av prövningen upprätthölls.

1. Åklagaren har varit tvungen att koppla övervakningen till ett redan inträffat brott av viss svårighetsgrad.[43]

2. Åklagaren har varit tvungen att koppla övervakningen till en viss person, skäligen misstänkt för det ovan inträffade brottet.

3. En proportionalitetsbedömning har varit möjlig att göra utifrån omständigheterna i det konkreta fallet.

4. Prövningen för huruvida dels de formella förutsättningarna för övervakning i 1 och 2 ovan och dels kravet på proportionaliteten för bruket av metoden var uppfylld låg hos en självständig domstol och inte hos den myndighet som utredde brottet i fråga.[44]

Dessa aspekter av det straffprocessuella systemet var dock illa anpassade till myndigheternas underrättelseverksamhet. Eftersom syftet med denna verksamhet framför allt är att samla och analysera information i syfte att upptäcka huruvida något brott kan vara på väg att inträffa, blev kopplingen till redan inträffade brott problematisk. Ett tidigare missbruk av existerande brottsutredande tvångsmedel som skett i syfte att kartlägga grupper och individer av intresse som dock inte varit misstänkta för brott, hade dessutom fått välförtjänt kritik av Säkerhetstjänstkommissionen (SOU 2002:87). I ett flertal olika utrednings- och lagstiftningssammanhang lyftes därför behovet av särskilda inhämtningsmöjligheter i de brottsbekämpande myndigheternas underrättelseverksamhet (SOU 2002:87; SOU 2003:32; Ds 2005:21).

2007 års tvångsmedelslag innebar vid sin tillkomst ett första tydligt formellt avsteg från principen om att hemliga tvångsmedel ska grunda sig på en skälig misstanke mot en specifik person.[45] Istället var förutsättningen för inhämtning enligt lagens 1 § vid dess införande att det ”med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva brottslig verksamhet” som innefattar de brott som räknas upp i lagen. Åtgärderna ska vidare enligt 5 § vara av synnerlig vikt för att förhindra sådan brottslig verksamhet som räknas upp i lagen, dessutom ska skälen för åtgärden uppväga det intrång eller men i övrigt som åtgärden innebär för den som utsätts för det eller för något annat motstående intresse.

[43] Vissa av dessa brott kan dock i praktiken vara ofullbordade i den mån försök, förberedelse eller stämpling till brott som faller under bestämmelsen avses, men i dessa fall är sådana handlingar kriminaliserade i sig.

[44] I praktiken har två från polisen externa myndigheter varit inblandade i tillståndsgivningen då åklagaren som förundersökningsledare först kunnat ta ställning till lämpligheten i att överhuvudtaget begära tillstånd om sådan övervakning.

[45] Lagstiftaren har framhållit att denna lagstiftning inte innebar ett sådant principiellt avsteg då lagen om särskild utlänningskontroll tidigare gav möjlighet till tvångsmedel för preventiva ändamål. Denna lag var dock endast tillämplig på sådana utlänningar som var föremål för beslut om avvisning med hänvisning till rikets säkerhet, men vars avvisning inte kunde genomföras av humanitära skäl och där övervakning skedde för att säkerställa att de inte ägnade sig åt exempelvis terrorverksamhet under tiden som verkställigheten av avvisningsbeslutet fick vänta. Det rörde sig därför om ett synnerligen avgränsat antal (enstaka) individer och var inte, som 2007 års tvångsmedelslag tillämplig på befolkningen i stort, något som också framhölls när den förra lagen tillkom.

Liksom vid användande av rättegångsbalkens tvångsmedel är det dock allmän domstol som prövar frågan om tillstånd till inhämtning och vid denna prövning ska offentliga ombud medverka under samma förutsättningar som vid rättegångsbalkens tvångsmedel.

Även om 2007 års preventivlag alltså innebar ett avsteg från principen om skälig misstanke som grund för hemliga tvångsmedel, så utgör 2012 års inhämtningslag en i förhållande till metadata ett än mer långtgående steg från rättegångsbalkens principer. Detta särskilt genom formerna för beslutsgivning och rekvisiten för inhämtning. Underrättelsemyndigheten kan genom den nya lagen själv fatta beslut om inhämtning och har således själv möjlighet att bedöma om förutsättningarna för detta är uppfyllda. Denna ordning är resultatet av att lagstiftaren inte ansåg det lämpligt för domstolar att utföra denna typ av bedömningar som ansågs ha karaktären av operativa beslut. Det riskerade, menade regeringen, leda till att domstolens roll som oberoende prövningsinstans i brottmålsförfarandet ifrågasätts (prop. 2011/12:55). Det kan dock konstateras att regeringens hållning i denna fråga har kritiserats (SOU 2012:44).

Förändringarna som 2012 års inhämtningslag medförde i förhållande till reglerna som gäller vid förundersökning kan sammanfattas i fyra punkter.

1. Ett konkret brott behöver inte längre ha ägt rum eller misstänkts ha ägt rum.

2. Misstanke mot en enskild rörande ett sådant konkret brott behöver således inte ha uppnåtts.

3. Proportionalitetsbedömningen för bruk av tvångsmedel sker i förhållande till uppgifternas potentiella nytta i underrättelseverksamheten och möjligheten att i denna verksamhet upptäcka, förebygga och förhindra vissa allvarliga brott från att förverkligas.

4. Den inhämtande myndigheten själv bedömer om förutsättningar för inhämtning föreligger.

Även i polisens brottsutredande verksamhet släpptes på de tidigare kraven på skälig misstanke, även om domstolsprövningen kvarstod, genom att polisen genom rättegångsbalkens 27 kap. 20 § 2 st. fick möjlighet att ansöka om tillstånd för hemlig övervakning av elektronisk kommunikation även i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen, men endast för inhämtning av historiska uppgifter. Detta var tänkt att kunna användas för att exempelvis kartlägga vilka som befunnit sig i närheten av en brottsplats när någon särskild individs identitet inte är känd av polisen (Prop. 2011/12:55).[46]

Genom ett lagförslag (prop. 2013/14:237) som trädde ikraft 1 januari 2015 så förändrades förutsättningarna för inhämtning enligt 2007 års preventivlag. Kravet på “om det med hänsyn till omständigheterna finns särskild anledning att anta” att en person kommer att utöva viss brottslig verksamhet sänktes till att inhämtning får ske om “om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer utöva brottslig

[46] Denna bestämmelse avsåg ersätta möjligheten till s.k. basstationstömning som polisen ägnat sig åt med hänvisning till bestämmelser i LEK, då utan domstolsprövning och utifrån ett lagstöd som svårligen gick att utläsa av lagtexten.

verksamhet[…]". Den senare skrivningen avsåg enligt regeringen förtydliga att det förvisso fortfarande gällde att det skulle finnas ett visst krav på sannolikhet för att risken ska förverkligas, men att ett krav på att kunna specificera en viss avsedd konkretiserad gärning som vuxit fram i praxis, inte längre ska gälla.[47]

Den individualiserade misstankens generalisering – du är ditt mönster

Den preventiva logik som på senare år etablerats i en rad olika lagstiftningsåtgärder på övervakningsområdet är förenad med en implicit fråga. Om individen inte längre blir föremål för åtgärder baserat på misstankar mot denna rörande ett visst brott, vad ligger då till grund för åtgärderna? Till viss del är svaret förstås oförändrat; på samma sätt som tidigare kan tips vara en god anledning för brottsbekämpande myndigheter att få upp ögonen för en person. Samtidigt visar förarbetena hur en annan bild framträder, där individens mer allmänna beteendemönster och sociala omgivning kan bli avgörande för vilken nivå av åtgärder denne kan förvänta sig bli föremål för och vilka rättsliga trösklar som blir gällande för dessa åtgärder.

Genom förändringen i 2007 års preventivlag ska, som tidigare nämnts, en riskbedömning ske som blir förutsättningen för att rikta hemliga tvångsmedel mot en individ. Denna riskbedömning, påpekar regeringen, får inte bygga endast på spekulationer eller allmänna bedömningar utan ska vara grundad på faktiska omständigheter. Dessa omständigheter kan exempelvis vara uttalanden eller hotelser, men även "annat faktiskt agerande som talar för att brottslig verksamhet av visst slag – med en viss typ av skada som följd – kommer att utövas" (prop. 2013/14:237:105). Bedömningen av risken bör vidare ta sin utgångspunkt "i både avsikt och förmåga" (prop. 2013/14:237:196). Begreppen avsikt och förmåga anknyter till den typ av bedömning som redan används inom underrättelsesfären vid riskbedömningar (jfr. Säkerhetspolisen 2014), vilket innebär att underrättelselogiken får direkt genomslag i lagstiftningen. Därutöver kommer individens eventuella samröre med kriminella organisationer bli direkt avgörande för de beviskrav som gäller för övervakning av dennes kommunikation. Kravet på *"påtaglig risk",* som gäller för övervakning av kommunikation i den preventiva verksamheten, sänks nämligen ytterligare i den mån "det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet som avses i första stycket och det *kan befaras* att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet." (prop. 2013/14:237:31f). Lagförslaget är tänkt att täppa till den bevismässiga lucka som uppstår när myndigheterna har uppgifter som tyder på att en viss grupp planerar brott, men inte kan koppla dessa uppgifter till en viss individ (prop. 2013/14:237). Regeringen understryker dock att medlemskap i en organisation inte är tillräckligt för ett tvångsmedelsbeslut mot någon, detta genom kravet på att ett eventuellt främjande ska ske medvetet. Man bör dock i sammanhanget ha i åtanke svårigheterna för myndigheterna att utifrån förhållandevis otydliga uppgifter utröna huruvida en individ agerar medvetet eller omedvetet i förhållande till en verksamhet som inte behöver vara känd för myndigheterna i någon större konkretionsgrad.

[47] Regeringen uttryckte detta på följande vis i författningskommentaren (Prop. 2013/14:237:195): "Däremot krävs det inte att risken avser en konkretiserad gärning på det sätt som har utvecklats i praxis beträffande misstankerekvisitet enligt den nuvarande lagstiftningen. Tillstånd till tvångsmedelsanvändning enligt lagen bör alltså kunna meddelas i fall när flera inträffade omständigheter kan påvisas som starkt talar för en risk för att ett brott av ett visst slag kommer att inträffa men utan att det går att konkretisera hur risken kan förverkligas, t.ex. vilket närmare tillvägagångssätt som kommer att användas vid ett terrordåd eller vilket mål detta kommer att avse. Bedömningen av risken bör ta sin utgångspunkt i både avsikt och förmåga."

I praktiken har det idag byggts upp tre parallella system för övervakning av elektronisk kommunikation där förutsättningarna för inhämtning skiljer sig åt på en högst grundläggande nivå. *För det första* återstår det ordinarie systemet i rättegångsbalken, där inhämtningen som nämnts ovan syftar till att utreda inträffade brott. *För det andra* finns ett system för underrättelseverksamhet, där förutsättningarna skiljer sig åt så till vida att de tar sikte på potentiella framtida brott, och där myndigheterna i fråga om historiska uppgifter själv kan besluta om inhämtning av metadata. *För det tredje* finns den strategiska signalspaning som bedrivs av Försvarets Radioanstalt, där all kommunikation passerar genom ett filter och där viss kommunikation, baserat på metadata och innehåll, separeras för ytterligare granskning. I detta sista system är mönstersökning i all metadata i relevanta signalbärare som passerar vissa knutpunkter i nätverket en förutsättning inte bara för vidare granskning, utan även för att separera sådan kommunikation som *inte* ska genomsökas. De tre systemen innebär samtidigt en gradvis övergång från den konkreta misstankens logik som syftar till att utreda brott, lagföra brottslingar och genom straffrättens allmänpreventiva och avskräckande verkan därigenom förebygga uppkomsten av nya brott.[48]

Underrättelseverksamhetens förutsättningar antyder att lagstiftaren i vissa avseenden övergett denna preventiva effekt till förmån för en form av *initialpreventiv* risklogik där brottet helt enkelt, om möjligt, inte tillåts äga rum. Misstanken byts under denna logik ut mot risk, och individen går från att betraktas som en potentiellt (presumerat) oskyldig part, till att ses som en utifrån vissa indicier, kapaciteter, eller beteendemönster potentiell riskfaktor där åtgärder vidtas tills dess att den enskilde visats vara ofarlig (jfr. Cameron 2007; Asp & Cameron 2009; Zedner, 2007). Inhämtningslogiken är i vissa avseenden frikopplad även från denna individuella riskbedömning och utgår istället från nyttan som uppgifterna har för verksamheten; att bedöma huruvida individen utgör en risk och i så fall förhindra denna risk för att realiseras. Inhämtningen är dock fortfarande i huvudsak riktad och avgränsad på förhand, även om vissa åtgärder även inom ramen för detta regelverk kan leda till inhämtning av en större mängd data.[49]

Den strategiska signalspaning som bedrivs av FRA i Sverige och av myndigheter som NSA i Förenta staterna och GCHQ i Storbritannien, generaliserar denna logik så till vida att enskilda individer inte längre nödvändigtvis står i fokus, utan fenomen, och där såväl risk som misstanke är frånkopplade bedömningen. Inhämtningen utgår istället från kommunikationens potentiella relevans för att kartlägga intressanta fenomen eller hot. Enligt denna logik är all kommunikation som passerar övervakningspunkterna i nätverket (exempelvis fiberoptiska undervattenskablar) *potentiellt* intressant och i praktiken (enligt tidigare logik) "misstänkt", varvid sorteringen i det närmaste sker baklänges. Konstaterat irrelevant kommunikation sållas stegvis bort genom tekniska metoder och individuell granskning för att så småningom nå fram till den förhoppningsvis relevanta nålen i höstacken.[50] I detta normativa system är individen

[48] Det är utifrån detta perspektiv inte helt rätt att tala om traditionellt kontra preventivt regelverk då straffrättens funktion till en inte obetydlig grad är just preventiv, om än indirekt och generellt (jfr. Asp 2007).

[49] I sammanhanget kan nämnas att regeringens redovisning till riksdagen av antal beslut om inhämtning ändrades 2013, det är nu utifrån denna svårt att utläsa hur många individer eller teleadresser som blivit föremål för inhämtning. Antalet beslut inom ramen för förundersökning var år 2012 redovisat som 4 095 st., antalet avslag var 48. Inom ramen för underrättelseverksamheten var antalet beslut 369. Några avslag i den senare verksamheten blir det inte tal om då myndigheten själv beslutar om inhämtning (Rskr. 2013/14:60).

[50] Signalspaning har förvisso goda möjligheter att utföra även riktad inhämtning mot en viss individ eller IP-nummer. Den svenska lagstiftningen tillåter dock endast sökord hänförliga till en viss person i undantagsfall,

reducerad till tekniska parametrar, mönster och söktermer, vilket i viss mån skymmer det faktum att miljontals individer blir föremål för granskande åtgärder – om än till stor del automatiska sådana – i syfte att bedöma om individernas kommunikationsmönster föranleder en vidare underrättelseåtgärd eller kan bidra till kartläggningen av för rikets säkerhet intressanta fenomen.

Till sist bör här nämnas fenomenet datalagring, som möjliggör en slags retroaktivitet i de traditionella och preventiva tvångsmedlen. Här sker dock inte något initialt urval. Istället blir all metadata rörande kommunikationen lagrad hos operatören för det fall att någon individ skulle visa sig vara intressant för brottsbekämpande myndigheter under kommande sex månader. Lagringen utgör således en omvänd skyldighet i förhållande till vad som gällde tidigare då operatörerna var skyldiga att radera information så snart den inte var relevant för exempelvis fakturering.[51] Den faktiska information som lämnas ut till brottsbekämpande myndigheter kan variera och utlämning kan ske utifrån såväl preventiva som brottsutredande ändamål. Lagringen sker endast i syfte att möjliggöra en sådan retrospektiv granskning av kommunikation. Just denna datalagring och den EU-lagstiftning som initierade den, kommer dock visa sig vara av särskilt intresse i den rättsliga diskussion rörande metadata som vi snart ska komma till.

En rättslig reaktion

Nya förutsättningar för den rättsliga analysen

Det kan tyckas som om det skulle vara svårt att dra paralleller mellan den massiva metadataanalys som sker i signalspaning, den inhämtning av metadata som sker i underrättelseverksamhet, lagring av metadata, och den mer inriktade, operativa övervakning som brottsbekämpande myndigheter ägnar sig åt. Samtidigt går det att konstatera att skillnaden inte går att återfinna i känsligheten i de uppgifter som behandlas, utan i formerna för inhämtningen. Uppgifternas känslighet var dock, vilket nämnts ovan, något som inte varit föremål för någon mer ingående analys. I detta avseende är det därför svårt att underskatta betydelsen av de avslöjanden som kom från Edward Snowden. Det blev plötsligt väldigt svårt att ignorera hur metadata kunde användas, hur stora mängder uppgifter som kunde bearbetas, och hur mycket denna information kunde avslöja om individen. Även om den massiva inhämtning som NSA ägnat sig åt, och legaliteten hos denna verksamhet kom att hamna i fokus, så är en av de mer påtagliga effekterna av avslöjandena att ett akademiskt hypotiserande rörande hur metadata kan användas kunde ersättas av konkreta exempel.[52] Sådana konkreta exempel hade tidigare existerat, bland annat i marknadsföringsmaterialet till olika typer av övervakningsmjukvaror (IBM 2012), men deras tillämpning i konkreta, normativa, termer var fortfarande svår att peka på. Domstolar som tidigare varit ovilliga att spekulera kring riskerna och integritetseffekterna fick nu anledning, och tillfälle, att ompröva

---

trots att sådan inriktning i praktiken kan vara ofrånkomlig för att kartlägga vissa fenomen och trots att så gott som alla tekniska parametrar i praktiken kan hänföras till någon, se SOU 2011:13.

[51] Detta krav gäller fortfarande, men inte för sådan information som omfattas av lagringskrav.

[52] Se *Klayman v. Obama 2013*, där en amerikansk domstol öppnade för en prövning av den amerikanska signalspaningslagstiftningens förenlighet med konstitutionen utifrån att de sökande kunde visa på talerätt som kunder hos Verizon, en av de teleoperatörer som genom Edward Snowdens dokument visats överlämna all metadata rörande deras kunders samtal till amerikanska myndigheter.

sina tidigare ställningstaganden baserat på att sådana effekter kunde illustreras konkret - och dessutom blev föremål för en allmän debatt som gjorde en förhållande teknisk diskussion föremål för en mer allsidig belysning.

Det finns också tecken som tyder på att en större medvetenhet om riskerna med metadatainhämtning fått genomslag i rätten. Ett av de mer påtagliga sådana tecken skulle komma från EU-domstolen under 2014.

Digital Rights Ireland – ett rättsligt trendbrott?

Som nämnts ovan har EU varit drivande i en utveckling som innebär att uppgifter om telekommunikation ska lagras för att kunna användas i brottsbekämpande verksamhet. Det så kallade datalagringsdirektivet har också genomförts i svensk rätt genom en lagstadgad skyldighet för tele- och internetoperatörer att lagra metadata som de behandlar vid förmedlandet av kommunikationen, i sex månader från kommunikationstillfället. Motsvarande genomförandelagstiftning återfinns i de flesta av EU:s medlemsländer. Implementeringen i två länder, Irland och Österrike, ledde dock fram till en prövning i EU-domstolens stora kammare rörande datalagringsdirektivets förenlighet med rätten till personlig integritet och rätten till skydd för personlig data i EU:s rättighetsstadga (joined cases C-293/12 och C-594/12 Digital Rights Ireland and Seitlinger and Others, hädanefter *Digital Rights Ireland*). Datalagringsdirektivet kom som ett resultat av denna prövning att ogiltigförklaras av EU-domstolen då det utgjorde ett oproportionerligt intrång i den personliga integriteten. Vid sidan av att domstolen ansåg att direktivet inte i tillräcklig utsträckning förenat lagringsskyldigheten med krav på tillräckliga rättssäkerhetsmekanismer, så går det i domen att även notera ett antal tecken på ett trendbrott rörande bedömningen av metadata – en bedömning som kom att vara avgörande för utfallet.

Redan i upptakten till domen hade generaladvokaten Cruz Villalón i sitt yttrande till domstolen pekat på att lagringen av data om enskilda människors kommunikationer under en längre tid skapar en "vag känsla av övervakning" hos befolkningen, en känsla som är problematisk i sig (*Opinion of Advocate General Cruz Villalón* 2013:52). Utöver detta, menade Villalón, var uppgifterna dessutom av en särskild art (Villalón 2013:74):

> *"The data in question, it must be emphasized once again, are not personal data in the traditional sense of the term, relating to specific information concerning the identity of individuals, but 'special' personal data, the use of which may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity."*

Det är redan i detta konstaterande påtagligt att generaladvokatens bedömning av dessa data skiljer sig från den förekommit i svenska förarbeten på senare tid. På mer än ett sätt gick dock EU-domstolen längre i sin bedömning än generaladvokaten föreslagit. För det första genom att domstolen ogiltigförklarade datalagringsdirektivet (*Digital Rights Ireland* 2014) där generaladvokaten endast förordade ett uppskjutet ogiltigförklarande med bibehållen giltighet i väntan på justering av vissa faktorer (*Opinion of Advocate General Cruz Villalón* 2013). För det andra genom domstolens bedömning av den aktuella typen av uppgifter. Domstolen gör nämligen en koppling som ofta förbisetts i dessa sammanhang, mellan intrånget i den personliga integriteten och effekten på andra, anknutna rättigheter.

> *"[Metadata] taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life,*

> *permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.*
>
> *In such circumstances, even though […]the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter. (Digital Rights Ireland 2014:27f)"*

Denna koppling mellan skyddet för den personliga integriteten och effekter på yttrandefrihet och andra politiska friheter är inte ett nytt påfund. Den har tidigare gjorts i tongivande litteratur rörande den personliga integriteten från andra halvan av 1900-talet när bruket av datorer för register och statistik lade startskottet för den integritetsdebatt som pågått sedan dess (Westin 1968; Gavison 1980). Däremot är det en koppling som tycks ha glömts bort i de svenska lagstiftningsåtgärder som skett på senare tid (Naarttijärvi 2013). Det är därför intressant att notera att EU-domstolen lyfter fram inte bara hur metadata kan ligga till grund för en mycket detaljerad kartläggning av individen, utan också hur tillgången på denna metadata kan inskränka på fler rättigheter än den personliga integriteten.

EU domstolen lade även vikt vid att direktivet inte lade fast något krav på att utlämnande av lagrad data skulle underställas beslut av domstol eller en fristående myndighet (*Digital Rights Ireland* 2014), vilket i sig gjorde att det saknades en instans vars beslut kunde minimera tillgången till data och dess användning till vad som är strikt nödvändigt för att nå de ändamål som föranlett begäran om uppgifter. Det saknades också enligt direktivet skyldighet att införa sådana gränser på tillgången till data. Detta är en intressant del av domen då frånvaron av (krav rörande) en sådan instans får ses som ett av de huvudskäl som låg till grund för att direktivet ansågs oproportionerligt. I sammanhanget kan påminnas om den ovan nämnda utvecklingen i svensk rätt som gett brottsbekämpande myndigheter större frihet att inom ramen för underrättelseverksamheten själv besluta om förutsättningar för inhämtning föreligger. Frågan är således om en sådan ordning kan anses stå i överensstämmelse med de rättssäkerhetskrav som EU domstolen tycks se som grundläggande (jfr. Ds 2014:23). Även om den svenska ordningen föreskriver vissa krav som ska vara uppfyllda för inhämtning, så tycks EU domstolen förutsätta att en prövning av huruvida dessa kriterier ska vara uppfyllda ska ske av en domstol eller åtminstone av en fristående myndighet.

Utveckling på FN-nivå

Uttalandena rörande metadata i Digital Rights Ireland speglar en växande diskurs inom det internationella systemet för mänskliga rättigheter. Liknande slutsatser hade redan året innan domen i EU-domstolen dragits av den särskilda rapportören för främjande och skydd av opinions- och yttrandefrihet i en rapport till Förenta Nationernas råd för mänskliga rättigheter.

> *"The communications data collected by third party service providers, including large internet companies, can be used by the State to compose an extensive profile of concerned individuals. When accessed and analyzed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone." (UNGA 2013:42)*

I oktober 2014 kom en ytterligare rapport från Förenta Nationernas särskilda rapportör för mänskliga rättigheter i kampen mot terrorismen, Ben Emmerson, att fortsätta analysen enligt samma linjer.

> *"By combining and aggregating information derived from communications data, it is possible to identify an individual's location, associations and activities […}. In the absence of special safeguards, there is virtually no secret dimension of a person's private life that would withstand close metadata analysis." (UNGA 2014a:53)*

Rapporternas rättsliga betydelse är i första hand sekundär i den bemärkelsen att resonemang som förekommer där kan lyftas upp och beaktas av politiska organ liksom rättsliga organ inom FN, Europarådet och EU. Därutöver kan dock denna typ av rapporter underbygga den rättsliga argumentationen hos de intresseorganisationer och MR-grupper som söker pröva nationell lagstiftning i internationella domstolar. Rapporternas effekt kan således bli mer långtgående än deras vikt som rättskälla antyder genom att de utgör en första tydlig signal om hur nya typer av övervakning av elektronisk kommunikation i det globala nätverkssamhället kan komma att betraktas inom ramen för de mänskliga rättigheterna.

Samtidigt visar inte utvecklingen på FN-nivån på en i alla avseenden rak linje. I ett förslag till FN-resolution "The Right to Privacy in the Digital Age" som lagts fram av Tyskland och Brasilien i oktober 2014 gjordes flera referenser till känsligheten hos metadata (UNGA 2014b). Flera av dessa referenser kom dock att beskrivas i svagare termer i den version av resolutionen som sedermera kom att godkännas av FN:s kommitté för mänskliga rättigheter i november samma år (UNGA 2014c). Bland annat beskrevs metadatainhämtning som "highly intrusive" i det första utkastet, en skrivning som saknas i det senare. Förändringarna har i media beskrivits som ett sätt att blidka USA och dess brittiska, kanadensiska, australiensiska och nya-zeeländska allierade i den s.k. "Five Eyes" gruppen som tillsammans driver ett gemensamt signalspaningsnätverk, och därigenom uppnå konsensus (Quinn 2014; Yoon 2014). Därtill ställde första utkastet av resolutionen krav på att åtgärder som innebar övervakning av kommunikationer förutom att ha klart lagstöd måste vara nödvändiga, proportionerliga och inte inskränka privatlivets kärna (UNGA 2014b). I det senare utkastet anges istället att sådana åtgärder inte får vara godtyckliga och olagliga, samt ska ha i åtanke vad som är "rimligt" i förhållande till ändamålet (UNGA 2014c), vilket i sammanhanget får betraktas som ett betydligt lägre ställt krav. Samtidigt innebär resolutionen i dess föreslagna form fortfarande ett normativt stöd för att aggregerad metadata kan innebära en detaljerad insyn i individens privata förehavanden, liksom ett tydliggörande av kopplingen mellan rätten till personlig integritet och yttrandefrihet. Resolutionen ger dessutom uttryck för att olaglig eller godtycklig inhämtning av kommunikationer, särskilt på massiv skala, kan stå i motsägelse till det demokratiska samhällets grunder (UNGA 2014c).

Kommande fall

Var utvecklingen är på väg kommer potentiellt att klarna inom de närmaste åren. Europadomstolen i Strasbourg har, i vad som är ett mycket ovanligt steg, valt att prioritera en ansökan från organisationen Big Brother Watch m.fl. som hos domstolen lämnat in klagomål mot den brittiska delen av NSA:s övervakningsnät och de övervakningsprogram så som PRISM och TEMPORA som avslöjats av Edward Snowden (*Big Brother Watch m.fl. mot Förenade konungariket* 2014). Det är sannolikt för tidigt att spekulera i om domstolen kommer att ge sig in i proportionalitetsfrågor och mer principiella bedömningar av åtgärderna i stort, eller om prövningen stannar vid formella legalitetsaspekter, men prövningen öppnar för att domstolen

kompletterar tidigare avgöranden rörande signalspaning i *Weber & Saravia* och *Liberty* och möjligen gör att domstolen utifrån mer konkreta exempel på den faktiska verksamheten törs gå längre i sina resonemang än tidigare. Det kan i sammanhanget nämnas att även en prövning av den svenska signalspaningslagstiftningen återfinns bland Europadomstolens väntande fall i *Centrum för rättvisa mot Sverige*.

Hos EU-domstolen och EU-kommissionen väntar dessutom nya prövningar av datalagringsdirektivets nationella implementeringar. Dessa är resultatet av att vissa länder, däribland Sverige, valt att bibehålla sina nationella bestämmelser om datalagring trots EU-domstolens dom rörande direktivet, vilket lett till rättsliga utmaningar från bl.a. internetoperatörer (Bahnhof 2014). Dessa fortsatta prövningar lär tydliggöra hur långtgående konsekvenser EU-domstolens dom i *Digital Rights Ireland* kommer att få.

Slutsatser och analys

En principiell kollision

Genom den förhållandevis tillåtande inställningen till metadatainhämtning som vuxit fram under 2000-talet och nya preventiva strävanden i lagstiftningen har principiella spänningar uppstått mellan de olika system för inhämtning som uppkommit. Ett antal av de primära rättssäkerhetsmekanismer som gäller vid traditionell brottsutredande tvångsmedelsanvändning har ansetts svårtillämpade i den preventiva verksamheten, här kan särskilt nämnas kravet på konkret misstanke. Samtidigt har också lagstiftaren medvetet valt att inte placera tillståndsgivningen för underrättelseverksamhetens inhämtning av historisk metadata enligt 2012 års inhämtningslag hos domstol, samt stegvis sänkt kraven för tillstånd till inhämtning enligt 2007 års preventivlag. Parallellt med detta har införandet av ett krav på datalagring inneburit att mängden historisk metadata som faktiskt kan tänkas innefattas av inhämtningsbeslut ökar, då dessa uppgifter tidigare omfattades av gallringskrav. Dessa val återspeglar en medveten strävan från lagstiftare och myndigheter att säkerställa tillgång till mer data och under mindre restriktiva former än vad som tidigare ansetts acceptabelt. Det är möjligt att gränserna för när och under vilka former myndigheterna ska få tillgång till metadata har varit i behov av att revideras utifrån nya hot och utifrån hur elektroniska kommunikationsmedel har underlättat för antagonistiska aktörer att planera och samordna aktioner. Avvägningsekvationen på säkerhetssidan har således förändrats, vilket lagstiftare och myndigheter inte varit sena att påpeka. Samtidigt har dock ekvationen även på den andra sidan förändrats genom den allt mer detaljerade bild av enskilda som går att utläsa genom tillgång till metadata och den enorma betydelse som elektronisk kommunikation har för opinionsbildning och andra opinionsfriheter, en förändring som inte lagstiftaren i alla avseenden tagit hänsyn till. Den senare tidens rättsliga utveckling kommer därför sannolikt att förändra förutsättningarna för lagstiftarens handlingsfrihet på området.

Betydelsen ur proportionalitetssynvinkel

Samtliga rättighetskomplex som aktualiseras i förhållande till rättighetsinskränkningar av den typ som diskuteras ovan ställer krav på proportionalitet hos åtgärderna. Detta krav återfinns i 2 kap. 21 § RF, i Europakonventionen för mänskliga rättigheters artikel 8, liksom i EU:s rättighetsstadga artikel 52(1). Detta proportionalitetskrav innebär en inskränkning av lagstiftarens frihet att inskränka på rättigheter även i det fall sådana åtgärder har stöd i lag och

faller in under något av de legitima ändamålen för inskränkningar - så som nationell säkerhet. Lagstiftaren måste kunna visa på att åtgärden inte kan uppnås på något sätt som innebär en lindrigare rättighetsinskränkning, samt att åtgärdens nytta i förhållande till dess ändamål står i proportion till de effekter för den skyddade rättigheten, eller andra anknutna rättigheter, som åtgärden innebär (Alexy 2002). Denna proportionalitet som riktar sig mot lagstiftaren är en annan, och ska inte sammanblandas med, det proportionalitetskrav som riktar sig mot de myndigheter som har att tillämpa rättighetsinskränkande lagar – exempelvis krav på proportionalitet i det enskilda fall när ett elektroniskt tvångsmedel ska tillämpas. Däremot kan *möjligheten* till en individuell proportionalitetsbedömning utgöra en faktor i en mer *generell* proportionalitetsbedömning på lagstiftningsnivå (UNGA 2014a).

Det är av flera anledningar betydelsefullt ur proportionalitetssynpunkt att metadata nu diskuteras utifrån en större förståelse för informationstypens faktiska integritetsrisker, samt inhämtningens potentiella effekter på anknutna politiska rättigheter. Den proportionalitetsanalys som tidigare ägt rum rörande metadata i svenska lagstiftningssammanhang har utgått från en huvudsakligen föråldrad bild av metadata, där avvägningsresonemang hämtats från tidigare lagstiftningsåtgärder utan att ta hänsyn till den förändring som skett i fråga om uppgifternas innehåll och potential. Detta trots att uppgifternas *nytta* i den brottsbekämpande verksamheten har avvägts utifrån dagens förhållanden. Trots att inhämtningens nytta och integritetseffekter i stor utsträckning är sammanlänkade har detta förhållande inte nödvändigtvis beaktats i förarbetena. En normativ signal från en av de högsta domstolarna i Europa öppnar upp för en mer allsidig bedömning i framtida lagstiftningsåtgärder. Det bör dock i sammanhanget nämnas att detta förhållande inte nödvändigtvis innebär att lagstiftningsåtgärder som innebär en förhållandevis tillåtande inhämtning eller lagring av metadata omöjliggörs, det illustreras av den utredning som utredde den svenska datalagringen utifrån EU-domstolens dom (Ds 2014:23). Denna utredning konstaterade att vissa av de centrala brister som EU-domstolen påpekat i direktivet inte kunde göras gällande mot den svenska lagstiftningen varför denna i huvudsak ansågs vara acceptabel utifrån EU-rätten.[53] Oavsett om slutsatserna i denna utvärdering håller för den granskning av den svenska lagstiftningen som sannolikt kommer att ske på EU-nivå, så har EU-domstolens dom redan inneburit att en mer ingående diskussion kring, och analys av, den svenska lagstiftningen påbörjats.

En annan effekt ur proportionalitetshänseende är att en vanligt förekommande *sleight of hand* i lagstiftningssammanhang försvåras; övergången från en diskussion om proportionalitet i ett enskilt fall till proportionaliteten i fråga om en åtgärd som påverkar ett mycket stort antal människor. Det blir utifrån resonemangen i EU-domstolens dom, liksom utifrån FN-rapporterna som nämnts ovan, betydligt svårare att låna avvägningsresonemang från äldre lagstiftning som rör riktad inhämtning, för användning i fråga om lagstiftning som rör preventiv eller massiv inhämtning och lagring. Proportionaliteten i båda de senare fallen skiljer sig nämligen åt i stor utsträckning. I fråga om individualiserad misstanke kan en proportionalitetsbedömning utgå från konkretiserade omständigheter i det enskilda fallet. Nytta i utredningen av brottet kan vägas mot intrånget i individens privatliv utifrån brottets art, utredningens läge och uppgifternas potentiella betydelse i denna, möjligheter till andra mindre inskränkande åtgärder etc. I frågor rörande preventiv avlyssning blir denna proportionalitetsbedömning i större utsträckning hypotetisk då det eventuella brottet ännu inte ägt rum. I frågor om massiv metadatainhämtning, eller lagring av sådan data, blir dock proportionalitetsbedömningen av en annan karaktär. Här måste nyttan hos åtgärden vägas mot

[53] Författarna ansåg exempelvis att det fanns skäl att noga överväga om det den externa kontrollen över inhämtning av abonnemangsuppgifter och inhämtning av uppgifter i underrättelseskedet bör stärkas.

det totala integritetsintrånget hos *samtliga* som omfattas av lagstiftningen som sådan (UNGA 2014a). Det går således inte att diskutera integritetsintrånget utifrån de som faktiskt blir föremål för åtgärder, då även andra blir föremål för den integritetseffekt som lagen som sådan innebär och således blir föremål för en rättighetsinskränkning. Lagstiftningen innebär dessutom en potential för övervakning som kan påverka individens faktiska utnyttjande av elektronisk kommunikation och därigenom genomslaget av såväl den personliga integriteten som yttrande- och informationsfrihet. Det blir i frågor rörande generaliserad inhämtning eller lagring också svårare att framgångsrikt hävda att det inte finns andra, mindre inskränkande åtgärder som skulle uppnå samma eller nästan samma ändamål till en mindre rättighetsinskränkande effekt. Även i frågor rörande denna typ av lagstiftning så kan det potentiellt gå att motivera sådan lagstiftning, men det kräver proportionalitetsresonemang som inte längre döljer den faktiska och långtgående rättighetsinskränkning som i praktiken äger rum.

Ett kommande vägskäl

Svenska brottsbekämpande myndigheter fick den 1 januari 2015 än mer tillåtande regler rörande möjligheterna till övervakning av elektronisk kommunikation. Den svenska lagstiftaren tycks också vilja behålla våra nationella datalagringsregler, trots att vissa oklarheter rörande förenligheten med grundläggande rättigheter kvarstår. Signalen från Europeiska ledare kort efter attacken mot *Charlie Hebdos* redaktion i Frankrike har varit ytterligare krav på ökad övervakning av internet (BBC 2015; Latvian presidency 2015; Nielsen 2015). Det finns således tecken på en ökande klyfta mellan nationella och Europeiska lagstiftares ambitioner i fråga om övervakning av kommunikationer å ena sidan, och å andra sidan de rättsliga principer och rättigheter som konstitutionella domstolar har som uppgift att upprätthålla. Det är sannolikt för tidigt att kunna slå fast huruvida domen i *Digital Rights Ireland* är ett första steg mot ett mer övergripande och långsiktigt skifte i den faktiska omfattningen av och förutsättningarna för statlig övervakning av elektronisk kommunikation i Europa. Svaret lär visa sig i takt med att de väntande fall som på olika sätt berör dessa frågor har avgjorts. Samtidigt finns det redan nu ett tydligt rättsligt ställningstagande rörande känsligheten hos kommunikationsmetadata. Det är i sig ett ställningstagande som kan, och bör, få genomslag i nationella domstolar och myndigheters bedömning av lagstiftning rörande samma typ av uppgifter. Ett trivialiserande av känsligheten hos metadata riskerar nu, i större utsträckning än tidigare, att öppna upp lagstiftningen för rättsligt mothugg från de högsta rättsliga instanserna i Europa.

Referenser

Alexy, Robert (2002) *A theory of constitutional rights*, Oxford: Oxford university press.

Asp, Petter (2007) *Går det att se en internationell trend? — om preventionismen i den moderna straffrätten*, Svensk juristtidning, nr. 1, 69.

Asp, Petter & Iain Cameron (2009) *Terrorism and Legal Security – A Swedish and European Perspective*, i Dahlberg (red.), *Uppsala–Minnesota Colloquium: Law, Culture and Values*, De Lege årsbok 2009, Uppsala: Iustus förlag.

Bahnhof (2014) *Vi anmäler Sveriges datalagring till EU-kommissionen*, pressmeddelande 12 september, tillgänglig på https://www.bahnhof.se/press/press-releases/2014/09/12/vi-anmaler-sveriges-datalagring-till-eu-kommissionen.

Cameron, Iain (2007) *Brottsbekämpning, rättssäkerhet och integritet – vissa internationella trender*, Svensk juristtidning, nr. 1, 83.

Connolly, Kate (2007) *Protests over terror arrest of German academic*, The Guardian 21 augusti, tillgänglig på http://www.theguardian.com/world/2007/aug/21/highereducation.internationaleducationnews.

Deutsche Welle (2007), *Court Overturns Controversial Arrest of Sociology Professor*, 25 oktober, tillgänglig på http://www.dw.de/court-overturns-controversial-arrest-of-sociology-professor/a-2846685.

Direktivet 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

Ds 2005:21, *Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet*, Justitiedepartementet.

Ds 2005:30, *En anpassad försvarsunderrättelseverksamhet*, Försvarsdepartementet.

Ds 2011:44, *Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet*, Justitiedepartementet.

Ds 2014:23, *Datalagring, EU-rätten och svensk rätt*, Justitiedepartementet.

Escudero-Pacual, Alberto & Ian Hosein (2004) *Questioning Lawful Access to Traffic Data*, Communications of the ACM, vol. 47, nr. 3, mars, 77-82.

Flyghed, Janne (2007) *Kriminalitetskontroll — baserad på tro eller vetande?*, Svensk juristtidning, nr. 1, 59.

Gavison, Ruth (1980) *Privacy and the limits of law*, The Yale Law Journal, vol. 89, nr. 3, 421-471.

Greenwald, Glenn (2013) *NSA collecting phone records of millions of Verizon customers daily*, The Guardian 6 juni.

Greenwald, Glenn & Ewen MacAskill (2013) *Boundless Informant: the NSA's secret tool to track global surveillance data*, theguardian.com, 11 juni.

IBM (2012) *i2 Pattern Tracer Datasheet*, November, tillgänglig på http://www-03.ibm.com/software/products/en/pattern-tracer/.

Latvian Presidency of the Council of the European Union (2015), *Joint statement of the ministers for the interior and/or justice of the European Union*, 11 januari, tillgänglig på https://eu2015.lv/images/news/2015_01_11_Joint_statement_of_ministers_for_interrior.pdf.

MacAskill, Ewen; Julian Borger; Nick Hopkins; Nick Davies & James Ball (2013) *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 juni.

Naarttijärvi, Markus (2013) *För din och andras säkerhet - Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, Uppsala: Iustus förlag.

Nielsen, Nikola J. (2015) *EU wants internet firms to hand over encryption keys*, EU observer, 22 januari, tillgänglig på https://euobserver.com/justice/127329.

Opsahl, Kurt (2013) *Why Metadata Matters*, EFF Deeplinks, 7 juni, tillgänglig på https://www.eff.org/deeplinks/2013/06/why-metadata-matters.

Pell, Stephanie K. & Soghoian, Christopher (2014) *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy* (15 maj). Harvard Journal of Law and Technology (kommande), tillgänglig på http://ssrn.com/abstract=2437678.

Proposition 1988/89:124, *Om vissa tvångsmedelsfrågor.*

Proposition 2006/07:63, *En anpassad försvarsunderrättelseverksamhet.*

Proposition 2010/11:46, *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG* .

Proposition 2011/12:55, *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.*

Proposition 2013/14:237, *Hemliga tvångsmedel mot allvarliga brott.*

Quinn, Ben (2014) *United Nations human rights committee resolves to protect privacy*, The Guardian, 26 november, tillgänglig på http://www.theguardian.com/law/2014/nov/26/united-nations-human-rights-privacy-security.

Ramberg, Anne (2007) *Tvångsmedel, rättssäkerhet och integritet – går det att förena?*, Svensk juristtidning, nr. 1, 154.

Sennett, Richard & Saskia Sassen (2007) The war on shapeless terror, theguardian.com, 20 augusti, tillgänglig på http://www.theguardian.com/commentisfree/2007/aug/20/thewaronshapelessterror.

Skr. 2013/14:60, *Redovisning av användningen av vissa hemliga tvångsmedel under år 2012.*

SOU 1975:95, *Telefonavlyssning*, betänkande av utredningen om telefonavlyssning.

SOU 2002:87, *Rikets säkerhet och den personliga integriteten*, Betänkande av Säkerhetstjänstkommissionen.

SOU 2003:32, *Vår beredskap efter den 11 september*, Betänkande av 11 september-utredningen.

SOU 2009:66, *Signalspaning för polisiära behov*, Betänkande av utredningen om underrättelseinhämtning för vissa polisära behov.

SOU 2010:103, *Särskilda spaningsmetoder*, Slutbetänkande av polismetodutredningen.

SOU 2011:13, *Uppföljning av signalspaningslagen*, Betänkande av Signalspaningskommittén.

SOU 2012:44, *Hemliga tvångsmedel mot allvarliga brott*, betänkande av utredningen om vissa hemliga tvångsmedel.

Säkerhetspolisen (2014) Årsbok 2013, Säkerhetspolisen, Stockholm.

Träskman, Per Ole (2007) *Brottsligheten och dess bekämpande — en reflektion om verkliga hot och hotbilder*, Svensk juristtidning, nr. 1, 101.

United Nations General Assembly (2013), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue,* A/HCR/23/40, 17 april.

United Nations General Assembly (2014a) *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397, 23 september.

United Nations General Assembly (third committee) (2014b)*The right to privacy in the digital age*, A/C.3/69/L.26, 31 oktober.

United Nations General Assembly (third committee) (2014c) The right to privacy in the digital age, A/C.3/69/L.26/Rev.1, 19 november.

Westin, Alan F. (1967) *Privacy and Freedom*, Atheneum.

Yoon, Sangwon (2014) *UN Expands Anti-Spying Resolution to Include Metadata Collection*, Bloomberg, 25 november, tillgänglig på http://www.bloomberg.com/news/2014-11-25/un-expands-anti-spying-resolution-to-include-metadata-collection.html.

Zedner, Lucia (2007) *Pre-crime and post criminology?*, Theoretical Criminology, nr. 11, 261-281.

Rättsfall

Al-Nashif mot Bulgarien, (50963/99), Europadomstolens dom meddelad den 20 juni 2002.

Amann mot Schweiz, (27798/95) Europadomstolens dom meddelad den 16 februari 2000.

Big Brother Watch m.fl. mot Förenade Konungariket, (58170/13), Europadomstolens kommunikation den 9 januari 2014.

Centrum för rättvisa mot Sverige, (35252/08), Europadomstolens kommunikation den 1 november 2011 och 14 oktober 2014.

Copland mot Förenade Konungariket, (62617/00), Europadomstolens dom meddelad den 3 april 2007.

Digital Rights Ireland and Seitlinger and others, (joined cases C-293/12, C-594/12), Judgement of the Court of Justice of the European Union (Grand Chamber) 8 april 2014.

Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013).

Leander mot Sverige, (9248/81), Europadomstolens dom meddelad den 26 mars 1987.

Liberty m.fl. mot Förenade Konungariket, (582443/00), Europadomstolens dom meddelad den 1 juli 2008.

Malone mot Förenade Konungariket, (8691/79), Europadomstolens dom meddelad den 2 augusti 1984.

Opinion of Advocate General Cruz Villalón, Digital Rights Ireland and Seitlinger and others (joined cases C-293/12, C-594/12), 12 december 2013.

Weber och Saravia mot Tyskland, (54934/00), Europadomstolens beslut meddelat den 29 juni 2006.

Nya aktörer och ny teknik i kontrollandskapet[54]

Janne Flyghed

> *The ease and cheapness of connecting everything to everything means there is no technical reason why anything digital in your life cannot be connected to anything else, with or without your knowledge. (Keenan 2014:76)*

Säkerhets- och kontrollindustrin växer och är mer lönsam än någonsin. De tekniska möjligheterna för att kontrollera och övervaka medborgare har aldrig varit större. Dessutom har nya aktörer etablerat sig på kontrollmarknaden. Värnandet om vår trygghetskänsla tycks omättlig. Bland beslutsfattare och praktiker finns därtill en utbredd uppfattning att lösningen för att motverka samhällsskadliga fenomen och eliminera otrygghet till stor del är en fråga om teknik. För detta kan kontroll- och säkerhetsindustrin erbjuda en mängd sofistikerade lösningar. Dock är intresset för åtgärdernas konsekvenser för den personliga integriteten inte alltid lika stort. Diskussioner om balansen mellan kontrollåtgärdernas effektivitet och grundlagsstadgade fri- och rättigheter lyser ofta med sin frånvaro.

I detta kapitel ges inledningsvis några exempel på nya kontrollteknologiska lösningar. Efter en kort beskrivning av de vanligast förekommande motiven till inrättandet av nya kontrollmetoder följer ett försök till att förklara varför kontrollen och övervakningen ständigt expanderar. Därefter följer ett avsnitt om en ny aktör inom den privata säkerhetsbranschen, nämligen revisionsbyråer. Vad händer när ny teknik kopplas samman med erbjudanden från säkerhetsbranschen att utföra brottsutredningar i privat regi? Om kontrollen av de offentliga övervakningsinstanserna, säkerhets- och underrättelsetjänster stundtals har visat sig vara undermålig[55], så är kontrollen av den privata säkerhetsbranschen så gott som obefintlig. I och med att priset blir allt lägre för mer avancerade tekniker har det uppstått stora möjligheter även för medborgarna att spionera på varandra. Hur värnar vi vår integritet om t.ex. illasinnade grannar eller före detta partners i hemlighet avlyssnar och filmar oss och sedan lägger ut det insamlade materialet på nätet?

Några exempel på teknikens expansion

Expansionen av kontroll och övervakning sker ofta i kölvattnen av dramatiska händelser, händelser som inledningsvis nästintill skapar ett paralyserat tillstånd men där det inom kort kommer starka krav på politikerna att visa handlingskraft. De som i sådana situationer förespråkar införandet av nya integritetskränkande kontrollmetoder har ett klart tolkningsföreträde framför försvararna av den personliga integriteten; oavsett om det finns belägg för metodernas effektivitet eller ej. Denna typ av nyckelhändelser har haft stor betydelse för kontrollteknologins frammarsch. Exempel på en händelse som starkt påverkat kontrollteknologins expansion var de flygplan som rammade World Trade Center och Pentagon den 11 september 2011. Inledningsvis vidtogs omfattande åtgärder i USA men strax där efter påverkades stora delar av övriga världen. Bland det första som åtgärdades var säkerheten vid de amerikanska flygplatserna. Bakgrunden går att spåra till Reagans tid som

[54] Tack till Majken Jul Sørensen för konstruktiva kommentarer på en tidigare version av denna text.

[55] Se t.ex. Säkerhetskommissionen (2003) samt Flyghed (2011).

USAs president då så mycket som möjligt av det offentliga i vågen av New Public Management skulle privatiseras. Det kom även att gälla luftfartsystemet, vilket resulterade i att säkerhetsarbetet på flygplatserna i USA 2001 var helt privatiserat. För att spara pengar, och därmed öka vinsten, lät man underbetalda säkerhetsvakter med bristfällig utbildning sköta kontrollen. När chefen för amerikanska transportministeriet vittnade inför 11 september-kommissionen, menade han att det slarvats med säkerheten för att hålla kostnaderna nere och att det var brister i USAs interna säkerhetskontroll som möjliggjorde de tragiska händelserna 11 september 2001. Dåvarande presidenten George W Bush svarade på kritiken genom att etablera en ny organisation, Transportation Security Administration (TSA), med fler än 50 000 anställda. Numera kostar kontrollen av flygpassagerare USA årligen drygt 10 miljarder dollar, av dessa är 4 miljarder för passagerarscreening och närmare 4 miljarder för kontroll av bagage (Mueller 2006). Trots att säkerhetsunderskottet huvudsakligen var en intern angelägenhet för USA, kom skärpningen av kontrollen även att sprida sig utanför USA. I det anti-terrorsamarbete som USA etablerade med EU, har skärpt flygplatskontroll och en mängd andra anti-terroråtgärder genomförts i de europeiska länderna; oavsett om de enskilda länderna varit i behov av dem eller ej. På till exempel flygplatsen Gardemoen i Oslo spenderas numera dryga 500 miljoner Nkr/år på säkerhetsåtgärder (Hammerlin 2009).

Bland de nya tekniker som utvecklats för flygsäkerheten finns möjlighet till s.k. kroppsscanning i och med systemet Thru-Vision T5000. Tekniken gör det möjligt att på upp till 25 meters håll se genom passagerarnas kläder och scanna deras kroppar i sökandet efter vapen och sprängmedel (Furedi 2007). För att ytterligare minska risken för attentat har företaget QinetiQ utvecklat en sensor som kan byggas in i flygplanets stolar och som mäter passagerarens nivå av oro. Därmed hoppas man kunna upptäcka eventuella flygplanskapare på ett tidigt stadium (Bovard 2003). Samma förhoppningar ligger bakom NASAs forskningsprojekt om att kunna avläsa passagerarnas stressnivå genom att registrera deras hjärn- och hjärtaktivitet, för att på så vis få indikation på vem som kan ha suspekta avsikter med sin flygresa (Hammerlin 2009). Man kan fråga sig hur det går för den ”normalt” flygrädda med hög puls. Dock har de omfattande säkerhetskontrollerna ökat lönsamheten hos de som producerar och sköter säkerhetskontrollerna, men även den affärsverksamhet som bedrivs inom själva flygplatsen har gynnats då vi numera måste vara tidigare på plats innan avresa. Och desto snabbare själva säkerhetskontrollen går, ju mer tid för shopping (Neyland 2009).

En kontrollteknologisk förändring som påbörjade långt innan 11 september 2001, är den explosionsartade ökningen av övervakningskameror (CCTV), kameror som numera också kan kompletteras med mikrofoner och högtalare. Samtidigt som kamerorna blivit mer högpresterande har de blivit allt mindre. De finns numera att tillgå såväl i smartphones som i ett par glasögon. Nästa steg är att ha kamera i kontaktlinser. ”Korean researchers have created a proof of concept of this and tested it on rabbits” (Keenan 2014:42). Bilderna (faceprints) från såväl dolda som öppna kameror kan samköras med bilder från exempelvis pass- och körkortsregistren för att identifiera vem som varit på vilken plats vid vilken tidpunkt.[56] Till kameranyheterna hör utvecklandet av 3D-bilder. Detta är möjligt genom att låta två parallella

[56] Den brottspreventiva effekten av CCTV, det skäl som motiverade att de från början sattes upp, har starkt ifrågasatts. Vad som framkommit är att kameror har haft betydelse vid övervakning av garage och liknande förvaringsutrymmen. Därtill har det i vissa fall visat sig ha en brottsuppklarande effekt. ”A 2009 Scotland Yard report estimated that only one crime was solved per year per thousand cameras” (Keenan 2014:29). Den omfattande användningen av CCTV ingår som en del i det som brukar benämnas ”säkerhetsteatern”. (Se t.ex. Schneier 2010).

kameror ta bilder, Biometric Optical Surveillance System (BOSS) (Keenan 2014). Förhoppningen är att på så vis kunna framställa en 3D-signatur. Genom att ”använda en kombination av infrarött och synligt ljus samt indexera de muskelrörelser som är unik för varje individ” kan man få fram en ”bio-signatur” (Keenan 2014:31).

Intresset för att utveckla biometriska data har sedan länge varit stort. Längst har man kommit vad det gäller scanning av ögats iris, system för identifiering och datalagring av hela ansiktet samt hela kroppen och dess rörelser. Vad det gäller analys av kroppsrörelser detekteras enstaka väldefinierade punkter på kroppen, exempelvis handled, armbågsled, höfter, knän och fotled. Hur punkterna sedan tidsmässigt rör sig i rummet och i förhållande till varandra registreras. På så vis får man fram ett antal mått som bildar en rörelsesignatur. Nya kameror har enligt forskare vid MIT möjlighet att även avläsa en sådan signatur ”through solid walls to an acurancy of ten centimeters” (Keenan 2014:35). Det blir därmed möjligt att identifiera vem som befinner sig i ett hus samt följa hur personen ifråga rör sig; förutsatt att väggarna inte är alltför tjocka. Kopplas sådana kameror till små drönare blir det svårt att värja sig från insyn.

Det handlar med andra ord om en mängd olika typer av insamlade identifieringsdata: fingeravtryck[57], faceprints, ögonscanning, helkroppsbilder i 3D för att inte tala om den gigantiska mängd kommunikationsdata som förmedlas genom telefoner och datorer, såväl i kabel som via satellit. Utveckling pågår även av högsensitiva doftdetektorer för att spåra individers unika kroppslukt som ytterligare en indikator för identifiering. All information kan sedan lagras och vid behov sökas i de hangarliknande dataterminaler som byggts upp. Den som tror att det idag är ett problem för säkerhets- och underrättelsetjänster att lagra och analysera stora mängder insamlad information ”ignores the tremendous increase in computing power, the decrease in storage costs, and rapid improvement in data mining and analysis algorithms that have taken place over the past two decades” (Keenan 2014:203). Idag är det med andra ord inga som helst problem för främst offentliga och privata övervakningsorganisationer att spara den ständigt växande mängden, ofta integritetskänslig, information.[58]

Radio Frequency Identification (RFID)

Taggning med minisändare, små chips som till och med kan injiceras under huden, är en annan teknik som sprider sig. ”In 2004 a beach club in Barcelona started to implant chips the size of a grain of rice into their VIP customers. These RFID chips provided access to restricted areas and also served as identification when buying drinks, allowing customers to wear skimpy attire without needing pockets for ID or credit cards” (Keenan 2014:120). Samma år (2004) beslöt ledningen i en skola i Sutter, Kalifornien, att eleverna skulle vara skyldiga att bära RFID-taggar så länge de var på skolområdet. På så vis kunde man automatisera närvarokontrollen samt ha exakt koll på var eleverna befann sig under skoldagen. Åtgärden väckte massiv kritik, en kritik som inte blev mindre när det framkom att utrustningen skänkts av ett lokalt företag som en marknadsföringsåtgärd för att kunna marknadsföra systemet nationellt. Kritiken resulterade i att taggningen upphörde (Rule 2007).

[57] Bara i USA finns mer än 100 miljoner fingeravtryck från flygplatskontroller lagrade och de ska ligga kvar i åtminstone 75 år. Även EU har infört ett liknande system för dem som reser in och ut i EU (Hammerlin 2009).

[58] Omfattande insamling och lagring av information sker även hos operatörer som Google, Facebook, Yahoo m.fl. (Se vidare Keenan 2014). En närmare belysning av hur dessa bl.a. kommersiellt exploaterar insamlade bilder m.m. faller dock utanför ramarna för denna framställning.

I grunden är det samma teknik som Google nu utvecklat för att vi ska slippa komma ihåg våra lösenord. Vi sväljer ett ”passwordpill” så kan datorn känna av att det är rätt användare. Ett annat alternativ de marknadsfört är att registrera en på kroppen befintlig tatuering som kan scannas för inloggning (Keenan 2014).

Alla dessa tekniska kontrollmetoder skapar en gyllene marknad för kontroll- och säkerhetsindustrin. Den som bemödar sig med att besöka deras branschmässor eller följa deras tidskrifter (t.ex. www.skyddosakerhet.se; www.aktuellsakerhet.se) kan studera företagens stundtals optimistiska marknadsföring av sina produkters effektivitet.

Första tanken som slår en är att dessa nya tekniker främst är av stort intresse för världens nationella säkerhets- och underrättelsetjänster. Tekniker som de vill få de politiska beslutsfattarna att godkänna och därmed få tillgång till. Men det är även möjligt för privatpersoner att skaffa och använda dessa tekniker. Det kan gälla allt från att vara allmänt nyfiken på sin granne som att stalka sin f.d. för att sedan sprida information på sociala media. Tystgående högtflygande minidrönare med kapacitet att fånga upp trådlösa signaler och utrustade med ”infra-red or thermal imaging cameras” (Keenan 2014:82;94) passar i sammanhanget som handen i handsken; vilket måste vara något av lömska paparazzis våta dröm. Men även personer som planerar begå kriminella handlingar som kidnappningar, inbrott och rån torde kunna utnyttja dessa tekniska framsteg.

Vad ska övervakas och kontrolleras?

Vilka är då argumenten för att införa nya övervakningsmetoder? Så gott som uteslutande handlar det om olika typer av samhällsskadliga hot som måste åtgärdas, till övervägande del rör det sig om kriminalitet. De hotbilder som förs fram är ofta exceptionella och dramatiska; hot som om de skulle realiseras skulle få förödande konsekvenser. Inte sällan handlar det dessutom om mycket vaga begrepp som ”terrorism” och ”grov organiserad brottslighet”, begrepp som är ytterst svåra att definiera och därmed kan inbegripa en mängd olika beteenden. Beläggen för de dramatiska hotbilder som presenteras av polisens och andra myndigheters analysenheter är sällan väl underbyggda, stundtals är de helt frånvarande. Det har konstaterats i flera sammanhang (se t.ex. Flyghed 2003; Andersson 2007; SOU 2012:44). Bristen på empiriskt underlag för uppmålade hotbilder framkommer även i den nyligen avlämnade utredningen om organiserad brottslighet (SOU 2014:63). Utredningen lyfter fram olika typer av hot riktade mot politiker, myndighetspersoner, brottsoffer, vittnen och andra som stöd för att den organiserade brottsligheten är ”systemhotande”. De menar vidare att detta är en ”ständigt pågående process” (SOU 2014:63:48) som riskerar att ”´infiltrera´ det lagliga samhället” (SOU 2014:63:66) och därmed leda till stor skada för hela samhället. Men trots att utredarna varken definierar organiserad brottslighet eller lägger fram några empiriska belägg för sina påståenden om samhällshotande brottslighet föreslår de utvidgningar av det straffbara området. De beaktar inte heller alternativa framställningar. T.ex. så har brottsförebyggande rådet visat att de fall av otillåten påverkan som kommer till rättsväsendets kännedom mer sällan förknippas med den organiserade brottsligheten utan oftast rör hot mellan unga och i nära relationer. Påtryckningar från den organiserade brottsligheten riktas också särskilt mot andra inom kriminella nätverk (Brå 2008). Även Säkerhetspolisen har påtalat att den grova organiserade brottsligheten saknar såväl avsikt som förmåga att omkullkasta det demokratiska statsskicket. Vidare framhåller de att ”trots ett relativt stort antal misstänkta fall finns inga exempel på att aktörer inom den grova organiserade brottsligheten tillskansat sig långvarigt inflytande eller betydande ekonomiska vinster genom otillåten påverkan” (SÄPO 2012:4). I

en tidigare utredning skriver tidigare rikspolischefen Sten Heckscher att ”I vissa fall kan det upplevas som att organiserad brottslighet har fogats till en lista över diffusa hot som ingått i politikers och myndigheters retorik” (SOU 2012:44:223). Men sådana mer nyanserande röster har inte haft någon större påverkan på den expanderande kontrollteknikens förespråkare. Dock kan man konstatera att det generellt brister i såväl vad det gäller belägg för hotens relevans som de nya teknikernas effektivitet innan de införs. Och när de väl finns där är det högst ovanligt att det i efterhand görs någon utvärdering om de verkligen varit effektiva på det sätt som påståtts när de introducerades.

Varför denna expansion?

Om det då ofta brister vad det gäller beläggen för dessa dramatiska hot, hur kommer det sig då att kontrollen och övervakningen ständigt expanderar? Även de mest exceptionella åtgärder tenderar efter hand att normaliseras. Ofta införs dessa kontrolltekniker i tvångsmedelsarsenalen mot extrema hot som ”terrorism”, ”grov organiserad brottslighet” eller liknande, för att med tiden expandera och även vara möjliga att använda mot lindrigare typer av brottslighet. En förklaring finns hos fem centrala aktörer i sammanhanget.[59] Deras olika motiv och intressen vad det gäller ny kontroll- och övervakningsteknologi samt aktörernas olika relation till integriteten påverkar expansionsprocessen. I figur 1 görs en idealtypisk framställning av förhållandet mellan aktörernas externa (manifesta) rationalitet respektive deras interna (latenta) rationalitet samt deras relation till integritet. En idealtypisk framställning utesluter självfallet inte att det förekommer överlappningar och interaktion mellan aktörerna. Främst är det de fem aktörernas interna rationalitet som bidrar till normaliseringen av det exceptionella (Flyghed 2000).

[59] De 5 aktörerna är inte rangordnade eller viktade på något sätt. Se vidare Flyghed (2007).

Aktör	Extern rationalitet	Intern rationalitet	Integritetshänsyn	
			Lagstadgade	Andra
Politiker	Bekämpa brott	Ny lagstiftning som symbol för handlingskraft	Primär uppgift Upprätthålla lagstadgade medborgerliga fri- o rättigheter	Opinionstryck från väljare
Polis	Bekämpa brott	Expandera organisationen, ökad resurstilldelning	Respektera, följa, lagstadgade medborgerliga fri- o rättigheter och annan lagstiftning	
Säkerhets-industrin	Effektiv kontroll av brott och brottslingar	Öka branschens betydelse, maximera profiten	Inte primärt	Kundens krav på diskretion Ev. etiska åtaganden, uppförandekoder
Media	Förmedla information	Lösnummerförsäljning, maximera profiten	Inte primärt	Källskydd, anonymitet till uppgiftslämnare
Experter	Producera kunskap	Uppmärksamhet, bli citerad, karriärkliv	Skyldighet etikgranska projekt.	Anonymisera enskilda individer i publicerade forskningsresultat

Figur 1: *Idealtypisk framställning av fem aktörers relation till kontrollexpansion*.

Politikernas uttalade syfte är att bekämpa brott. Målet är att minska brottsligheten och öka människors trygghet. Men politikerna använder också lagstiftningens symbolfunktion för att visa sina väljare att de är handlingskraftiga. Kontrollpolitiken är en arena som uppfyller de nödvändiga rekvisiten för sådana manifestationer.

Till *polisens* huvuduppgifter hör att kontrollera brott samt upprätthålla allmän ordning och säkerhet. Detta utgör den externa rationaliteten. Den interna rationaliteten är att de av organisationsegoistiska skäl ständigt önskar expandera verksamheten och få mer resurser. För att legitimera organisationens fortlevnad hänvisas till nya hotbilder som för att kunna

motverkas kräver nya övervakningstekniker (Benyon 1996). En sådan organisationsrationalitet är inget unikt för polisen utan gäller alla byråkratier (Emsley 1997).

Av särskilt intresse här är den *privata kontrollindustrin.* Dess externa rationalitet är att erbjuda effektiv kontroll och därmed öka medborgarnas trygghet. Men företagen vill också maximera sina marknadsandelar, bland annat genom att öka intresset för att allt fler områden i samhället övervakas och kontrolleras. I affärsidén ligger att göra profit på individers och institutioners rädsla för brott, såväl berättigad som oberättigad. Exploaterandet av denna oro är en stark drivkraft till kontroll- och övervakningsexpansionen.[60] Kontrollindustrin, i synnerhet övervaknings- och informationsteknologin, har ett starkt fokus på de olika produkternas tekniska effektivitet. De presenterar ständigt nya produkter som ger polisen, men även politiker, förhoppningar om att teknik effektivt ska kunna minska brottsligheten.

Medias externa rationalitet ligger i att förmedla information. Men dess intresse att sälja lösnummer samt samla många lyssnare och tittare, och därmed öka intäkterna genom reklam och abonnemang, leder till en fokusering på dramatiska och exceptionella händelser. Denna selektion av det extrema resulterar i en skevhet i bilden av de hot som sägs motivera den kontrollteknologiska utvecklingen.

Experternas externa rationalitet är att bistå med kunskap. I stor utsträckning handlar det om forskare som anlitas av myndigheter och organisationer för att leverera beslutsunderlag. Även säkerhetsföretagen och övriga delar av näringslivet har stort behov av experter; experter som ofta är kopplade till olika typer av tankesmedjor (Rich 2004). Medias behov av experter som uttalar sig är också mycket stort, något som stundtals leder till att epitetet ”expert” inte alltid är liktydigt med kunnande. Till experternas interna rationalitet hör att på olika sätt skaffa sig uppmärksamhet som kan vara till fördel i samband med framtida forskningsansökningar och avancemang i karriären. Jakten på uppmärksamhet gynnar inte alltid producerandet av god vetenskap.

Den högra kolumnen, *Integritetshänsyn*, vill indikera att de fem aktörerna i sina respektive verksamheter skyddar helt olika kategoriers integriteter. För vissa av dem, främst då politiker och polisen, finns det lagstadgad skyldighet att beakta och värna medborgarnas integritet. För de andra tre handlar det om andra hänsynstaganden. Media ska framförallt garantera uppgiftslämnares integritet genom anonymitetsskyddet. Experterna i form av forskare har etiska regler att följa vad det gäller att skydda de enskilda personers integritet som ingår i studerade populationer. Säkerhetsindustrins integritetsskydd utgör ytterligare en kategori. Den integritet de primärt värnar är den betalande kundens rätt till diskretion, d.v.s. slippa offentlig insyn. Hur detta tar sig uttryck utvecklas i följande avsnitt.

Privata brottsutredningar

Men det är inte enbart själva tekniken av kontrollen som snabbt förändrats. Det gäller även förekomsten av nya aktörer inom kontrollandskapet. Ett för svenska förhållanden relativt nytt sådant område är att privata aktörer på konsultbasis erbjuder olika typer av utredningar, däribland regelrätta brottsutredningar, d.v.s. klassisk polisiär verksamhet. På deras hemsidor

[60] Se Mueller 2006 för en beskrivning av orons betydelse i dessa sammanhang.

hamnar sådan verksamhet främst under rubriken Forensic.[61] Säkerhet har blivit en vara som säkerhetsföretagen kan marknadsföra till de organisationer och individer som har möjlighet att betala. Internationellt handlar det om mycket stora företag. Som exempel kan nämnas att Group4Securicor (G4S), som är det internationellt största privata säkerhetsföretaget, har närmare 600 000 anställda i 110 länder (Abrahamsen & Williams 2011). Även Securitas tillhör de större med en verksamhet i 40 länder och med drygt 240 000 anställda (Abrahamsen & Williams 2011). I Sverige har G4S och Securitas omkring 4000 respektive 9000 anställda (Berndtsson & Stern 2011). För samtliga gäller att de vuxit mycket snabbt, såväl vad det gäller omsättning som personal. Med tiden har branschen också blivit alltmer nischad mot olika specialområden (Abrahamsen & Williams 2011).

Ett exempel på en ny privat aktör som hittat en nisch på säkerhetsmarknaden är revisionsbyråerna. I deras verksamhet ingår numera mycket mer än traditionell revisorsverksamhet. Modellen att enbart detaljgranska varje enskild verifikation är idag föråldrad, nyckelbegreppet har blivit intern kontroll vilket omfattar en betydligt vidare verksamhet (Wallerstedt 2009; Arwinge 2015). Ett nytt verksamhetsområde är att de större byråerna har startat underavdelningar som erbjuder företag och organisationer kompetens för att utreda oegentligheter, även misstänkt brottslighet. De stora firmorna i Sverige, som Ernst and Young (E&Y), KPMG, PriceWaterhouseCoopers (PWC) och Deloitte and Touche, har satsat på kvalificerad utredningsverksamhet och inrättat särskilda enheter för riskanalys.

I en studie av tre av de största revisionsbyråerna i Sverige (PWC, E&Y och KPMG) framkom att de bland sina tjänster kan erbjuda brottsutredande verksamhet. Denna verksamhet bedrivs inom särskilda forensicavdelningar.[62] Omfattningen av verksamheten varierar mellan de tre där PWC är störst och KPMG minst. På deras forensicenheter arbetar revisorer, jurister, f.d. åklagare, ekonomer, IT-experter samt säkerhetsexperter med tidigare erfarenhet främst från polisen eller militären. Alla tre har stort utbyte med sina respektive moderbolag som är verksamma över större delen av världen. T.ex. har PWC drygt 2200 anställda i 59 länder som enbart sysslar med Forensic. Av Ernst & Youngs mer än 100 000 anställda över hela världen arbetar cirka 1000 personer i ett 40-tal länder med vad de benämner som Fraud Investigation and Dispute Services (FIDS). Inom KPMG har det internationellt funnits avdelningar för forensic i drygt 15 år, men enligt chefen för svenska KPMG/Forensic är verksamheten i Sverige förhållandevis nystartad. Den drog igång 2003 och idag arbetar tre revisorer, en IT-expert samt analytiker med ekonomi och/eller IT-bakgrund på avdelningen. I och med att de har kontor över hela världen finns stor språkkompetens vilket ofta är betydelsefullt. T.ex. kan KPMG i Sverige som är relativt små här kontakta ”KPMG/Holland som har kommit långt vilket vi kan utnyttja”.

Uppdragen kommer oftast från större företag, och det behöver inte handla om lagbrott utan kan även röra sig om brott mot företagets uppförandekod eller branschens etiska regler. Det kan t.ex. gälla dataintrång, korruption, förskingring, finansmarknadsbrott som finansiell rapportering och falska fakturor eller brott mot antitrustlagar. I uppdragen ligger fokus huvudsakligen på att reparera, säkra tillgångar och förhindra att det händer igen.

[61] Forensics, eller egentligen forensic science, är ett inte helt lättöversatt begrepp. Stundtals står det för brottsutredning andra gånger för kriminalteknik eller teknisk utredning. Här kommer jag använda det som beskrivning för olika tekniker ämnade för att utreda normöverträdelser.

[62] Om inte annat sägs är uppgifterna i detta avsnitt hämtat från Flyghed (2014).

Det förekommer också att de får uppdrag från olika typer av ideella organisationer och offentliga verksamheter. De har t.ex. utrett flera fall av korruption/mutor inom kommun och landsting. Det är inte ovanligt att sådant förekommer vid t.ex. upphandling där det stundtals kan röra sig om kontrakt på stora belopp. Men ”vi sysslar ju med större affärer, där de kan betala, så enskilda med mindre kontokortsbedrägerier blir ju inte aktuella för oss”, som chefen för KPMG:s forensicavdelning formulerat det.

PWC är även i vissa fall med och assisterar polis och åklagare i förundersökningar. Till exempel kan PWC göra DNA-analyser i samband med sina utredningar. I Sverige har de ”ett eget forensic-lab i huset med hög kompetens att spegla hårddiskar och mobiltelefoner”. De har kapacitet att kolla många personer samtidigt. Detta har gjort att svenska PWC har många utländska företag som kunder. T.ex. ”speglades” (kopierades) i ett uppdrag från Tyskland 1150 persondatorer. Oftast går man tillbaka flera år och kollar e-post m.m. All information sparas så länge utredning pågår. Företagen gör även personliga bakgrundskontroller, huvudsakligen baserad på offentliga uppgifter som att kolla inkomst och jämföra med ”livsstil” och stora utgifter. De gör även sociogram över släkt och bekanta, ”bygger träd”, för att hitta kopplingar, t.ex. till personer i andra företag. I dessa utredningar använder de all den teknologi de har tillgång till för att samla information och kartlägga den person den fått uppdrag att utreda. Därefter blir det upp till deras respektive analysavdelningar att bearbeta materialet och skriva rapport.

Revisionsbyråerna gör inga juridiska bedömningar, utan lämnar över det sammanställda materialet till kunden som får besluta om och hur de vill gå vidare. Dock finns det ett undantag och det är om det finns anledning att misstänka penningtvätt. Då ska informationen lämnas vidare till den egna huvudrevisorn som i sin tur är skyldig att rapportera till polisen. Under hela processen är det i övrigt kunden, uppdragsgivaren, som bestämmer om utredningen ska lämnas vidare till polis och åklagare. Det är det företag som betalar som äger frågan om hur ärendet ska hanteras. Detta är ett viktigt inslag i deras affärsidé. Därmed sagt att misstänkta brott som utreds av privata firmor inte alltid kommer till polisens kännedom. Den internationella erfarenheten är att företag endast undantagsvis väljer att åtala sina anställda. ”It is typical for the private sector to settle internal problems quietly” (Dorn & Levi 2007:224. Se även Ericson & Haggerty 1997).

En betydelsefull skillnad mellan polisen och säkerhetsfirmorna är att de förstnämnda ser normbrott som lagbrott medan de sistnämnda huvudsakligen betraktar det som affärsproblem. För de privata aktörerna är inte det viktigaste att få någon straffad i domstol; istället ligger prioriteringen på att stoppa läckan, få tillbaka förlorade tillgångar/minska förlusten samt förhindra att det sker igen.

Effektiv diskretion

Hur kommer det sig att etablerade företag och organisationer vänder sig till revisionsbyråer och säkerhetsföretag och inte enbart till polisen när de misstänker brottslighet? I den studie som gjorts av svenska förhållanden framkom att det huvudsakligen finns två skäl som gör att företag vänder sig till revisionsbyråer och säkerhetsföretag i sådana situationer. Det ena är effektivitet och det andra är diskretion. Effektivitetsskälet grundar sig i att man anser att dessa säkerhetsfirmor på flera områden har såväl högre kompetens som arbetar snabbare än vad polisen med sina begränsade resurser har möjlighet till. Flera av de tillfrågade företagen beskrev polis- och åklagarvägen som trög. Men det kanske viktigaste skälet att anlita en privat

firma är möjligheten till diskretion. Den som betalar för den produkt som säkerhetskonsulterna levererar behåller kontrollen över hur den sammanställda informationen skall användas, om de vill ha offentlighet eller ej. Gör företaget bedömningen att ett överlämnande till polis och åklagare riskerar att leda till negativ publicitet som kan skapa badwill, är det stor sannolikhet att information om eventuella lagbrott aldrig hamnar i offentlighetens ljus utan får stanna inom företaget. Hamnar det hos polis och åklagare, och eventuellt senare i domstol, tappar de kontrollen över hur mycket som blir offentligt. Därtill kommer risken för informationsläckage inom polisen. Revisionsbyråernas diskretion och sekretess väger alltså tungt, det vill säga värnandet om kundens integritet. Men den höga sekretessnivån och viljan att undvika offentlighet handlar inte enbart om oro för badwill, utan även om att skydda affärshemligheter från konkurrenter (Manning 2000).

De privata aktörerna i polislandskapet

En möjlighet att förstå vilken plats revisions- och säkerhetsfirmors forensic-verksamhet har i ett polisiärt landskap är att utgå ifrån en schematisk framställning av polisarbetet (se vidare Flyghed 2000). Proaktivt polisarbete syftar på verksamhet *innan* brott begåtts och reaktivt på åtgärder *efter* det att brott begåtts.

	PROAKTIVT	REAKTIVT
REPRESSIVT (Integritetskränkande)	***1*** Inhämta, sammanställa och bearbeta information i förebyggande syfte. Förspaning. Underrättelseverksamhet.	***2*** Inhämta, sammanställa och bearbeta information om misstänkta oegentligheter, brottslighet. Brottsutredningar.
ICKE REPRESSIVT (Ej integritetskränkande)	***3*** Prevention, skapa säkra rutiner. Utbildning och information.	***4*** Utredningar och rapporter. Klassisk revision och bokföring.

Figur 2: *Schematisk framställning av privata aktörers verksamhet.*

Revisionsbyråernas forensic-verksamhet återfinns i ruta 2: repressiv reaktiv verksamhet genom sin underrättelsebaserade brottsutredande verksamhet; samt i ruta 3: proaktiv icke-repressiv verksamhet i och med deras utbildning och information om riskbedömningar. I ruta 4 befinner sig den klassiska revisionsverksamheten. Här återfinns även den typ av utredningar

som advokatbyråer utför på uppdrag av företag, som t.ex. Mannheimer Swartlings[63] rapport om TeliaSonera. Förutom vid bakgrundkontroller vid anställningar har det inte framkommit något som tyder på att repressiv proaktiv verksamhet (ruta 1) för närvarande bedrivs i Sverige inom de företag som är aktuella här. Däremot har säkerhetsföretag på konsultbasis utfört sådant arbete utomlands. Ett exempel är den svartlistning av fackligt aktiva som svenska SKANSKA och andra byggföretag gjorde 2013 utifrån underrättelsematerial som sammanställts av ett konsultbolag (Green 2013). I USA, Canada och Storbritannien utför såväl risk- och säkerhetsföretag som revisionsbyråer repressivt proaktivt polisarbete. Privatiseringen av amerikanskt underrättelsearbete tilltog drastiskt efter 11 september i och med att Department of Homeland Security (DHS) inrättades[64].

Det finns även exempel på fall där privata säkerhetsfirmor använt sig av olagliga metoder, i vissa fall på uppdrag av polisen som ansett sig vara ”kringskurna av lagstiftning” (Williams 2005:199). Säkerhetsfirmor har även på uppdrag av företag utfört underrättelseverksamhet mot organisationer och personer som företaget uppfattat som kritiska mot deras verksamhet. Enligt Eveline Lubbers har denna typ av verksamhet gått från att tidigare huvudsakligen ha varit reaktiv till att i allt större utsträckning bli proaktiv. Som exempel nämner hon bl.a. Shells strategi för att neutralisera kritiken mot deras engagemang i Sydafrika under apartheidtiden (Lubbers 2012). O´Reilly och Ellison nämner hur McDonalds använt privata säkerhetsföretag för att infiltrera och delta i protestgruppers möten (O´Reilly & Ellison 2006). Nestlé gjorde för några år sedan detsamma i Schweiz (Gautier 2009).

I vilken utsträckning kommer dessa privata aktörer utöka sin användning av ny kontrollteknologi? Och vilka konsekvenser kommer deras förhållandevis oreglerade verksamhet ha för vår integritet? Redan nu finns det anledning att fråga sig hur integriteten för den anställde som utreds av privata aktörer beaktas. Det har framkommit att i vissa fall får de inte ens reda på att de varit föremål för en intern utredning, främst då det visat sig att misstankarna var ogrundade. Man kan också undra hur en anställds integritet och rättssäkerhet värnas i samband med att den konfronteras med en utredning som är gjord på företagets uppdrag. Vid samtal med de större fackliga organisationerna i Sverige uppgav de att de hade väldigt liten koll på detta, i vissa fall visste de inte ens att det förekom.

Staten tappar kontroll?

I och med säkerhetsföretagens inträde på arenan har statens kontroll möjligen naggats något i kanten. Hos företagen resoneras det vidare i strikt ekonomiska termer om kostnadseffektivitet och profitmaximering, såväl för det utredande säkerhetsföretaget självt som det företag som anlitar deras konsulttjänster. Detta skiljer sig från hur staten resonerar kring medborgarnas säkerhet; där finns inte samma typ av vinstintresse som driver privata företag. För framtiden

[63] ”Vi anlitas ofta för att genomföra internutredningar av potentiella oegentligheter, såsom anklagelser om korruption, oriktig redovisning och liknande brister som förs fram av tillsynsmyndigheter eller så kallade whistleblowers”. Från Mannheimer Swartlings hemsida 2014-11-19. http://www.mannheimerswartling.se/expertis/verksamhet/corporatecomplianceandinvestigations/.

[64] Vid starten i november 2002 hade DHS 170000 anställda, fördelade på 22 underavdelningar. 2009 tilldelades DHS 44,3 miljarder dollar i den amerikanska statsbudgeten (Hammerlin 2009). Därtill kommer ytterligare miljarder spenderade av ”state and local governments” (Mueller 2006:31). En stor del av dessa pengar hamnade hos privata säkerhetsföretag. Även delar av analysarbetet har outsourcats på sådana företag, bland annat görs en stor del av CIA:s analyser av kontrakterade säkerhetsföretag (Hughes 2007; Shorrock 2008).

blir det intressant att se i vilken utsträckning de nya kontrollteknikerna kommer att användas av privata intressen, såväl inom säkerhetsbranschen som av enskilda personer. Vad händer med integriteten om privata utredare som revisionsbyråer, säkerhetsföretag och advokatbyråer använder ny kontrolteknologi som exempelvis avancerade kameror och avlyssningsapparatur? Om integritetsskyddet stundtals är bristfälligt vad det gäller den offentliga maktens övervakning, hur ser det då ut inom den privata sektorn? När verksamheten bedrivs i statens regi är uppdragsgivaren, åtminstone teoretiskt, i slutändan medborgarna i egenskap av skattebetalare och det är deras säkerhet som ska värnas. Det är gentemot dessa som statens säkerhets- och underrättelsetjänster har sitt ansvar. Men de kontrakterade företagen och revisionsbyråerna står till svars inför en helt annan kategori: nämligen ägare och bolagsstyrelse och vars intresse är att öka sina marknadsandelar och maximera sin profit. De privata firmornas profitintresse gör också att de har ett stort intresse av att påverka det offentligas hotbildsuppfattning och de blir därmed delaktiga i ”shaping the politics of protection” (Berndtsson 2012:2). Då dessa privata processer är skyddade från insyn väcker det frågor om vilken grad av rättssäkerhet och integritet en person inom ett företag som är misstänkt för oegentligheter kan räkna med. Hur påverkas valet av metoder när det inte finns någon tillståndsgivande och granskande instans? Bristen på legal och politisk kontroll och därmed insyn är ett genomgående problem beträffande den privata säkerhetsindustrin (Pütter 2010; Evans & Lewis 2013).

Integriteten och den rena mjölpåsens dilemma

Avslutningsvis vill jag beröra två oroväckande inslag i debatten om ny kontrollteknologi, det ena är argumentet om ”rent mjöl i påsen” och det andra är tendensen till invertering av betydelsen av integritet och därmed urholkning av begreppets ursprungliga betydelse. Det sistnämnda framkom bland annat i en debatt om kameraövervakning våren 2014 mellan företrädare för säkerhetsbranschen och Datainspektionen (DI). Säkerhetschefen för Jernhusen AB, Leif Svensson, anklagade DI för att inte respektera brottsoffrens integritet då DI överklagat ett antal beviljade tillstånd att sätta upp övervakningskameror.[65] ”Nu är det dags att sätta fokus på att skydda brottsoffrens integritet och inte brottslingens” (SvD 140429). Någon vecka senare fick han medhåll av ytterligare några branschföreträdare, då med Säkerhetsbranschens ordförande Björn Eriksson och ordföranden för Säkerhet för Näringsliv och Samhälle, Åke Andersson, i täten (SvD 120505).[66] Även de hävdade att skepsis till nya övervakningsmetoder gynnar brottslingarnas integritet på bekostnad av brottsoffrens integritet. Det grundlagsstadgade skyddet för vår personliga integritet, värnandet om vårt privatliv, ska därför inskränkas med hänsyn till tänkbara framtida brottsoffer. Givetvis är det positivt att minska antalet brottsoffer, men dessa två kan inte ställas mot varandra på det sättet. Men det är ju inte brottslingars integritet som står i främsta rummet utan den absoluta dominerande delen av dem som fångas på kamerorna: d.v.s. vi andra. Det är de som inte ens är i närheten av att misstänkas för brott vars integritet det handlar om. Konsekvenserna av att ställa vårt integritetsskydd åt sidan med motivet att förhindra framtida brottsoffer skapar stora möjligheter för mycket omfattande ingrepp i det för demokrati och rättsstat så viktiga integritetsskyddet.

[65] Det visade sig inte vara fler än 10 % av samtliga tillstånd som DI hade överklagat.

[66] Övriga undertecknare i denna andra artikel var Lennart Alexandrie ”publisher, SecurityUser.com” samt Dick Malmlund ”säkerhetsexpert och före detta säkerhetschef för Svensk Handel”. En poäng i sammanhanget är att någon vecka efter detta meningsutbyte kom Brås utvärdering av kameraövervakningen på Stureplan och Medborgarplatsen och som visade högst marginella effekter av övervakningskameror.

Ett annat återkommande inslag i debatten om kontrollsamhällets expansion är det vi kan kalla rentmjölipåsen-argumentet. Den som har rent mjöl i påsen har inte något att dölja och därför är det inga problem att bli avlyssnad, filmad och registrerad. Men ett sådant resonemang leder fel då tanken om rentmjölipåsen är baserad på vad som kan liknas med omvänd bevisbörda. Det leder nämligen till att det blir upp till oss som medborgare att styrka vår oskuld för myndigheterna, när det är de som enligt vedertagna rättsstatsprinciper ska belägga vår skuld. För att bevisa att vi är oskyldiga måste vi paradoxalt nog godkänna att vi behandlas som misstänkta och där detta accepterande utgör själva beviset på vår oskuld. Även den som inte begått något lagstridigt blir potentiellt misstänkt. Grundfrågan är och förblir om vi vill att övervakarnas smutsiga fingrar ska få peta i vårt rena mjöl. Och detta oavsett om det är den statliga säkerhetspolisen eller privata säkerhetsföretag som kontrollerar oss.

Referenser

Abrahamsen, R. & Williams, M. (2011) *Security beyond the State. Private Security in International Politics*, Cambridge: Cambridge University Press.

Arwinge, O. (2015) *En introduktion till intern styrning och kontroll*, Riga: Sonoma.

Berndtsson, J. (2012) Security Professionals for Hire: Exploring the Many Faces of Private Security Expertise, *Millennium – Journal of International Studies*, no. 1/2012, 1-18.

Berndtsson, J. & Stern, M. (2011) Private Security and the Public-Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage, *International Political Sociology* no.5, 408-425.

Bovard, J. (2003) *Terrorism and tyranny: Trampling freedom, justice, and peace to rid the world of evil*, New York: Palgrave Macmillan.

Brå (2008) *Otillåten påverkan mot brottsoffer och vittnen*, Rapport 2008:8, Stockholm: Brottsförebyggande rådet.

Dorn, N. & Levi, M. (2007) European Private Security, Corporate Investigation and Military Services: Collective Security, Market Regulation and Structuring the Public Sphere, *Policing & Society* vol.17, no.3, 213-238.

Ericson, R. & K. Haggerty (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.

Eriksson, B.; Andersson, Å.; Alexandrie, L.; Malmlund, D. (2014) Kameror oroar DI mer än kriminaliteten, *Svenska Dagbladet Brännpunkt* 5 maj.

Evans, R. & P. Lewis (2013) *Undercover. The True Story of Britain´s Secret Police*, Croydon: Guardian books.

Flyghed, J. (red.) (2000) *Brottsbekämpning – mellan effektivitet och integritet. Kriminologiska perspektiv på polismetoder och personlig integritet*, Lund: Studentlitteratur.

Flyghed, J. (2003) Den hotfulla säkerheten i Flyghed, J & Hörnqvist, M (red.): *Laglöst land. Terroristjakt och rättssäkerhet i Sverige*, Ordfront förlag.

Flyghed, J (2007): Kriminalitetskontroll – baserad på tro eller vetande? *Svensk Juristtidning*, årg.92, nr.1.

Flyghed, J. (2011) Cover Up or Dig Up? Inquiries into Security Services in Welfare States: The Cases of Norway, Sweden and Denmark i Stuart Farson & Mark Phythian (red.): *Commissions of Inquiry and National Security: Comparative Approaches*, Praeger/ABC-CLIO.

Flyghed, J (2014) Privat område? Revisionsbyråers och säkerhetsföretags polisarbete i Finstad & Lomell (red.) *Motmæle – en antologi til Kjersti Ericsson, Cecilie Høigård og Gurli Larsen*. Oslo.

Furedi, F. (2007) *Invitation to terror: The expanding empire of the unknown*, London: Continuum.

Gautier, D. (2009) Nestlégate. Private Spioninnen im Dienste von Nestlé, *Bürgerrecht & Polizei* nr. 2,76-82.

Green, A. (2013) Skanskas ursäkt pr-strategi, *Arbetaren* nr.42.

Hughes (2007) *War on Terror, Inc. Corporate Profiteering from the Politics of Fear*, New York: Verso.

Lubbers, E. (2012) *Secret Manoeuvres in the Dark. Corporate and Police Spying on Activists,* London: Pluto Press.

Manning, P.K. (2000) Policing New Social Spaces i Sheptycki, James (red.) *Issues in Transnational Policing*, London: Routledge 2000.

Mueller, J. (2006) *Overblown. How politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*, New York: Free Press.

O´Reilly, C. & Ellison, G. (2005) `Eye Spy Private High´. Re-Conceptualizing High Policing Theory, *British Journal of Criminology*, vol.46, 641-660.

Pütter, N. (2010) TSC, FACI, TCS: Privatisierte Sicherheit im globalen Kontext, *Bürgerrecht und Polizei* nr. 3, 53-60.

Rich, A. (2004) *Think Tanks, Public Policy, and the Politics of Expertise*, Cambridge: Cambridge university press.

Rule, James B. (2007) *Privacy in Peril. How we are sacrificing a fundamental right in exchange for security and convenience*, New York: Oxford university Press.

Schneier, B (2010). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, New York: Copernicus.

Shorrock, T. (2008) *Spies for Hire. The Secret World of Intelligence Outsourcing*, New York: Simon & Schuster.

Svensson, L. (2014) Datainspektionen ser inte till brottsoffren, *Svenska Dagbladet Brännpunkt* 29 april.

Wallerstedt, E. (2009) *Revisorsbranschen i Sverige under 100 år*, Stockholm: SNS förlag.

Williams, J.W. (2005) Governability Matters: The Private Policing of Economic Crime and the Challenge of Democratic Governance, *Policing & Society* vol.15, no.2 June, 187-211.

En virtuell kompis

Petrus Bolin

Kärt barn har många namn, men ordet övervakningskamera gör ju att man får helt fel inställning till fasta kameror (CCTV, Closed Circuit Television). Jag tänker skriva några rader utifrån användarens perspektiv och på så sätt försöka få in vardagens verklighet i en teoretisk debatt.

Undertecknad har tio års poliserfarenhet i Stockholm och därefter tio år som säkerhetschef i tre stora detaljhandelskedjor, Pressbyrån, 7/eleven och Coop/KF koncernen. Jag har även snart fem år bakom mig som Koncernsäkerhetschef för Handelsbanken så det är från en ganska bred operativ och strategisk bakgrund jag uttalar mig.

Idag har i princip alla större detaljhandelskedjor och banker kameror installerade i sina butiker och kontor. Syftet med installationerna är att öka tryggheten för personal och kunder samt minska risken för brott. Ytterligare ett syfte är att om ett brott skett öka sannolikheten att kunna lagföra en gärningsman.

Vid installation av CCTV så finns det en mängd regler att förhålla sig till. Jag tänker inte gå in på alla regler i detalj utan kan bara konstatera att de bolag jag jobbat i sköter sig och givetvis lägger stor vikt vid att följa lagar och förordningar.

Problemet med dessa regler är att det inte är användaren som skrivit dem. Det medför problem i den verkliga världen, ute i samhället, i butiker och på kontor eller arbetsplatser där medarbetare dagligen utsätts för brott. En kamerainstallation i en liten Pressbyråbutik är en stor investering eftersom varje enhet måste bära sina egna kostnader. Låt oss säga att ett system lågt räknat kostar ca 40tkr att sätta in och driftsätta. Det skall ställas mot en mindre omsättning och inte ovanlig slutlig vinst på kanske 100tkr/år för en liten Pressbyråbutik. En sådan investering är kännbar och det krävs därför att systemet som köpts faktiskt har ett tydligt syfte och att det någonstans finns en payback, antingen i rena pengar (minskat svinn, färre brott) och/eller ökad trygghet (färre eller inga brott).

Det är alltså inte, om någon nu trodde det, för nöjes skull som ett kamerasystem installeras i en butik eller i ett kontor.

Utifrån en användares ögon så är ju kameror något subjektivt, något man har svårt att förhålla sig till eftersom namnet övervakningskamera är så negativt laddat. Gemene man har vanligtvis heller ingen kunskap om tekniken och eventuella syften med den. Här har lagstiftaren, Polis, leverantörer, fackliga företrädare och säkerhetsbranschen ett, som jag tycker, delat ansvar. Även vi säkerhetschefer har en intellektuell utmaning i att utbilda och övertyga de som arbetar i driften till att acceptera kameror som en given brottsförebyggande del i det brottsförebyggande arbetet.

Sammantaget kan jag säga att jag anser att branschen misslyckats med att beskriva varför kameror behövs. Och igen har branschen låtit sig styras alltför mycket av lagstiftaren och underlåtit att driva en innovativ och verklighetsförankrad samhällsdebatt i ämnet. Leverantörer och tillverkare har varit alldeles för inne på att utveckla tekniken men helt glömt bort att prata om syftet och eventuell payback. Tillverkarnas ointresse att prata utveckling

med sina kunder är även det anmärkningsvärt. Lagstiftaren har i sin tur valt att se CCTV som något läskigt, integritetskränkande och negativt. Polisen har haft en märkligt osynlig roll i debatten kring CCTV i samhället vilket även det är mycket intressant. Inte minst med tanke på att det idag nästintill är omöjligt att få en förundersökning initierad UTAN bild eller film på den anmälda händelsen.

Resultatet blir att CCTV-anläggningarna inte nyttjas fullt ut och att det förebyggande säkerhetsarbetet försämras. De som vinner på detta är givetvis gärningsmännen eftersom risken att åka dit kraftigt minskar.

Sammantaget anser jag att regler och lagar i allt för stor del fått utformas av teorier och för lite utifrån ett samhälle i rasande snabb teknisk utveckling, en förändrad och mer komplicerad kriminalitet samt, inte minst med utgångspunkt från brottsoffret.

Bild 1. *Tagen ur en film på ett kontorsrån på en Pressbyrå i västra Stockholm 2003. Denna och ytterligare ett par bilder från samma rån visades under 2003 i Efterlyst och fick rånarna gripna för sammanlagt 5 grova rån.*

När den nya kameralagen utformades blev jag uppringd av ”utredaren” som ryktesvis fått höra att jag hos min tidigare arbetsgivare Coop arbetat med att ta reda på vad brott ekonomiskt kostade företaget. Det som förvånade mig, var att det var första gången som utredaren pratade med någon som kunde prata om payback när det gäller CCTV-installationer. Jag menar att frågan om payback och bevisat positiva effekter med CCTV-övervakning är av avgörande värde i ett beslut eller en lagstiftningsprocess. Utan den informationen överlåts till andra att föra oemotsagda teoretiska diskussioner, någonstans måste ju den teoretiska personliga integriteten vägas mot andra eventuella positiva effekter.

Jag kommer att försöka utveckla min syn på detta längre fram i skriften.

Förutom payback och positiva effekter finns det ytterligare en sak som jag anser har missats i lagstiftningen och det är synen på CCTV-installationens syfte och eventuella krav och regler för innehavare av systemen.

Min uppfattning är att regelverket i samband med en CCTV-installation i mycket högre grad skall fokusera på syftet med installationen. Jag tycker också att regelverket i högre grad skall kravställa hur det inspelade materialet får hanteras. Idag finns teknik som tydligt möjliggör en ökad möjlighet att minska ner antalet individer som har tillgång till det inspelade materialet. Finns det ett klart och accepterat syfte skall användaren enligt min uppfattning få filma i hela butiken/kontoret och givetvis spara bilderna efteråt. Jag anser också att användaren bör få filma utanför butiker och kontor, jämför exempelvis med bankomater. Hårdare krav skall istället läggas på hur det inspelade materialet skall hanteras. Exempelvis krav på polisanmälan eller liknande.

Det skulle innebära att kamerorna skulle kunna användas till sin fulla potential och det är något vårt samhälle i stort skulle ha stort värde av.

Sammantaget anser jag att större vikt skall läggas på syfte och på tydligare krav på användaren. Kraften bör läggas vid att tydligt lagstifta mot felaktig användning av inspelat material, inte som nu att alla dras över en kam. Att jämföra med ett skjutvapen, det är inte farligt förrän det hamnar i fel händer.

Syfte, payback och positiva rånförebyggande effekter

Jag skulle vilja återvända till syftet och eventuell payback. En användare (köpare) av ett CCTV-system har en inte en helt lätt uppgift. Först skall köparen se ett behov och ta beslut om en möjlig investering. Därefter skall köparen ta reda på vilken teknik som är bra för just dem, begära in offerter och ta beslut. Vid offertgenomgång så bör köparen få någon insikt i varför de skall köpa ett visst system och vilket värde systemet kan komma att tillföra. Dessutom skall köparen av ett CCTV-system sätta sig in i lagstiftning, förhålla sig till den, informera personal, eventuella kunder samt förhandla med fackliga företrädare.

Vad jag skulle vilja fördjupa mig i är just värdet för köparen i samband med en investering i ett CCTV-system. Under alla mina femton år som säkerhetschef så har jag aldrig (!) sett en payback-kalkyl i samband med svar på en offertförfrågan. Inte en enda av de tillverkare och leverantörer till de bolag jag jobbat i och som köpt CCTV-anläggningar, har en enda gång kunnat tala om bevisat positiva effekter eller ens kunna visat upp den enklaste payback-kalkyl.

När jag år 2001 började som säkerhetsassistent i Pressbyrån och 7/Eleven så fick jag bland annat som ansvar att motverka det ökade antalet rån som företagets butiker utsattes för. Under år 2003 blev sammanlagt 49 Pressbyråbutiker utsatta för någon form av rån. Sammanlagt ca 100 st anställda och kunder som alla allvarligt kränktes och fick med sig ett negativt minne för resten av sitt liv. En person som blivit utsatt för ett rån glömmer aldrig händelsen. Där någonstans läggs nivån i hur viktigt det är att förebygga bort just rån.

Branschen delar in rån mot butik i huvudsak efter tre brottstyper, motvärnsrån (våld i samband med snatteri eller stöld, räknas inte in i statistiken eftersom syftet oftast varit att stjäla, inte genomföra ett rån), kassarån och kontorsrån. Kassarånen är ofta snabbt genomförda och sträcker sig till att gärningsmannen vill åt pengarna i kassalådan. Oftast är kassarånet över inom ett par minuter. Kontorsrånet däremot är riktat mot butikens lager och det där ståendes värdeskåpet eller motsvarande. Kontorsrånet har som syfte att komma åt större summor pengar, det tar i allmänhet längre tid än kassarånet och har oftare inslag av våld eller allvarligt hot om våld.

Bild 2. *En entrédörr någonstans i Sverige.*

Av de 49 rån som vi utsattes för 2003 var 20 st kontorsrån som vi ganska snabbt kunde stoppa genom att byta ut värdeskåpen till deponeringsskåp som personalen inte kunde öppna.

Att förebygga kassarånen skulle visa sig väldigt mycket mer komplicerat. Vi provade under början av 2000-talet alla möjliga sätt för att motverka kassarån men efter att ha jobbat med problemet i ca tre år insåg vi att det egentligen bara finns två saker man skall rikta in sig på för att nå en verkligt förebyggande effekt:

1. Ta bort eller kraftigt reducera tillgången till det rånaren vill ha, i fallet Pressbyrån kontanter.
2. Öka risken att åka fast.

Att reducera tillgången är en komplicerad sak att lösa och här har olika företag valt olika lösningar exempelvis kraftigare skalskydd, ändrade rutiner eller införande av viss teknik (slutna kontanthanteringssystem). De företag jag arbetat för valde främst att lägga kraft på teknik och då mot slutna kontanthanteringssystem. Den tekniken var dock år 2003 inte fullt utvecklad och de system som fanns hade många initiala problem, förenade med stor kostnad och var komplicerade att montera och integrera in i företagets system.

Det som år 2003, utifrån verkligt rånförebyggande värde, stod till buds var främst CCTV . Nedan bifogar jag en riskanalys kopplat till en större rånanalys som jag och en kollega genomförde i slutet av 2003 (figur 1). Inventeringen hade som syfte att visa för företagets ledning och beslutsfattare att:

1. CCTV installationerna fyller en bevisat brottsförebyggande funktion, minskar antalet rån och ökar därmed tryggheten för anställda och personal.
2. Därmed är investeringar på CCTV system ekonomiskt försvarbara.

Förutom att vi arbetade med att få beslut om investeringar arbetade vi givetvis vidare operativt och strategiskt. Två saker vi gjorde, kopplade till vårt ökade antal moderna CCTV-system i butik, var att förbättra vårt samarbete med polis och med tv-programmet Efterlyst. Kontakterna med polis och Efterlyst hade som ett och enda syfte att öka antalet uppklarade rån och på så sätt signalera:

1. Till presumtiva rånare att Pressbyrån har bra CCTV-teknik och ett effektivt samarbete med polis och media.
2. Att visa för medarbetare att företaget tar ansvar för sin personal och agerar.
3. Att öka tryggheten för personal och kunder genom att fler rån blir uppklarade. Varje dömd rånare ger en viss upprättelse för rånarens brottsoffer.

Riskanalys Rån AB Svenska Pressbyrån
Kamerasystem

Hittills i år har vi haft 39 rån riktade mot våra butiker i landet. 18 av dessa rån var kassarån eller försök till kassarån. Av dessa 18 butiker saknade 14 kamerasystem.

Endast fyra gärningsmän var maskerade, och det var de i de butiker som har kamerasystem. Den övervägande delen av våra kassarån har alltså förövats mot butiker som saknar kamerasystem. Då skall man också lägga in faktum att de butiker vi idag har kamera i är de som rånats under de senaste två åren i huvudsak. Dessa butiker är procentuellt mer riskutsatta än andra butiker, dvs har man blivit rånad en gång så ökar risken markant att bli rånad igen inom en treårs period (se BRÅ;s rapport BUTIKSRÅN 2002:16).

De individer som genomför våra kassarån väljer alltså tydligt butiker som saknar kamerasystem, liksom att man undviker butiker som har.

Kriminellas egna uppgifter samt vår egen kunskap om denna typ av rånare visar på följande intressanta punkter i deras planerande;

Nybörjaren:
- Risken att åka dit
- Rädsla, stress
- Avskräcks av hinder, tex teknik, tidslås, kameror
- Planerar lite

Detta stämmer enligt min uppfattning mycket väl in på de rånare som idag genomför kassarån mot våra butiker.

I den lista som bifogas har vi med rött listat de butiker som vi anser har en ökad rånrisk sett till den utredning vi lämnat tidigare. Jag är övertygad om att vi kan halvera antalet kassarån genom att sätta ut kamerasystem i butikerna.

Mitt förslag är därför att vi köper in minst fyrtio kamerasystem i en upphandling och placerar ut dessa enligt lista. De återstående systemen kan sättas ut i butiker som antingen blir rånade alternativt har en högre risk än andra, tex i Göteborgs utkanter.

Säkerhetsavdelningen

Petrus Bolin

Stockholm 2003-11-05

Figur 1. Riskanalys

De förslag som kom fram genom riskanalysen ledde till att företagsledningen tog ett antal investeringsbeslut. Resultatet lät inte vänta på sig. Rånen halverades på två år.

Förutom det minskade mänskliga lidandet som varje rån medför så innebar halveringen av antalet rån en stor ekonomisk besparing för företaget. Den beräknade kostnaden för ett rån i Pressbyrån uppskattades år 2003 till ca 200tkr. Till det skall samhällets kostnader läggas till, Polisutryckning, utredning, eventuell sjukvård, mm.

Pressbyråns kostnader utgjordes av:

- Bevakningskostnader
- Ersättning karensdagar
- Stängd butik, Polisbeslut
- Minskad försäljning i ca 1,5 vecka pga mindre aktivitet i butiken, minskad personlig försäljning samt att vissa kunder drar sig för att återkomma.
- Arbete utfört av centrala avdelningar för att stötta butiken efter händelsen
- Komma in i jobbet, dubbelbemanning
- Krishantering

Bild 3. *En Coop-butik i Stockholm utsatt för rån.*

Ytterligare en effekt som CCTV-anläggningarna medförde var den ökade uppklarningsprocenten efter att ett rån genomförts. Under mina ca femton år som säkerhetschef har programmet Efterlyst löst ca 15 rån åt de bolag jag arbetat för. Flera av dem grova serierån. Ytterligare ett stort antal rån har lösts av polisen själva tack vare de bilder och filmer som vi kunnat ge dem efter utfört brott.

En intressant detalj var den diskussion som fördes internt i Pressbyrån kring att samarbeta med Efterlyst. Någon ansåg att vi inte skulle visa upp i TV att vi utsattes för rån samt hur de gick till. Min uppfattning då, var att jag var övertygad om att vårt samarbete med Efterlyst skulle visa sig vara positivt och förebyggande, inte tvärtom. Resultatet av samarbetet blev bättre än jag trott. Nästan samtliga ärenden som visades i Efterlyst löstes tack vare tittarna och genomslaget blev enormt positivt.

Sammanfattningsvis kan man säga att de CCTV-system som Pressbyrån investerade i dels förebyggde rån och dels hjälpte till att rånarna greps och dömdes. Vilket i sin tur är förebyggande.

Övriga effekter av CCTV installation i butik

Butiker drabbas inte bara av rån, ett annat stort problem är stölder och snatteri. Det svinn som stöld och snatteri står för kan vara väldigt påfrestande för många butiker eftersom det direkt påverkar butikens ekonomiska resultat. En annan negativ effekt som snatteri och stölder har är att de skapar en nervositet och obehagskänsla hos personalen vilket direkt påverkar arbetsmiljön. Därför var det för oss på Pressbyråns säkerhetsavdelning viktigt att även försöka, så gott det gick, arbeta mot ett minskat stöldsvinn.

Eftersom det inte gick att få fram ekonomiska uträkningar från leverantörerna fick vi undersöka det själva. Det första testet genomfördes på en Pressbyråbutik i Mälardalen. Butiken låg vid en järnvägsstation och hade stort flöde av kunder vid vissa givna tider, framför allt morgon och sen eftermiddag. Kunderna bestod mestadels av pendlare till och från deras arbetsplatser. Det stora flödet av kunder under ett fåtal avgränsade timmar möjliggjorde för presumtiva tjuvar att med liten eller ingen risk för att åka fast stjäla det de inte ville betala för. Särskilt stort svinn hade butiken på dyra tidningar och pocketböcker. Vi valde då att installera ett CCTV-system i syfte att minska stöldsvinnet i butiken. Arbetshypotesen var att rädslan att åka dit skulle få ett stort antal presumtiva tjuvar, normalt sett vanliga arbetande medborgare, att avstå när de insåg att butiken installerat CCTV.

Installationskostnaden var på ca 40tkr och svinnet varje kvartal låg på ca 30tkr, mestadels på press.

Efter sex månader så utvärderade vi projektet. Vi kunde då konstatera att svinnet sjunkit per kvartal till 10tkr, en minskning med 20tkr/kvartal. Det innebar att systemet, via minskat stöldsvinn, betalat sig själv på 6 månader!

En sak som vi lärde oss var att det är oerhört viktigt att tydligt kommunicera att en butik har CCTV. Förutom lagstadgade klistermärken som informerar om att en butik har CCTV valde vi att sätta upp en monitor i taket vid kundentrén där kunden ser sig själv i bild när han kommer in. Den signaleffekten skall inte underskattas.

En annan sak som är av intresse är ju vad kunderna anser om CCTV-bevakning i butiker eller på kontor. På femton år har jag endast nåtts av en negativ åsikt från en kund. En på femton år! Den kunden hade blivit bestulen inne i en Konsumbutik av en ficktjuv. Kunden kunde, efter att ha upptäckt stölden, konstatera att butiken hade en kamera riktad mot den plats där stölden skett.

Det visade sig dock när kunden kontaktade butikschefen att olyckligtvis just den kameran var ur funktion. Då ringde sagda kund till mig och skällde ut mig för att vi inte hade fungerande kameror. Så kan verkligheten också se ut.

En virtuell kompis

Pressbyrå- och 7/Elevenbutikerna drabbades inte bara av rån utan också att situationer där de blev utsatta för hot eller våld. Butikerna har ofta city och/eller transportlägen med långa öppettider där alla typer av människor är kunder. Det innebär att det då och då kommer in personer i butikerna som inte har ärliga avsikter eller av olika anledningar är aggressiva och hotfulla. På en del platser kan man öka säkerheten med så kallade bevakningsringar, ett antal butiker går ihop och betalar för en väktartjänst som kan tillkallas vid behov. På de flesta platser finns inte den möjligheten eftersom underlaget för tjänsten är för litet, dessutom är det över tid en relativt dyr lösning och inte alltid helt effektiv. På platser där Pressbyrån hade problem med ordningsstörningar, hot och våld, sökte vi andra, mer långsiktiga, lösningar.

Ett problem för butikerna var hur man skulle kalla på hjälp, särskilt i när händelsen inte motiverade att trycka på överfallslarmet. En lösning mellan allt eller inget. Vad jag menar är att de sökte en lösning att kalla på hjälp, eller rättare sagt kalla på uppmärksamhet, om något var på väg att ske. Då kunde personalen antingen att ringa Polis eller väktare alternativt trycka på överfallslarmet. Att ringa kan vara svårt eller helt omöjligt i en stressad eller hotfull situation, särskilt om man arbetar ensam. Att trycka på överfallslarmet för en situation som skulle kunna bli hotfull kändes alltför drastisk och var inget vi kunde rekommendera. Istället var tanken att personalen skulle kunna trycka på en ”CCTV-knapp” och realtidsbild skulle visas på en monitor i en larmcentral. Vår personal visste då att någon annan person kunde se och höra vad som skedde i butiken och på så sätt se till att hjälp snabbt kunde komma på plats, om så behövdes.

Bild 4. *Ytterligare ett rån, denna gång Pressbyrån.*

I samband med att det arbetet påbörjats så blev vi kontaktade av en leverantör som saluförde en kamera med just den teknik vi då eftersökte. Utan att gå in på tekniska detaljer så fungerade kameran så att man satte upp den i butik med uppsikt över kassalinjen, bilder och ljud (medhörning) överfördes i realtid via ett telekomföretags försorg på ett säkert sätt till larmcentralen. Det låter enkelt, men det var en operation som tog flera månader att realisera. Dels var tekniken relativt ny, dels var marknaden (läs väktarbranschen) skeptisk till lösningen som de såg som en konkurrent till sina egna väktare. Vi menade istället att det var ett komplement som i sig skulle skapa arbetstillfällen till branschen.

Vi döpte projektet till ”En virtuell kompis”.

Efter mycket arbete lyckades vi få till ett test på tre butiker i Stockholmsområdet. Butikerna valdes ut för att de hade problem med regelbunden ordningstörning. En av butikerna låg lite avsides på centralstationen i Stockholm och hade problem med påverkade missbrukare som snattade i butiken och var aggressiva mot personalen. Vi fick mycket positiv feedback från butikerna som upplevde en ökad trygghet med det nya systemet. Jag besökte vid ett tillfälle ansvarig larmcentral och vi kopplade då upp oss mot just butiken på Centralstationen. Vid den tidpunkten var kameran uppkopplad konstant mot larmcentralen eftersom vi ännu inte fått tekniken med tryckknappar att fungera fullt ut. Medarbetaren som då arbetade i kassan visste att kameran var på men inte att vi tittade på bilderna just då. Efter att medarbetaren hjälpt en kund så vänder hon sig om och tittar mot kameran, ler och vinkar.

Efter besöket på larmcentralen åkte jag ut till butiken för att prata med den kvinnliga medarbetaren. Hon berättade att hon kände en ökad trygghet av att veta att om något var på väg att hända så kunde hon få hjälp och att det kändes tryggt att någon såg. Hon sa också att personalen i butiken upplevde det som att missbrukarna i området uppmärksammat den nya kameran med den utökade CCTV-skyltningen och därmed drog sig för att begå brott i butiken.

Syftet med installationen hade nått sitt huvudsyfte, att personalen skulle uppleva en ökad trygghet. En trygg personal agerar klokare i svåra situationer och på så sätt förebyggs våld och hotsituationer som annars kunnat gå över styr. Dessutom upplevde butikerna en faktiskt minskning av antalet hotfulla situationer, även om det var svårt att faktiskt mäta.

Jag har försökt att beskriva hur CCTV fungerar i verkligheten i detaljhandeln. Att jobba 24/7 i en 7/Eleven butik i Stockholms innerstad är något helt annat än att sitta på ett kontor framför en dator. Det är en verklighet där medarbetarna riskerar att utsättas för allvarliga brott under sin arbetstid. Butiksmedarbetarna förtjänar en så hög säkerhet och arbetsmiljö som det är möjligt att skapa.

Enligt min uppfattning är CCTV ett för handel och bank mycket viktigt brottsförebyggande hjälpmedel. Låt det fortsätta få vara det och prioritera brottsoffret, inte förövaren.

Säkerhetskultur och kollektiv acceptans - en säkerhetschefs betraktelse över hur samhället kan förhålla sig till kameraövervakning inför behovet av en ökad trygghet

Per Gustafson

En ledstjärna som jag arbetat med för att ur ett retoriskt perspektiv kunna övertyga min omgivning gällande säkerhetsrelaterade åtgärder, är att ”den enskilde måste ge avkall på sin personliga integritet i förhållande till kollektivets säkerhet”. Ett sådant förhållningssätt skulle kunna kallas säkerhetskultur. En god samhällelig säkerhetskultur grundar sig på, enligt mig, en ömsesidig acceptans för vad som gemensamt måste uppnås för att erhålla en gemensam trygghets- och säkerhetsnivå. I den nya kameraövervakningslagen (2013:460) har lagstiftarna infört en möjlighet för detta, genom den så kallade överviktsprincipen (Datainspektionen). Överviktsprincipen innebär att kameraövervakning får ske om övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad, oavsett om allmänheten har tillträde dit eller inte (Datainspektionen). Jag vill här ge min personliga betraktelse på hur acceptansen kan uppnås genom ökad förståelse i förhållande till säkerhetsbehovet.

Tidigare tillståndsbedömningar enligt lag om allmän kameraövervakning

När ett tillstånd i enlighet med kraven i Lag (1998:150) om allmän kameraövervakning skulle beslutas, fick man ta hänsyn till vad som även omnämndes avseende integritet i personuppgiftslagen (1998:205). Bestämmelserna i lagen om allmän kameraövervakning och tillämpliga bestämmelser i personuppgiftslagen har nu sammanförts i en ny lag om kameraövervakning (Strandevall 2013). Vid en ansökan om tillstånd i slutet av 2011, för en kameraförsedd porttelefon, var kravet att endast ansiktet på den som stod utanför dörren skulle synas i bild och inget av den omgivande gatubilden. Nu hör det till saken att den trappavsats som besökaren skulle använda var näst intill omöjlig att stå på. Av den anledningen kom besökaren istället att befinna sig på trottoaren när porttelefonen aktiverades, varpå bildytan blev för stor och personer på andra sidan gatan kom att befinna sig i bild. Kravet från tillståndsgivaren blev då att linsen skulle maskeras (att rent funktionellt maskera en kameralins, som har en storlek likt en gammal tjugofemöring låter sig inte göras med bibehållen kvalitet). Därmed kom kravet på personlig integritet att ta överhanden från syftet med den kameraförsedda porttelefonen, nämligen att göra öppnandet av dörren tryggare. Min uppfattning är att de, som då eventuellt skulle befinna sig på andra sidan gatan vid de få tillfällen som porttelefonen aktiveras, inte skulle bry sig om varken om de var med på bild, sin integritet eller om det fanns tillstånd eller ej för denna installation.

Vid samma tillståndsprocess idag, när överviktsprincipen gäller, skulle tillståndshandläggarna förhoppningsvis se på saken med andra ögon och istället göra en mer pragmatisk bedömning över nyttan med porttelefonen och den eventuellt lilla påverkan av övervakning som installationen skulle ha för de förbipasserande. Om syftet hade varit att övervaka de förbipasserande, skulle en bättre effekt uppnås genom att helt enkelt ställa sig bakom en gardin i fönstret mot gatan och titta på dem som passerar. För detta ändamål krävs ingen faktisk utrustning och det är inget som hindrar att den som tittar ut på gatan rent av med en kamera i handen spelar in vad som försiggår utanför. Omständigheten att ingen kanske skulle bry sig, återfinns även i Brottsförebyggande rådets (Brå) rapport från 2003 om

kameraövervakning i brottsförebyggande syfte. Där påvisar Brå att det är mest accepterat med kameraövervakning på platser där vem som helst kan iaktta personen i vanliga fall, exempelvis i butiker och taxibilar samt på gator och torg. Vidare pekar rapporten på att en negativ konsekvens av kameraövervakning kan vara att den upplevs som ett intrång i den personliga integriteten. Trots detta, tycks emellertid majoriteten av allmänheten generellt sett inte ha något emot kameraövervakning i brottsförebyggande syfte (Brå 2003).

Kameror och dess eventuella bevisvärde

Sett i det tidigare integritetsfokuserade perspektivet fick kameror inte placeras hur som helst. De fick inte uppta större område än vad som var befogat för uppgiften. Trots detta har kameraplaceringar skett, där förbipasserande kan ha förekommit i bild under kortare och längre tid, och då även vid installationer där inspelning skett av materialet. Exempel på detta är kameror som sitter på varuhus, i butiker och har filmat ytor som är större än vad de egentligen är avsedda för (tidigare var dessa tillståndspliktiga, efter kameraövervakningslag (2013:460) gäller anmälningsplikt). Många gånger har det rört sig om kameror som på grund av felaktiga vinklar tittar ut över ett för sakens skull oväsentligt område, som kanske på grund av bristande kunskap om kamerans möjligheter gjort att de monterats fel. I de fall då dessa kameror kommer att dokumentera händelser som kan ha betydelse för en eventuell utredning, kan detta resultera i att innehavaren tvingas att montera ner sina kameror.

Om kamerorna inte hade suttit som de gjort från början, kanske utredningarna om händelserna inte kommit vidare, just beroende på avsaknaden på bevis. I det avseendet kan faktiskt intresset av övervakning väga tyngre än den enskildes intresse av att inte bli övervakad. Sett i ett preventivt syfte och som ett proaktivt förfarande kan detta ses som skäl nog för att övervakning ska få bedrivas trots att kamerorna varit felmonterade i lagens mening, något som numera är möjligt.

Tyvärr är det dock oftast så att bevisvärdet från felmonterade kameror mynnar ut i intet, då deras information och bildkvalitet inte ger något mervärde. Kraven på bildkvalitén är indelade i tre nivåer, händelseförlopp, typiska drag och identifiering (Bergström 2005). Detta kan bero på att kamerorna monterats i felaktiga vinklar (för hög placering, ger dålig översiktsbild) eller på placering med motljus från fönster och belysning (ger svarta siluetter av personer i bilden). Om aspekter som dessa inte tas med vid planering och uppsättning av kameror, spelar det inte någon roll hur bra kameror man sätter upp. Det är samspel och balans som måste råda vid kameraanvändning. Det finns vanligtvis två typer av kameraplacering, närbildskamera och översiktskamera. En närbildskamera ska placeras i normal ansiktshöjd. Tyvärr kan det bli så att vid placering av kameran i ansiktshöjd kan den komma att titta ut över ett allt för stort område där andra personer än den som kameran är avsedd för, kan synas i bild. Därför används översiktskameran som ett slags universallösning, oftast med en placering snett uppifrån och ner vilket inte är gynnsamt sett i ett identifieringsbehov. Med en mer frisinnad syn på användandet av säkerhets/trygghetskameror där bedömning enligt överviktsprincipen kommer in och med ett mindre fokus på den enskildes integritet, kan samhället få ut mer nytta av kameraanvändandet. Om personer som inte vet att de är filmade på grund av dessa till synes tekniska begränsningar kommer med på bild, så tror jag att de egentligen inte bryr sig om detta. Framförallt om de inte har något olagligt i görningen. Det hela handlar om tillit och förtroende. Tillit och förtroende för att den som är i besittning av bildmaterialet inte använder det till något annat än vad det är avsett för. På så sätt kan en kollektiv säkerhets- och trygghetsnivå uppnås med den utrustning som är befintlig. Här är även lagen tydlig med att

man använder teknik som främjar skyddet av den enskildes personliga integritet. När något har hänt kommer det alltid ”rop” på kameror. Dessa rop grundar sig på att det finns en bred uppfattning att kameror kan och ska lösa de problem som gäller trygghet/säkerhet och att dessa då ska till så fort som möjligt. Troligtvis kan det vara så att den bild som ges av filmindustrin och fiktionen hur kameror kan användas är orsaken till denna lösningsinsikt.

I filmer visas de mest optimala funktioner som kameror kan hantera och med hur forensiker gör de mest fantastiska utredningar av det inspelade materialet. Tyvärr kan informationen i verkligheten endast erhållas genom en från början riktig genomförd installation.

Kan det finnas en acceptans?

I en utvärdering av ett enkätmaterial, som bland annat syftade till att mäta acceptans för integritetskränkande teknik vid offentlig riskhantering med hjälp av tekniska säkerhetsåtgärder, kan man se en förhållandevis hög acceptans gällande användning av övervakningskameror (Sildemark 2011). I diskussionen tar författaren upp förhållandet att acceptansen för kameraövervakning ökar, när det sker saker i samhället som skulle kunna upptäckas eller rent av förhindras genom denna teknik. Dock reserverar sig författaren med att det behövs ytterligare studier innan några slutsatser kan dras från resultaten.

I en nyligen framlagd rapport (Brå 2014) om kameraövervakningen som infördes 2012 på Stureplan och Medborgarplatsen i Stockholm, kan Brå konstatera att både allmänheten och polisen har en positiv inställning till kameraövervakningen. Allmänhetens uppfattning, bland de som vistas på Medborgarplatsen och Stureplan, är att kamerorna leder till ökad trygghet trots att andelen personer som anger att de känner sig trygga inte har blivit större sedan den första undersökningen som gjordes 2012. Detta skulle kunna tyda på att det föreligger såväl en ökad förståelse som en ökad acceptans för användandet av kameror. Polisen å sin sida upplever att kamerorna underlättar deras arbete med att upptäcka och förhindra brott samt att utredningsarbetet förenklas. Kamerorna uppfyller således polisens behov av att få ytterligare hjälpmedel i sitt arbete.

Brås utvärdering ger emellertid inget stöd för att kameraövervakningen har haft någon effekt på vare sig brottsligheten eller tryggheten på de två platserna (Brå 2014). Detta kan tyda på att användningen av kamerorna ger en större tillfredställelse av behovet, samt en ökad såväl förståelse som acceptans, än på egennyttan av den faktiska användningen. Denna tillfredställelse för såväl allmänheten som hos polisen kan därmed utgöra grunden för en god säkerhetskultur.

Med anledning av den lilla effekt som kameraövervakningen har haft på brottsligheten, föreslår Brå (2014) en del förbättringsmöjligheter, bland annat mer information om kamerorna till besökare. Brå (2014) anser att potentiella gärningspersoner måste känna till övervakningskamerorna för att de ska fylla en avskräckande funktion. Ett trettiotal skyltar sattes upp på och kring Medborgarplatsen och Stureplan, och trots detta har de som vistas på platserna tydligen inte uppmärksammat dessa i önskad omfattning och därmed inte blivit medvetna om kamerornas existens. I vårt samhälle idag har vi en överexponering av information vilket kan förklara att de som befinner sig på Medborgarplatsen och Stureplan kanske selekterar informationen avseende sitt intresse till att vara där, istället för att ta till sig upplysningsskyltar om kameraövervakning. Här behövs det andra åtgärder enligt Brå (2014), såsom bättre kommunikation om att kamerorna finns på plats för ökad trygghet och säkerhet. Detta är något som påpekats tidigare i en rapport om kameraövervakning i brottsförebyggande

syfte (Brå 2003). I den rapporten angavs det att många och tydliga skyltar och även andra informationskanaler bör användas i samband med att åtgärden införs.

Skyltar, kameror och dess effekter för säkerhetskultur

Syftet med skyltning gällande kameraövervakning är att ge den som ska bege sig in i ett område med kameror ett val, ett val att acceptera intrång gällande den personliga integriteten eller ett val att kalkylera risken av att bli upptäckt och avslöjad vid planering eller utförande av brottslig handling. För den som sätter upp kameror handlar det om att spela med öppna kort att övervakning sker. Brå kunde konstatera (Brå 2003; Brå 2014) hur allmänheten inte uppfattar informationen och budskapet om kamerainstallationerna på det sätt som skyltning vanligtvis utförs. Min upplevelse är att det inte ligger i allmänhetens intresse att selektivt leta efter skyltar och annan information gällande kameraövervakning i första hand, utan att de istället mer omedvetet kan reflektera att den finns. Detta kan då vara förklaringen till låga medvetenheten av kameraförekomsten. Skyltar ger däremot den kriminelle en möjlighet att göra ett val i förhållande till det önskade utfallet.

Brås utvärdering (Brå 2014) visar att kameraövervakningen inte har haft någon effekt på brottsligheten vid Medborgarplatsen och Stureplan. Detta förhållande kan förklaras av den studie som Gill och Loveday (2003) genomförde. De intervjuade 77 fängslade personer i Storbritannien om hur de som kriminella upplever kameraövervakning. Sammantaget tyder mycket på att de flesta kriminella inte verkar se kameraövervakning som ett hot vid de enskilda brott de begår. Troligtvis kan detta förhållande bero på att den som har en kriminell avsikt kalkylerar med risken i förhållande till utfallet och konsekvensen av brottet. Kriminella vet hur de ska dölja sin identitet genom att bära en förklädnad och/eller genom att titta bort från kameran. Enligt Gill och Loveday var de flesta även av den uppfattningen att bildkvaliteten var dålig. Dessutom kände många av de intervjuade (och andra som begår brott övervakade av kameror), att de inte utför sina kriminella handlingar tillräckligt öppet samt att de även agerar för snabbt för att fångas på bild. Även det faktum att bilder kan användas senare (mestadels sker övervakningen i Storbritannien i realtid) för att identifiera och användas som bevis vid åtal sågs inte som ett stort bekymmer. Vissa kriminella påpekade att polisen saknar resurser för att följa upp eventuella bevis och att polisen inte prioriterar de brott som utförs för att finansiera droger (Gill och Loveday 2003).

Gill och Loveday drog slutsatsen att kameraövervakningen inte uppfattas som ett hot av de brottslingar som intervjuats. Upplevelsen av det hot som kameraövervakningen skulle innebära varierade med den hastighet som brottet utfördes med samt hur det begicks. Exempel på snabba brott är rån och handel med droger, som även kan ske i kamerornas döda vinklar utan att det kan observeras som pågående handling. En viktig aspekt som framkom var att respekten för kameraövervakningen står i förhållande till hur många poliser det finns, vilka snabbt kan göra ingripanden på det som upptäckts med hjälp av kameraövervakningen. Dock kunde Gill och Loveday se att de som tidigare hade åkt fast på grund av kameraövervakning var mer benägna att uppfatta det som ett hot mot deras gärningar, än de som inte åkt fast med hjälp av denna teknik.

Om kameraövervakning har en roll att spela i att förhindra och upptäcka brott samt att underlätta för utredning av brott så finns det mycket att vinna på att identifiera de erfarenheter som finns hos just de människor man riktar sig till, menar Gill och Loveday. Därför kan kanske intrång gällande den personliga integriteten bortses i den framtida diskussionen om

kameraövervakning, då inte ens kriminella ser detta som ett påtagligt hot, utan att det är en del av kalkylering av risken i förhållande till utfallet och konsekvensen av brottet. På samma sätt skulle allmänheten kunna förhålla sig till kameraövervakning, då gemene man inte har för avsikt att göra något som skulle innebära ett brott mot samhället. Därmed kan detta förhållningssätt bli ett slags säkerhetskultur i samhället och att den då kan delas av såväl kriminella som av övriga i samhället.

Hur ska en god säkerhetskultur uppnås?

Min upplevelse är att den allmänna uppfattningen om kamerors användning egentligen är mer frisinnat hållen än vad lagstiftarna har haft i tanke. Idag är det inte bara de fasta och tillståndspliktiga kamerorna som ska diskuteras i sammanhanget. Det finns även stora mängder handhållna högupplösta kameror i samhället (som inte faller under kameraövervakningslagen), exempelvis mobiltelefoner. Kameralagen omfattar inte dessa portabla kameror och därmed är det i princip fritt fram att filma var som helst, under förutsättning att det inte sker kränkande (regleras till exempel i brottsbalken (1962:700) angående kränkande fotografering). Men vad händer då om kameran förses med ett stativ, där kameran inte längre hålls under uppsikt, utan lämnas filmandes helt själv? Ja, här går troligtvis förhållandet över i att falla under kameraövervakningslagen. Detsamma gäller sannolikt även för hjälmkameror på motorcykelförare och skid- och snowboardåkare, då dessa inte hålls i handen. Kan definitionen för var gränsen går mellan filmning och kameraövervakning, beskrivas med hur kameran är monterad eller inte? Under hösten 2014 har Datainspektionen (Integritet i fokus, 3-2014) meddelat vad som gäller för radiostyrda, kameraförsedda leksaker samt den typ av kamera som kan monteras i fordon (detta gäller även en i vindrutan med sugkopp monterad mobiltelefon och med videoinspelning aktiverad). Här är svaret tydligt, det krävs tillstånd för dessa utrustningar, och rent av kan leksakerna bli förbjudna. Inom segmentet fordonsmonterade kameror räknas även den utrustning som används av en del trafikskolor för att i pedagogiskt syfte öka medvetandet om hur eleverna hanterar en trafiksituation. I Datainspektionens tolkning kräver denna typ av utrustning tillstånd.

Datainspektionen är den myndighet som har i uppdrag att göra dessa tolkningar, enligt kameraövervakningsförordning (2013:463). I och med tolkningen som Datainspektionen gör uppstår det ett motsägelsefullt förhållningssätt som inte helt enkelt låter sig svaras på. Kan en annan tolkning istället vara, så som jag försöker beskriva det i en värdemodell (fig. 1), att tolkningen istället ska baseras på hur syftet med användandet ska eller kan förhålla sig till acceptansnivån? Syftet får givetvis inte missbrukas och detta missbruk regleras således enligt gängse ordning, det vill säga enligt brottsbalken (1962:700) om kränkande fotografering. Modellen i figur 1 beskriver exempel på dessa förhållanden. Ett av exemplen är den tidigare diskuterade porttelefonen, som enligt modellen blir ett slags övervakning, men accepteras då syftet att ha kontroll på vem som släpps in har större acceptansnivå än den eventuella kränkning som förbipasserande kan utsättas för, o.s.v.

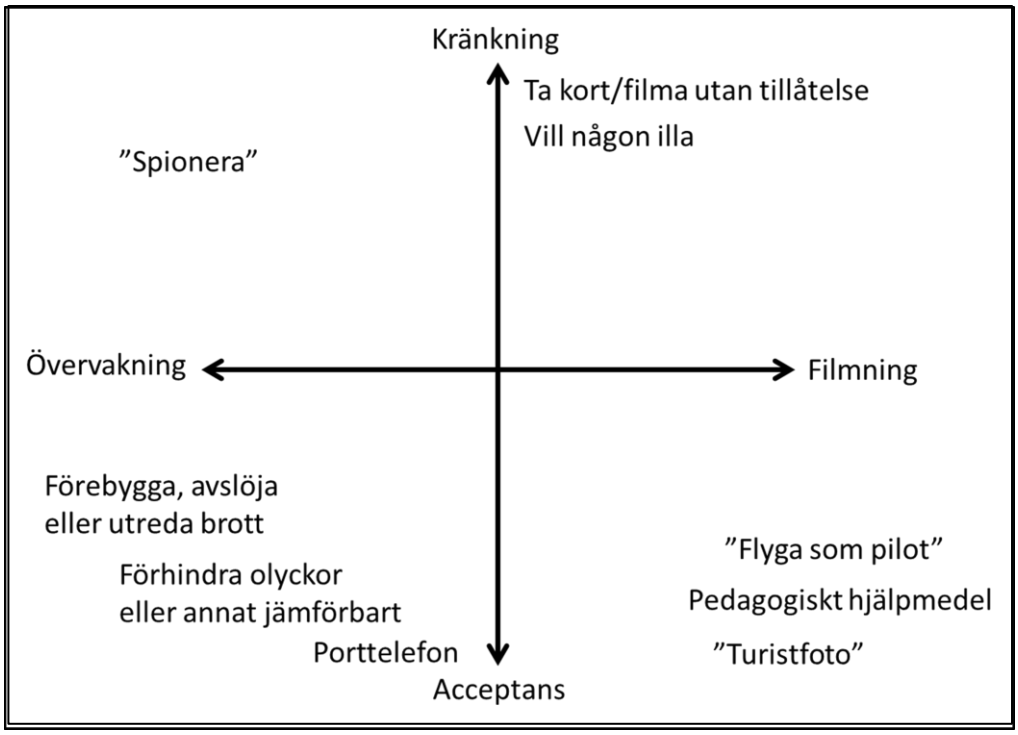


Fig 1: Värdemodell avseende syfte

Ska det vara förbjudet att uppleva känslan av att kunna flyga med modellflygplan, för att teknikutvecklingen gjort det möjligt att montera en kamera i farkosten? Kan ett turistfoto taget med stativ vara föremål för tillståndprövning? Vad har dessa miljontals kameror för inverkan på den personliga integriteten? Kan de rent av påverka rättssäkerheten? Kan de för olika yrkesgrupper rent av utgöra ett arbetsmiljöproblem? Bara för att man har tillgång till en kamera och att den kan användas så kanske det inte innebär att man alltid kan och ska få göra det? Ja, frågorna som kan ställas är många och ytterligare forskning behövs för att klargöra kollektivets ställningstagande inom motsatsförhållandena.

Här är det läge för att föra in begreppet säkerhetskultur igen. Säkerhetskultur (eller kanske säkerhetsklimat) inom organisationer avspeglar det uppfattade värdet av att agera säkert vilket bestäms av och ömsesidigt bekräftas av de anställda. Denna definition av förhållningsätt skulle även kunna appliceras inom samhällsstrukturen, genom att en gemensam uppfattning om vad som är det grundläggande behovet är och om förståelsen finns om hur detta ska uppnås. Därför kan begreppet säkerhetskultur/säkerhetsklimat även användas inom samhället, om det bygger på en ömsesidig överenskommelse gällande hur acceptansen ska uppnås i kollektivet. Alvesson (2002) beskriver detta som att kultur kan ses som att den formar individen, men även att individerna formar kulturen. Han belyser även svårigheten av att mäta kulturen. Kulturen enligt Alvesson förstås bäst som en sammankopplad och komplex uppsättning betydelser, värderingar och riktlinjer som de organisatoriska medlemmarna inte är fullt medvetna om. De kulturella aspekterna i ett samhälle består därmed mer generellt av hur medborgarna själva påverkar och påverkas av attityder, värderingar, förståelse och acceptans. För att skapa en god säkerhetskultur måste det därmed till en förståelse för säkerhetsbehovet där acceptansen kanske är den viktigaste beståndsdelen.

Hur ska en positiv acceptans uppnås?

Tyvärr när det gäller kameror används begreppet övervakning. Övervakning upplevs oftast som ett negativt laddat ord. Övervakning förknippas således med att ”någon” tittar över axeln på dig och att du då inte är betrodd för den du är eller vad du gör. Här kan det behövas en begreppsförändring för framtida hantering av sakfrågan. Kan begrepp som säkerhet eller trygghet användas istället för övervakning? Skulle ”över” istället bytas mot ”be”? I så fall kan syftet framhävas på ett mer positivt sätt och diskussionen gå mer mot en avdramatisering.

Kanske kan begreppen redas ut ytterligare och i samma stund även plocka fram ett nygammalt samlingsbegrepp för såväl säkerhet som trygghet, nämligen ”sekuritet”? Sekuritet är den svenska varianten av latinets Securitas, engelskans Security, franskans sécurité och likt svenskan hittas i en bortglömd variant gammaltyskans Sekurität. Säkerhet som begrepp används i olika sammanhang. Det finns det ingen distinktion mellan säkerhet, säkerhet, säkerhet, säkerhet och säkerhet, utan det är sammanhanget och förförståelsen som är avgörande. Genom att förtydliga och därmed införa ett nytt begrepp avseende säkerhet som avser skyddsverksamhet för samhället, medborgare och andra parter och som behövs för att motverka fara, skada, förlust eller brott, är det kanske dags för gammalsvenskans ”sekuritet”. Sekuritet är ett ord som tidigare fanns i svenska språket och som betyder just trygghet (SAOB 1967). Införandet av detta ord igen, innebär att distinktionen mellan *säkerhet* och *säkerhet* uppnås. Säkerhet kan då användas som engelskans *Safety* och sekuritet i betydelsen av *Security*. Därmed skapas en distinktion och definition om vad som menas med säkerhet och säkerhet vid varje enskilt tillfälle. Jag kommer fortsättningsvis i texten att använda sekuritet för att prova på lite hur ordet kan uppfattas.

En modell för sekuritetsacceptans

Grunden för en god sekuritetskultur angående kameraövervakning kan beskrivas i en modell och sägas bestå av tre samverkande delar, som tre linjer i ett koordinatsystem (*fig 2*). Sekuritetsbehovet är en pågående process vilken visas som en tidsaxel. Förståelse visas som en värdeaxel. Acceptansen blir därmed en produkt av sekuritetsbehovet och förståelsen. Ju mer kommunikation, mellan beskrivning av sekuritetsbehovet och uppnådd förståelse, desto mer acceptans. Brå (2014) konstaterade att informationen om kameror vid Medborgarplatsen och Stureplan behövde förstärkas gällande deras existens, vilket därmed även skulle kunna komma att öka acceptansen. Modellen för beskriver därför hur ett strategiskt systematiskt sekuritetsarbete ska borga för framgångsfaktorerna till en god sekuritetskultur och kollektiv acceptans.

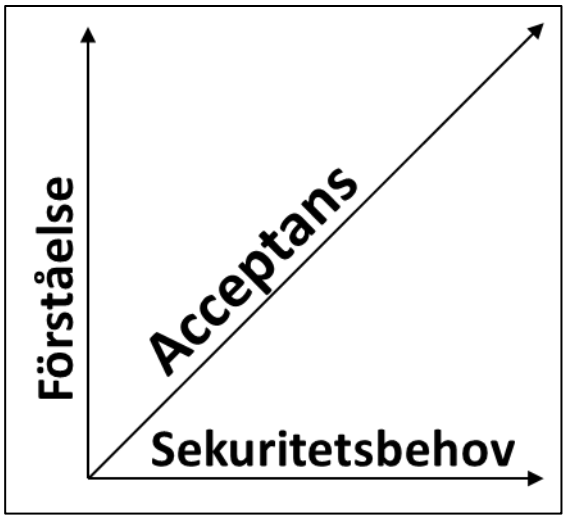


Fig 2: Modell för sekuritetsacceptans

En av framgångsfaktorerna när det gäller att skapa en god sekuritetskultur är att skapa ett slags positivism. Ett positivt klimat föder även en inställning till förändring. En definition av säkerhetskultur (*Safety Culture*) gällande förekomsten om olyckor, kan vara som Health and Safety Commission (HSC) uttrycker det 1993: "Säkerhetskulturen hos en organisation är produkten av individuella- och gruppvärderingar, attityder, uppfattningar, kompetens och beteendemönster som avgör engagemanget för, och stilen och färdighet för en organisations arbetsmiljöledning" (HSE 2005). Organisationer med en positiv säkerhetskultur präglas av kommunikation som bygger på ömsesidigt förtroende, genom delade uppfattningar om vikten av säkerhet och förtroende för effekten av förebyggande åtgärder gällande olyckor. Därmed kan detta sammanfattas med att om en positiv acceptans uppnås, kan samhället förhålla sig till kamerabevakning som en åtgärd inför behovet av en ökad trygghet och sekuritet. I och med detta ställningstagande kan skydd mot olyckor likaställas med den sekuritet som behövs för organisationen, anställda och andra parter genom att motverka fara, skada, förlust eller brott. Detta kan således sammanfattas som sekuritet för och i samhället.

Slutsats

Som säkerhetschef skulle jag vilja att den framtida utvecklingen går mot en ökad acceptans. Sammantaget ser jag att kamerornas betydelse fyller en funktion som en viktig del i det arbete som måste utföras gällande upplevd trygghet och i att förebygga, avslöja eller utreda brott. Samtidigt måste hänsyn tas till den enskildes integritet. Här spelar överviktsprincipen en viktig roll. För att få en större möjlighet att nyttja denna teknik måste en ökad acceptans uppnås. Detta kan åstadkommas genom en ökad förståelse om säkerhets- och trygghetsbehovet med användandet av en modell för sekuritetsacceptans. Ett annat förhållningssätt till användandet behöver införas, där syftet är avgörande. Vid missbruk av tillit och förtroende föreligger beivrande enligt gängse ordning. Genom att övergå från det mer negativa begreppet övervakning till det mer positiva trygghet, sätts fokus på integritet på ett annat sätt. Därmed kan den enskilde ge avkall på sin personliga integritet i förhållande till kollektivets sekuritet och därmed uppnås acceptansen.

Referenser

Alvesson, Mats (2002) Understanding organizational culture, London: SAGE.

Bergström, Peter (2005) Kameraövervakning – Testa ditt system innan brottslingen gör det!, Statens kriminaltekniska laboratorium – SKL, http://www.skl.police.se.

Brottsbalk (1962:700), http://www.riksdagen.se.

Brå (2003), Rapport 2003:11, Kameraövervakning i brottsförebyggande syfte, http://www.bra.se.

Brå (2014), Rapport 2014:12, Kameröverovakning på Stureplan och Medborgarplatsen, delrapport 2, http://www.bra.se.

Datainspektionen, Den nya kameraövervakningslagen, http://www.datainspektionen.se.

Datainspektionen (2014) Integritet i fokus, (3-2014), http://www.datainspektionen.se.

Gill, Martin & Loveday, Karryn (2003) What Do Offenders Think About CCTV?, Crime Prevention And Community Safety, vol 5, nr 3-1-1, ISSN: 1460-3780.

Health & Safety Executive (HSE) (2005) A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit, Research report 367, Prepared by Human Engineering for the Health and Safety Executive.

Kameraövervakningslag (2013:460) http://www.riksdagen.se.

Kameraövervakningsförordning (2013:463) http://www.riksdagen.se.

Lag (1998:150) om allmän kameraövervakning, http://www.riksdagen.se.

Personuppgiftslagen (1998:205) http://www.riksdagen.se.

Sildemark, Björn (2011) Perception och acceptans för integritetskränkande säkerhetsåtgärder, Brandteknik och Riskhantering, Lunds tekniska högskola, Lund: Lunds universitet.

Strandevall, Jan (2013) PM – En ny kameraövervakningslag, Observera - Konsult inom CCTV,http://www.observera.se

Svenska Akademien (1967) SAOB, spalt S1799, hämtad från http://g3.spraakdata.gu.se/saob/show.phtml?filenr=1/237/27.html.

Kameraövervakningens effekter – vad vet vi och vad vet vi inte?

Benjamin Weaver och Markus Lahtinen

Inledning

Intresset för att använda kameraövervakning ökar stadigt i Sverige såväl som i resten av världen. Videokameror blir ett allt vanligare inslag i offentliga miljöer som skolor, sjukhus, butiker och köpcentrum. Den teknologiska utvecklingen har gjort det möjligt att i större utsträckning installera övervakningskameror även på bussar, i tunnelbanan och i taxibilar. Kameraövervakning av allmänna platser som gator och torg har hittills varit ett sällsynt fenomen i Sverige, men på senare år har flera försök gjorts av både polisen och i kommunal regi.

I takt med att antalet övervakningskameror ökar är frågan om huruvida kameraövervakning är ett effektivt verktyg i kampen mot brottslighet ständigt aktuell. Frågan är särskilt viktig i samband med övervakning av allmänna platser, där den eventuella nyttan av kameraövervakning ställs mot den enskildes rätt att skyddas mot onödigt intrång i den personliga integriteten, den s.k. överviktsprincipen. Då integritetsaspekten väger tungt i svensk lagstiftning, krävs tillstånd för kameraövervakning av allmän plats. Dessa tillstånd beslutas av länsstyrelserna, som också bedömer under vilka villkor som kameraövervakning får ske och utövar tillsyn i efterhand.

Den 1 juli 2013 infördes en ny kameraövervakningslag (SOU 2013:460). Syftet med den nya lagen var att uppdatera och förtydliga regelverket och göra det enklare att använda videoövervakning i vissa typfall (bl.a. butiker och tunnelbana) utan krav om tillstånd. I samband med den nya lagen fick också Datainspektionen ett övergripande tillsynsansvar över tillämpningen av kameraövervakningslagen och har rätt att överklaga länsstyrelsernas beslut till högre instanser.

En vanlig uppfattning bland säkerhetschefer, installatörer av säkerhetsutrustning och konsulter som arbetar med kameraövervakning är att länsstyrelsernas tillståndsgivning är restriktiv och ofta hårt villkorad. Aktörer som söker tillstånd i flera regioner – t.ex. landsomfattande butikskedjor – rapporterar ofta att bedömningar och tillståndsgivning är väldigt olika mellan de olika länsstyrelserna i landet. I samband med att Datainspektionen fått utökade befogenheter i tillsynen av videoövervakning, överklagas i allt högre grad de tillstånd som redan getts av länsstyrelserna (Eriksson & Svensson 2014). I de fall som överklagats vidare, verkar förvaltningsrätten i de flesta fall gått på Datainspektionens linje. Trots att ett av syftena med den nya kameralagstiftningen var att göra tillståndsförfarandet enklare och tydligare, tycks det i många fall alltså ha blivit svårare att få tillstånd. Ett problem för både användare och branschen i stort är att tillstånd till inspelning av videomaterial kräver att ansökan visar att den övervakade platsen är ”särskilt brottsutsatt”. Ofta tillåts inspelning bara ske i samband med att incidenter inträffar, t.ex. då personalen aktiverar ett överfallslarm, och ibland ges inget tillstånd alls till inspelning. Då nästan inga kamerasystem idag säljs eller installeras i syfte att övervakas kontinuerligt i realtid, förtas mycket av den tänkta nyttan av att installera ett videoövervakningssystem under sådana villkor (Von Sivers 2014).

En övertro på kameraövervakningens effekter?

Politiker, lagstiftare och beslutfattare i tillstånds- och tillsynsmyndigheter ska alltså alla förhålla sig till den grundläggande frågan om – och på vilket sätt – eventuella nyttor eller önskvärda effekter av kameraövervakningen ska väga tyngre än allmänhetens integritetsintresse. Då man på förhand inte kan veta vilka effekter en installation av övervakningskameror kommer att ha, måste politiker och tjänstemän vända sig till vetenskapliga utvärderingar av tidigare försök på området. Det är rimligt att anta att inställningen till kameraövervakning bland dessa beslutsfattare starkt påverkas av det samlade resultatet och intrycket av dessa utvärderingar. Om kameraövervakning visat sig ge svaga påvisbara brottsförebyggande resultat i tidigare försök, borde integritetsintresset i de allra flesta fall väga betydligt starkare än om resultatet vore det motsatta. Utvärdering och forskning av övervakningens effekter spelar alltså en central – om än implicit – roll vid tillståndsgivning och användande av kameraövervakning i Sverige idag.

Då allmän kameraövervakning i större omfattning hittills har varit sällsynt i Sverige är de vetenskapligt dokumenterade erfarenheterna begränsade till ett fåtal fallstudier utförda av Brottsförebyggande rådet (BRÅ). I samband med förarbetet inför den nya kameraövervakningslagen beställde BRÅ därför en metaanalys av internationell forskning på effekterna av videoövervakning (Welsh & Farrington 2007; 2009). Resultatet av denna forskningsgenomgång visar att effekten på brottsligheten var starkt kopplade till den kontext där kamerorna användes. Störst och tydligast effekt hade kameraövervakning av parkeringsplatser där tillgreppen minskade med mer än 50 %. Kameraövervakning av allmänna platser och bostadsområden visade däremot bara på en marginell brottsförebyggande effekt. Dessa tydliga skillnader förklaras med att typen av brott och förövarens beteende skiljer sig åt markant mellan de olika studerade miljöerna. Bilstölder på parkeringsplatser är oftast planerade brott, där potentiella förövare uppträder rationellt och därmed undviker övervakade och väl belysta parkeringsplatser där det finns en hög risk för upptäckt. Brottslighet i stadskärnor är oftast våldsbrott som sker i plötsligt affekt och under alkohol- eller drogpåverkan, där kameraövervakning oftast inte visat sig ha någon större avskräckande effekt.

De flesta bedömare torde vara överens om att dessa resultat inte är särskilt förvånande. Mot ljuset av de omfattande skattefinansierade investeringar som gjorts i framförallt Storbritannien kan det dock anses vara anmärkningsvärt att den samlade bilden av forskningen de senaste 30 åren visar att kameraövervakning inte har en märkbar brottsförebyggande effekt.

Stort mediegenomslag

Slutsatserna från BRÅs forskningsgenomgång 2007 fick stort genomslag i svensk media där resultatet sammanfattades med att kameraövervakning inte fungerar, förutom på parkeringsplatser (Brå-rapport dömer ut övervakning 2008; Andrén, 2009). I en senare utvärdering utförd av BRÅ (Lindahl 2009), av en för svenska förhållanden ovanligt stor kamerainstallation i Landskrona centrum, kunde samma resultat konstateras. Antalet våldsbrott ökade snarare än minskade, och övervakningen hade således inte haft någon brottsförebyggande effekt. Under 2012 bjöd Länsstyrelsen i Skåne län in den norska kriminologen Heidi Mork Lomell till ett seminarium på temat ”Den övervakande blicken –

trygghet eller fara” [67]. Återigen befästes de tidigare intrycken av forskningsresultaten, och media kunde till och med rapportera att övervakningen – förutom att vara verkningslös – även kan skada samhället genom att människor börjar ta mindre socialt ansvar när det gäller att ingripa mot eller rapportera brott (Strömkvist 2012; Silberstein 2013). Samma resultat har bekräftats i en BRÅ-utvärdering av kameraövervakning i polisens regi på Stureplan och Medborgarplatsen i Stockholm, där ingen tydlig minskning av anmälda brott ännu kunnat noteras (Kindgren och Marklund 2014).

I en replik till ett kritiskt inlägg författat av representanter från säkerhetsbranschen, sammanfattade Datainspektionens generaldirektor Kristina Svahn Starrsjö den inställning till kameraövervakning som myndigheterna tycks ha idag:

> *[Säkerhetsbranschen] tycks ha en övertro till övervakningskameror. Bara vi får fler övervakningskameror kommer stölder, skadegörelse och misshandel att minska, ja kanske helt försvinna, verkar resonemanget gå. Detta trots att forskningen inte stöder den tesen. (Svahn Starrsjö 2014)*

Mediegenomslaget för kameraövervakningens bristande effekter påverkar inte bara politiker och tillsynstjänstemän och den allmänna opinionen, utan uppmärksammas av alla typer av beslutsfattare med ansvar för säkerhetsinvesteringar, allt ifrån säkerhetschefer inom stora organisationer till småföretagare och enskilda butiksägare. Uppfattningen att videoövervakning inte fungerar har således kommit att bli en ofta upprepad ”sanning” som tycks bekräftad genom vetenskaplig forskning på området.

Forskning om kameraövervakning

Frågan om kameraövervakningens effekter spelar alltså en central roll när myndigheterna gör avvägningar mellan eventuell samhällsnytta och intrång i den personliga integriteten. Av detta skäl kan det vara relevant att mer i detalj syna denna forskning och förstå på vilka grunder den har utförts och vilka kontext som har undersökts.

Vetenskapliga studier av kameraövervakningens effekter utförs huvudsakligen av – eller på uppdrag av – statliga myndigheter som BRÅ i Sverige eller The Home Office i Storbritannien. Ungefär hälften av de 44 studierna som refereras i BRÅs stora metaanalys (Welsh och Farrington 2007) härrör från myndighetsrapporter, medan de övriga är publicerade i vetenskapliga tidskrifter eller motsvarande. De forskare som intresserar sig för empiriska studier av kameraövervakningens effekter på brottslighet är till övervägande del kriminologer, vars forskning publiceras i kriminologiska facktidskrifter. I stort sett alla sådana studier utgår från en och samma kvantitativa forskningsdesign: en jämförelse mellan brottsstatistik över tid, före och efter införande av videoövervakning för ett visst geografiskt avgränsat område. Efter statistiska korrigeringar för olika felkällor, t.ex. säsongsvariationer, och jämförelser med näraliggande kontrollområden utan kameraövervakning, erhålls ett resultat som är lätt att tolka och förstå.

Inom det tvärvetenskapliga ämnet övervakningsstudier (surveillance studies), som bl.a. samlar sociologer, rättssociologer, statsvetare och urbanforskare finns också ett stort intresse för kameraövervakning, huvudsakligen utifrån ett kritiskt perspektiv. Inom övervakningsstudier

[67] Heidi Mork Lomells anförande är i sin helhet publicerad på Youtube: http://youtu.be/ZgsH3VkePs8

finns dock väldigt få empiriska studier av kameraövervaknings effekter, med undantag för några enstaka etnografiska studier av bl.a. kameraoperatörer och deras arbete (Smith 2004).

En majoritet av de empiriska studierna av kameraövervakning härstammar från Storbritannien och i princip alla akademiska forskare som studerar kameraövervakning är verksamma vid brittiska eller nordamerikanska universitet. I tabellen nedan redovisas den geografiska spridningen av de 44 studierna som ingår i BRÅs forskningsgenomgång från 2007.

Land	**Allmän plats**	**Allmän-nytta**	**Kollektiv-trafik**	**Parkering**	**Övrigt**	**Totalt**
UK	17	7	3	6	3	37
USA, Kanada	3	2	1			6
Sverige, Norge	2					2
Totalt	22	9	4	6	3	44

Tabell 1: Den geografiska fördelningen av studierna i BRÅs metaanalys (Welsh och Farrington 2007)

Storbritannien är en unik kontext för allmän kameraövervakning

Nästan all forskning kring kameraövervakningens brottspreventiva effekter härstammar alltså från Storbritannien. Då man analyserar denna forskning måste man förstå att Storbritannien utgör ett världsunikt fall i fråga om kameraövervakning i allmänhet och i övervakning av offentliga platser i synnerhet. Kameraövervakning lanserades under tidigt 90-tal av John Majors konservativa regering som en metod för att öka den allmänna tryggheten samtidigt som man gjorde stora nedskärningar inom den offentliga sektorn, inklusive polisväsendet (Norris 1999; Norris, McCahill och Wood 2004; Webster 2004).

Fallet med den då 2-årige Jamie Bulger, som fördes bort från ett köpcentrum i Liverpool 1993 och sedermera hittades mördad, anses vara den händelse som innebar ett genombrott för kameraövervakning i Storbritannien (Norris 1999), Övervakningsbilderna som visade hur Bulger fördes bort var av mycket dålig kvalitet och hade inte något värde som bevismaterial, men de visade tydligt att förövarna var två andra barn. Polisen kunde direkt rikta in sina resurser på rätt spår och snabbt klara upp brottet. Fallet med Bulger fick den allmänna brittiska opinionen av tydligt ta ställning för kameraövervakning, vilket i kombination med en accelererande brottslighet, legitimerade den konservativa regeringens omfattande satsningar under de kommande åren.

De brittiska CCTV-programmen

Genom ett antal s.k. CCTV-program riktade till lokala myndigheter, spenderade den brittiska staten över 250 miljoner pund på kameraövervakning av allmänna platser under perioden 1992-2002 (McCahill och Norris 2002). De efterföljande tio åren kan den totala summan för skattefinansierad allmän kameraövervakning ha ökat till närmare 500 miljoner pund (Norris 2010). Den brittiska regeringens kamerasatsningar blev snabbt populära bland lokala politiker och representanter för näringsliv och handel då de sågs som ett sätt att öka tryggheten bland invånarna och göra stadskärnorna mer attraktiva. Förutom det riktade stödet för övervakning av lokala stadskärnor, gjordes också stora statliga investeringar i kameraövervakning av

sjukhus, skolor och kollektivtrafik. Under åren 1994-1997 motsvarade samtliga dessa investeringar i videoövervakning närmare 80 % av regeringens budget för brottsförebyggande åtgärder (McCahill och Norris 2003).

Maktskiftet till Labour under Tony Blair 1997 medförde i inga förändringar i viljan att investera kameraövervakning, då de konservativas tuffa linje mot brottslighet varit populär bland den brittiska allmänheten (McCahill och Norris 2003). Alltsedan attentaten i New York den 11 september 2001, har Storbritannien varit USAs närmaste allierade i kampen mot den globala terrorismen. Detta har gett kameraövervakningen en ny viktig roll som ett viktigt nationellt säkerhetsverktyg i kampen mot terrorismen (Webster 2009).

I samband med bombdåden i London 2005, då fyra attentatsmän slog till på olika platser mot Londons kollektivtrafik, spelade bildmaterial från övervakningskameror en stor roll i polisens arbete med att snabbt identifiera förövarna och kartlägga deras tillvägagångssätt. Även om kamerorna – precis som i fallet med Jamie Bulger – inte kunde förhindra attentaten, blev den bestående bilden som förmedlades i brittiska media att kameraövervakning var effektiv och därmed bidrog till en ökad känsla av trygghet (Kroener 2013).

Med tanke på de omfattande satsningarna under 1990-talet och det faktum att brittiska myndigheter fortsätter att spendera stora summor på kameraövervakning i ett uttalat brottsförebyggande syfte, är det inte svårt att förstå det stora behovet av utvärdering och forskning kring just de preventiva effekterna av kameraövervakning i Storbritannien. Efter att flertalet studier visat tveksamma effekter på brottsligheten, har kritiker bland annat pekat det omdömeslösa i att lansera sådana omfattande skattefinansierade investeringar i ny och oprövad teknologi utan att först noggrant utvärdera resultaten genom pilotförsök i mindre skala (Groombridge 2008). Efterhand har de brittiska myndigheterna tagit till sig av denna kritik, och bl.a. tagit initiativ till omfattande utvärderingar (framförallt Gill och Spriggs 2005) vilka i sin tur lade grunden till utvecklandet av en nationell strategi för kameraövervakning (Gerrard et al. 2007).

Storbritannien och analog videoteknologi

Ett annat unikt problem för Storbritannien är de stora investeringarna i analog videoteknologi. Då de statliga CCTV-programmen kom i form av en engångsfinansiering, passade många lokala politiker på att investera i stora avancerade och kostsamma system med hög andel rörliga PTZ-kameror (pan-tilt-zoom), övervakade från dygnet-runt bemannade kameracentraler. Efterhand har kostnaden för drift och underhåll för dessa installationer blivit en tung börda för de lokala myndigheterna, vilket bl.a. lett till att många system inte har uppgraderats sedan de installerades (Webster 2009; Smith 2012). De stora brittiska investeringarna gjordes huvudsakligen innan övergången till digitala teknologier såsom nätverksvideo och digital bildinspelning. I takt med att digitaliseringen av kameraövervakning tog fart i början av 2000-talet, blev de brittiska systemen snabbt omoderna och svårare att uppgradera.

En konsekvens av detta för forskningen är att nästan alla studier som idag refereras, är gjorda på analoga installationer, vilket innebär att de har betydligt lägre upplösning och inspelningskvalitet än dagens digitala system. I BRÅs stora forskningsgenomgång 2007 var närmare hälften av studierna gjorda före 2000, medan resten var gjorda mellan 2000-2005. Digital inspelning av analoga övervakningskameror lanserades brett i början av 2000-talet och hade i de flesta nyinstallationer ersatt inspelning på videokassett vid mitten av 2000-talet. Helt

digitala kameralösningar som möjliggör högre bildupplösning fick inte något större genomslag förrän mot slutet av 2000-talet.

Problemet med att använda den brittiska forskningen på kameraövervakning som mall

Övervakning av stadskärnor är ett specialfall

Efterhand som man i Storbritannien insåg behovet av utvärderingar av kameraövervakningen, fokuserade man naturligt nog på de installationer som finansierats med skattemedel i samband med CCTV-programmen. De flesta studierna är därför utförda på kamerainstallationer i stadskärnor, som utgjorde huvuddelen av den brittiska regeringens satsningar. Denna typ av kameraövervakningssystem har således kommit att bli själva sinnebilden av kameraövervakning i medierapporteringen i såväl Storbritannien som i Sverige och de flesta andra länder.

I själva verket är denna typ av installationer ett specialfall, även i Storbritannien. Enligt Big Brother Watch (2012) – en intresseorganisation som kontinuerligt utvärderar övervakningssamhället – har drygt 50 000 kameror avsedda för övervakning av allmänna platser, installerats av brittiska statliga och lokala myndigheter. Denna typ av installationer utgör alltså några enstaka procent av alla kameror i Storbritannien, där det totala antalet övervakningskameror uppskattas till mellan 2 och 6 miljoner (Barrett 2013). När det paneuropeiska forskningsprojektet Urbaneye (Hempel & Herman 2004) kartlade utbredningen av videoövervakning i sex europeiska länder, fann man i Storbritannien runt 500 system med 40 000 kameror i som bevakade allmänna platser. I resten av de undersökta länderna – Tyskland, Norge, Danmark, Österrike och Ungern – fann man uppskattningsvis färre än 1 000 sådana kameror. Vid tiden för denna undersökning fanns det bara enstaka installationer i de nordiska länderna, där Sverige varit särskilt återhållsamt (Gras 2004). De första två systemen i Sverige kom 2001, med tre kameror på Möllevångstorget i Malmö och fem kameror i Stadsparken i Helsingborg (Blixt 2003). Trots detta är det alltså resultaten från det unika specialfallet övervakning av stadskärnor i Storbritannien, som får stå som typexempel för nästan alla former av kameraövervakning i rapporteringen av forskningsresultaten.

De flesta kamerasystem som övervakar allmän plats är privata

Det är alltså de ”privata” kamerainstallationerna som ägs och drivs av företag och organisationer som utgör den stora massan av kameror som på något sätt bevakar allmänna platser. Kostnaden för dessa kamerasystem belastar inte skattebetalarna, men deras användning regleras av myndigheterna och eventuellt inspelat bildmaterial är tillgängligt för polisens utredningsarbete. Även om de flesta bedömare är ense om att de storskaliga brittiska CCTV-satsningarna på allmän kameraövervakning varit ogenomtänkta, vore det något naivt att tro att alla andra aktörer i Sverige och internationellt, lika ogenomtänkt investerar i kameraövervakningssystem utifrån en övertro på kameraövervakningens effekter. Säkerhetschefer och andra beslutsfattare ger ofta en helt annan bild av kameraövervakningens effekter, baserat på egna eller andras tidigare positiva erfarenheter. Förutom stadskärnor och parkeringsplatser – där kameraövervakning visat sig vara effektivt – har forskningen, med några få undantag, inte studerat några andra kontexter där övervakningskameror används. Det är troligt att många av de sammanhang där kameraövervakning upplevs vara effektiv, liknar situationen vid parkeringsplatser, där syftet är att skydda mot olika former av mer eller

mindre ”rationell” brottslighet, som t.ex. skadegörelse, inbrott och tillgrepp av egendom. Det faktum att ingen relevant forskning gjorts på t.ex. effekterna av kameraövervakning för butiker, köpcentrum, arenor eller skolor, innebär alltså att vi knappast kan säga att kameraövervakning inte fungerar brottspreventivt i dessa fall.

Få likheter mellan situationen Sverige och Storbritannien

Utifrån diskussionen ovan, torde stå klart att den historiska och politiska kontexten när det gäller kameraövervakning i Storbritannien är unik, och skiljer sig markant från situationen i Sverige och de flesta andra länder. Övervakning av allmänna platser i stadskärnor i polisens eller lokala myndigheters regi är ett sällsynt fenomen utanför Storbritannien. I Sverige tillåter myndigheterna normalt sådan övervakning bara under en försöksperiod, varefter effekterna utvärderas. Dessa utvärderingar – som hittills alltid utförts av BRÅ – representerar i stort sett hela den empiriska forskningen kring kameraövervakning som genomförts i Sverige.

Det har heller aldrig funnits en svensk nationell politisk strategi kring kameraövervakning i brottsförebyggande syfte, och än mindre några riktade skattefinansierade investeringsprogram av brittisk typ. I Sverige har initiativ till videoövervakning på allmän plats tagits på lokal nivå, av polisen eller kommunerna. Syftet har därför inte alltid varit lika entydigt inriktat på brottsprevention som i Storbritannien, utan det har också funnits inslag av att vilja öka tryggheten bland allmänheten på gator och torg (Paulson 2012) eller att använda kameraövervakning som ett av många samverkande verktyg i en bredare satsning mot brottslighet (Blixt 2003; Johansson, Kindgren och Marklund 2013).

Forskning saknas på effekterna på brottsuppklarning

Ur ett brittiskt perspektiv är det alltså logiskt att utvärdering och forskning kring kameraövervakning fokuserar på brottsförebyggande effekter, med tanke på att detta vara ett uttalat politiskt mål i Storbritannien, och de stora offentliga satsningar som genomfördes för att uppnå detta mål.

Det är dock viktigt poängtera att studier av brottsstatistik bara mäter *en* av flera potentiella effekter, eller ”nyttor” som kan uppnås med kameraövervakning. Utöver prevention, är ambitionen med de flesta kamerainstallationer att inspelat material skall kunna användas i polisens utredningsarbete, och i bästa fall vara av sådan kvalitet att det kan klara upp brott och i bästa fall användas som fällande bevis vid lagföring.

Erfarenheter från Storbritannien när det gäller brottsuppklaring

Bilder från övervakningskameror används dagligen som hjälp i polisens utredningsarbete i Storbritannien såväl som i Sverige, men det är svårt att exakt utvärdera hur mycket detta videomaterial i varje unikt fall bidrar till en uppklaring av brottet. I den nationella strategin för brittisk CCTV som utarbetades 2007 beklagade utredarna avsaknaden av forskning på uppklarning, men påpekade att det anekdotiska bevisläget talade för att kameraövervakning är en stor hjälp i polisens utredningsarbete:

> *Little formal research has been undertaken to establish the impact that CCTV has on the investigation of crime. Those examining the issue therefore have to rely on limited research and anecdotal evidence provided by operational police officers. Despite the lack of formal research*

> *evidence, there appears little doubt that the police service utilises CCTV images in the investigative process and has had considerable success in doing so. High profile cases have reinforced the investigative benefits of CCTV which not only assist police officers in the identification of offenders but also help to establish the nature, location and time of the crime. (Gerrard et al, 2007:24)*

Troligen är det svårigheten att definiera, mäta och kvantifiera, som gör att det inte finns några jämförande statistiska studier av denna typ av effekter. Att utreda dessa frågor kvalitativt är också betydligt mer resurskrävande än att räkna på brottsstatistik, då det krävs djupintervjuer med poliser och detaljerade granskningar av brottsutredningar. Ett annat skäl är troligen att det interna polisiära utredningsarbetet faller utanför den traditionella ramen för det akademiska kriminologiska ämnesområdet, vilket gör att det saknas både metodologi och relevanta forskningsfrågor.

En rapport av Owen, Keats och Gill (2006) är en av de få studier som gjorts med fokus på nyttan av brottsuppklaring snarare än statistisk brottsprevention. Denna utvärdering pekar på en rad tydliga utredningstekniska nyttor för polisen med kameraövervakning. Ett system med 36 kameror som övervakar stadskärnan i Milton Keynes, uppskattades medföra nära två miljoner pund per år i besparingar för polis och rättsväsende. Dessa härrörde framförallt från möjligheten att göra tidiga insatser och avbryta pågående brott, och från utredningsmässiga tidsbesparingar, inte minst då gärningsmän ofta erkänner direkt när de får se sig själv på video.

I sammanhanget bör man också påpeka att för den allmänna opinionen tycks uppklarningen av brott vara en minst lika viktig effekt av kameraövervakning som brottsprevention. I Storbritannien har en rad uppmärksammade fall – från Bulger-fallet fram till bombdåden 2005 och upploppen 2011 – lett till ett ökande folkligt stöd för kameraövervakning ('More support' for CCTV after riots, 2011). I samtliga dessa fall har uppklarning av brotten snarare än prevention stått i fokus. I Sverige har liknande uppmärksammade fall, som övervakningsbilderna från NK på Anna Linds mördare och filmsekvenserna på den s.k. tunnelbanerånaren troligtvis haft samma effekt.

Upploppen i London i augusti 2011 medförde enligt Londonpolisen ett tydligt genombrott i att i stor skala visa den utredningsmässiga nyttan med både privat och offentlig videoövervakning. Cirka 4 000 av de 5 000 gripanden som följde i spåren av upploppen kunde kopplas till material som genererats från någon form av kamerasystem (Mick Neville at ST13 Newcastle, 2013).

Brottsuppklaring och bristande rutiner och processer

Då det inte finns någon forskning som tittat på kameraövervakningens effekter på brottsuppklaring, brukar ett vanligt argument vara att peka på att brottsuppklaringen i London eller Storbritannien i sin helhet inte ökat trots de massiva CCTV-satsningar som gjorts (Norris 2012; Strömkvist 2012). Till detta finns ett antal orsaker som utreddes i samband med utvecklandet av det brittiska nationella strategidokumentet för CCTV (Gerrard 2007). Ett övergripande problem i Storbritannien har varit en nästan total brist på utbildning och standardiserade rutiner och processer inom polisen för införskaffande och granskning av inspelat videomaterial från olika källor. Ett annat problem har varit bildkvaliteten från de åldrande analoga systemen, som ofta inte kunnat användas för identifikation. Teknologiskiftet från VHS-kassetter till digital inspelning har också vållat problem, då tillverkarna av denna utrustning ofta använder sig av proprietära digitala inspelningsformat i syfte att låsa in sina

användare, vilket lett till problem och fördröjningar i samband med inhämtandet av videomaterial.

Mot bakgrund av bl.a. utredningsarbetet efter uppploppen 2011, tyder mycket på att många av dessa problem nu är nära att lösas. I enlighet med det nationella strategidokumentet för CCTV, är arbetet med utbildning, upprättandet av rutiner och processer och skapande av expertroller på god väg inom den brittiska polisen och rättskedjan (Micke Neville at ST13 Newcastle, 2013). Ytterligare ett teknologiskifte till helt digitala nätverksbaserade övervakningssystem har också underlättat för insamlandet av video och bilder, som nu snabbt kan överföras via Internet.

Erfarenhet av brottsuppklaring med hjälp av kameraövervakning i Sverige

När det gäller utredning med hjälp av bildmaterial från kameraövervakning har situationen i Sverige liknat den i Storbritannien. Bristande kunskaper om att kamerasystemen existerar, oklara rutiner och incitament och besvärliga filformat har lett till ett underutnyttjande av videomaterial inom polis och rättsapparat (Lindahl 2009; Wiklund 2010). Ett mer generellt problem är polisens begränsade resurser och prioriteringar. Många kamerasystem inom handeln fångar snatterier och småstölder med låga straffvärden, vilket gör att de inte utreds vidare av polisen trots att bildbevis av god kvalitet finns tillgängliga (Söderlund 2014).

Medan en nationell strategi för kameraövervakningsarbetet inom rättsapparaten inte upprättats i Sverige, finns det initiativ för att rationalisera arbetet med brottsutredning med hjälp av kamerabilder. Ett sådant är kameraprojektet Sydsamverkan (SOU 2009:87), ett samarbete mellan polisen i södra Sverige, Statens kriminaltekniska laboratorium (SKL), Länsstyrelsen och Svensk Handel som inleddes 2005. Inom ramen för detta projekt har alla tillgängliga kameror (25 000 vid projektets start) och kontaktuppgifter till innehavarna samlats i en sökbar databas som visar kamerornas position på en karta. Samtidigt skapades en särskild videogrupp inom Malmöpolisen, med ansvar för att samordna inhämtande och hantering av bildmaterial. Erfarenheterna från detta projekt, där ca 2 500 ärenden med bildmaterial hanteras varje år, har varit mycket positiva när det gäller brottsuppklaring:

> *I de fall där en misstänkt gärningsman förekommer på bilder identifieras denne i ungefär hälften av fallen. Vid de tillfällen då filmer har visats i TV-programmet Efterlyst har omkring 70 % av misstänkta gärningsmän identifierats. År 2006 lämnade polismyndigheten bilder på nio misstänkta rånare till Kvällsposten som publicerade bilderna. Samtliga misstänkta gärningsmän kunde sedan med hjälp av tips från allmänheten identifieras. (SOU 2009:87:74)*

Inför arbetet med en ny kameraövervakningslag tycks svenska beslutsfattare ha tagit intryck av dessa erfarenheter, och uppmärksammat vikten av att bredda synen på de eventuella samhällsnyttor kameraövervakning av allmän plats kan ha. Detta reflekteras i lagstiftningen genom att texten i kameraövervakningslagen som beskriver vilka nyttor som skall ställas mot intrånget i den enskildes integritet skall, utökats med uppklaring och avslöjande:

> ***1998:*** *Vid bedömningen av intresset av allmän kameraövervakning skall särskilt beaktas om övervakningen behövs för att förebygga brott, [förf. kursivering] förhindra olyckor eller därmed jämförliga ändamål. Lag (1998:150) om allmän kameraövervakning, 6 §.*
>
> ***2013:*** *Vid bedömningen av intresset av kameraövervakning ska det särskilt beaktas om övervakningen behövs för att förebygga, avslöja eller utreda brott, [förf. kursivering] förhindra olyckor eller andra därmed jämförliga ändamål. Kameraövervakningslag (2013:460), 9 §.*

De senaste utredningarna från BRÅ (Johansson et al. 2013, Kindgren och Marklund 2014) av kameraövervakning på Stureplan och Medborgarplatsen i Stockholm reflekterar denna ändring i lagtexten genom en breddning av utvärderingsmetoden, där större vikt läggs vid att utreda nyttan med kameraövervakningen i polisens utredningsarbete. Den preliminära utredning som BRÅ publicerat 2014, visar att av 600 anmälda brott under en period av nio månader, har video från systemen begärts in vid 81 tillfällen (Kindgren och Marklund, 2014). Detta videomaterial hade dock bara avgörande betydelse för en fällande dom i tre fall. Ett problem med denna utvärdering av brottsuppklaringen är att BRÅ fokuserar för snävt på några enkla nyckeltal som är lätta att mäta. Till skillnad mot Owen et al. (2006) finns ingen ansats till att uppskatta eventuella resurs- och tidsbesparingar för polis och rättsväsende, som kameraövervakningen kan ha medfört.

Integritetsaspekten vid kameraövervakning

Efter att ha diskuterat de eventuella nyttorna av kameraövervakning, kan det vara intressant att också titta närmare på den andra sidan av vågskålen, d.v.s. den personliga integriteten. Kritiken mot allmän kameraövervakning kommer huvudsakligen från två håll. Inom framförallt övervakningsstudier, där flertalet forskare har ett på förhand kritiskt förhållningssätt, ser man kameraövervakning som en del av en övergripande trend mot ett övervakningssamhälle, där staten i allt högre grad söker kontrollera och socialt sortera sina medborgare.

Det perspektiv som torde ligga närmare svenska lagstiftare och myndigheter, är det som lutar sig mot mer klassiska och liberalt normativa idéer kring fri- och rättigheter och vikten av ett helgat privatliv utan inblandning från staten. När individer rör sig på allmänna platser som gator och torg blir det svårare att definiera och avgränsa den enskildes privata sfär, och bedömningen av eventuella integritetsintrång blir alltid en avvägningsfråga.

Integritetsrisker vid kameraövervakning

Vilka är då de konkreta riskerna med kameraövervakning ur den enskilde individens perspektiv? Erfarenheterna från Storbritannien visar att det finns särskilda risker vid direkt liveövervakning av stadskärnor, då kameraoperatörer kan styras av sina egna fördomar och fokusera på individer som uppfyller vissa stereotypa kriterier, vilket kan bidra till en social sortering (Smith 2004). Denna typ av installationer är dock ytterst sällsynta i Sverige, där majoriteten av kamerainstallationer inte övervakas live, utan istället spelar in bilder som sedan kontrolleras i efterhand vid eventuella incidenter. Riskerna här ligger framförallt i felaktiga utpekanden vid brottsutredningar, vilket är särskilt allvarligt om bilder förs vidare till media. Sådana fall har förekommit, och har varit ett resultat av bristande rutiner hos polisen, snarare än felaktig hanteringen av själva kamerasystemen.

En annan farhåga, är s.k. ändamålsglidning, där kameraövervakning – när den väl är på plats – börjar användas till andra syften än brottsbekämpning, t.ex. att övervaka personal, eller på annat sätt samla information om enskildas förehavanden på ett otillbörligt sätt. Oron för ändamålsglidning brukar kopplas till införandet av nya avancerade digitala teknologier såsom ansiktsigenkänning som på ett dramatiskt sätt skulle underlätta identifiering och automatisk kartläggning av enskilda individer för olika syften (Norris 2003; Norris 2010).

Det finns dock inget som tyder på att risken för ändamålsglidning idag är särskilt stor i samband kameraövervakning. Teknologier som ansiktsigenkänning har fortfarande en mycket begränsad funktionalitet och har inte fått något praktiskt eller kommersiellt genomslag. De bilder som lagras i kameraövervakningssystem är därför ostrukturerad data som inte kan kopplas till någon viss person, och informationen skall under alla omständigheter raderas efter några månader. För att en person skall identifieras – och en risk för integritetsintrång skall föreligga – krävs alltså en okulär granskning av materialet i realtid. System för ansiktsigenkänning kommer säkerligen att förbättras avsevärt i framtiden, men användningen av sådana teknologier kan enkelt villkoras bort i samband med tillståndsgivning, på samma sätt som myndigheterna idag förbjuder kontinuerlig inspelning i många fall.

Skillnader mellan rättspraxis i Sverige och på EU-nivå

De svenska lagstiftarna, och framförallt tillsynsmyndigheterna – länsstyrelserna och Datainspektionen – lägger en särskild vikt vid inspelningen av materialet, då detta ofta villkoras bort i samband med tillståndsgivningen. Detta skapar problem för användarna, då inspelning ofta är ett av de tänkta huvudsyftena vid införskaffande av ett kamerasystem. Om ingen allvarlig incident inträffar, kan ett typiskt kamerasystem med inspelning vara i drift under flera års tid utan att bilderna som spelats in någonsin granskas (utom möjligen i samband med underhåll och systeminställningar). Det tycks alltså som att svenska lagstiftare och myndigheter lägger en stor vikt vid en risk för integritetsintrång som kan sägas vara *abstrakt* (Axberger 2009) i den meningen att den inte i praktiken existerar förrän någon granskar bilderna och eventuellt sprider dem vidare.

Svensk rättspraxis verkar här skilja sig mot den som utvecklats på europeisk nivå. Europadomstolen har i ett antal fall prövat om olika former av övervakning och spridning av material från sådana aktiviteter är förenligt med Europakonventionens artikel 8, som reglerar rätten till den enskildes skyddade privatliv, och även gäller som lag i Sverige. Ur de domar från Europadomstolen som specifikt behandlat kameraövervakning framkommer det tydligt att själva förekomsten av allmän kameraövervakning, inklusive lagring av bildmaterial, inte i sig strider mot artikel 8 i Europakonventionen (Gallagher 2004). Istället är det först vid en eventuell användning, och framförallt *spridning* av materialet, som en risk för integritetsintrång kan uppstå. Spridning av bilder tagna vid allmän kameraövervakning till media anser dock Europadomstolen vara en viktig del av det brottspreventiva syftet med sådana system, då det uppmärksammar allmänheten på förekomsten och effekterna av kameraövervakning och kan leda till uppklaring av brott (Gallagher 2004). Det bör därför, enligt Europadomstolen, finnas ett relativt stort utrymme för avvägning mellan nyttan av allmän kameraövervakning i brottspreventivt och brottsutredande syfte, och de eventuella riskerna för integritetsintrång för de enskilda, även vid spridning av övervakningsmaterial.

Kameraövervakningslagen och Ipred- och FRA-lagstiftningen

I svensk praxis uppstår alltså ett abstrakt, eller potentiellt, integritetsproblem redan när en installation av allmän kameraövervakning görs, medan det enligt EUs praxis först uppstår ett problem när bildmaterial från ett sådant system sprids till en vidare krets. Denna strikta svenska tolkning i samband med just kameraövervakning ter sig något märkligt när man betraktar senare års införande av bl.a. Ipred- och FRA-lagarna. Förre justitieombudsmannen Hans-Gunnar Axberger (2009) beskriver hur attityderna kring integritetsskyddet snabbt kan ändras till följd av en accelererande teknikutveckling. I samband med att både de fasta

telenäten och mobiltelefonin digitaliserades på 80- och 90-talet infördes initialt ett *lagringsförbud* för all trafikdata som inte direkt behövdes för fakturering och liknande. Detta förbud förbyttes alltså efter bara tiotal år till en *skyldighet* för tjänsteleverantörerna att lagra trafikdata, i syfte att underlätta för statens signalspaning och brottsbekämpande arbete. Axberger pekar på hur attitydförskjutning följer ett tydligt mönster i den svenska rättshistorien:

> *Den tekniska utvecklingen och med den ändrade attityder och beteendemönster i samhället synes således relativt snabbt och utan större gensagor kunna medföra kraftiga förskjutningar i det som vid varje enskilt tillfälle uppfattas som principiellt motiverade ställningstaganden. Exemplet visar på en återkommande mekanism. Först ett närmast instinktivt avståndstagande gentemot de risker som upplevs förenade med ny teknik. Sedan en förvånansvärt snabb omvärdering och anpassning, när den nya tekniken visat sig praktiskt användbar. Konkret nytta slår ut abstrakt risk, skulle man kunna säga. (Axberger 2009:479)*

I fallet allmän kameraövervakning tycks denna attitydförändring märkligt nog snarare gå åt andra hållet – en restriktivare hållning och en övervikt i bedömningarna till fördel för den abstrakta risken för integritetsintrång. Ett skäl kan vara att den ”konkreta” nyttan inte ännu ansetts bevisad av bl.a. forskningen kring kameraövervakningens effekter. Ett annat kan vara att de grupper bland allmänheten som eventuellt skulle dra nytta av kameraövervakning – t.ex. enskilda brottsoffer eller butiksägare som kan få upprättelse genom att brott löses och lagförs med hjälp av bildmaterial – helt enkelt inte är lika starka och inflytelserika som internationella upphovsrättsinnehavare och deras lobbyapparater.

Allmänhetens inställning till kameraövervakning

Ett sätt att indirekt mäta riskerna för integritetsintrång är att direkt fråga allmänheten vad den anser om kameraövervakning. Ett stort antal sådana studier har gjorts, både lokalt och nationellt såväl som för särskilda grupper, t.ex. skolelever (se t.ex. SOU 2009:87 för en sammanställning). I princip alla sådana studier utförda i Sverige visar på ett stort stöd bland allmänheten för användning av allmän kameraövervakning i brottsbekämpande syften. På samma sätt som man kunnat se i Storbritannien, verkar också opinionen för kameraövervakning öka över tiden (Blixt 2003). En bidragande faktor till en ökande acceptans är att kameraövervakning får allt mer utrymme i media, t.ex. i TV-program som Efterlyst och nyhetskanaler på Internet.

I en av de senaste studierna som utförts av TNS Sifo på uppdrag av branschorganisationen Säkerhet för Näringsliv och Samhälle (SNOS), säger sig 92 % vara positiva till allmän kameraövervakning och 93 % anser att den kan bidra till att brott klaras upp (Säkerhetskameror på offentliga platser är trygghetsskapande, 2014). En något mindre andel, 87 %, anser att kameraövervakning bidrar till att förebygga brott, medan 41 % känner sig tryggare på platser där det finns kameraövervakning.

En tvärvetenskaplig studie om tillit i det digitala samhället, utförd vid Pufendorfinstitutet vid Lunds universitet (Larsson och Runesson, 2014), visar att 20 % av de tillfrågade ansåg att kameraövervakning av allmän plats inkräktar på den personliga integriteten i hög grad, medan 59 % ansåg att den gjorde det i låg grad och 21 % var indifferenta. I samma studie svarar 37 % instämmande på frågan om det är bra att myndigheterna övervakar och kontrollerar Internet. Vid en tidigare undersökning om allmänhetens inställning till Ipred-lagen, ställde sig 48 % av de tillfrågade emot att upphovsrättsinnehavare skulle ha rätt att begära in personuppgifter från internetoperatörerna (Klart nej till ny fildelningslag, 2009).

Det verkar alltså som om allmänhetens uppfattning skiljer sig från myndigheternas, när det gäller avvägningen mellan den personliga integriteten och kameraövervakningens eventuella nyttor. Vid en jämförelse med de näraliggande Ipred- och FRA-lagarna, tycks det också som att allmänhetens åsikter kring upplevda integritetsintrång inte är ett särskilt relevant riktmärke för lagstiftare och myndigheter.

Slutsatser

Kameraövervakning av allmän plats är idag ett ofta debatterat ämne. Efter att en ny kameraövervakningslag infördes 2013, anser många bedömare att det blivit svårare att få tillstånd till allmän kameraövervakning, och framförallt till kontinuerlig inspelning av videomaterial. Vid tillståndsgivningen görs alltid en avvägning enligt den så kallade överviktsprincipen, som syftar till att balansera kameraövervakningens potentiella samhällsnyttor mot effekterna på den enskildes integritet. Enligt den praxis som används vid bedömningarna idag, utgör själva förekomsten av videoövervakning en (abstrakt) integritetskränkning, oavsett om videomaterialet används eller inte. Detta innebär att de potentiella nyttorna därför måste väga tungt i vågskålen för att tippa över balansen till förmån för ett kameratillstånd.

När myndigheterna utarbetar en praxis för uppskattningen av kameraövervakningens nyttor, är tidigare forskning på området ett mycket viktigt beslutsunderlag. En ofta upprepad slutsats från denna forskning är att kameraövervakning inte förebygger brott, vilket har kommit att ha blivit något av ett mantra för svenska tillståndsmyndigheter.

Vi har i det ovanstående försökt bidra till att nyansera bilden av vad forskningen kring kameraövervakningens effekter faktiskt visar och inte visar. Uppfattningen att kameraövervakning inte fungerar, baserar sig på en förenklad och selektiv rapportering av resultaten från en politiskt motiverad forskning från Storbritannien, som genom sina enorma statsfinansierade CCTV-satsningar de senaste 20 åren utgör en helt unik kontext. Forskningen är vidare nästan helt fokuserad på ett specialfall: allmän kameraövervakning av stadskärnor, där våldsbrott ofta begås under alkohol- eller drogpåverkan. Denna typ av installationer finns i varje stad och stadsdel i Storbritannien, där uppemot 50 000 kameror övervakar medborgarna när de rör sig på gator och torg. I Sverige finns bara ett fåtal sådana övervakningssystem installerade på försök i särskilt brottsutsatta miljöer i storstäderna.

En av de få andra typiska miljöer som beforskats är parkeringsplatser, där kameraövervakning visat sig ha en tydlig preventiv effekt. Ingen relevant forskning har gjorts på effekterna av kameraövervakning på sådana platser som idag är utgör den stora massa av kamerainstallationer som övervakar allmän plats, d.v.s. butiker, kontorshus, köpcentrum, arenor och skolor, vilket innebär att man bör vara försiktig med att påstå att kameraövervakning inte fungerar brottspreventivt i dessa miljöer.

Samtidigt saknas forskning nästan helt kring alla andra effekter av kameraövervakning än brottsprevention. Detta snäva fokus är ett arv från Storbritannien, där brottsprevention var ett uttalat politiskt mål med de skattefinansierade satsningarna på kameraövervakning. Dokumentation av brott som kan leda till brottsuppklaring, har alltid varit ett av huvudsyftena med kameraövervakning, och många undersökningar visat att det är denna samhällsnytta som allmänheten värderar högst. Trots avsaknaden av relevant forskning, finns det ändå studier

och anekdotisk evidens som visar hur kameraövervakning kan vara en mycket stor hjälp i polisens och rättsväsendets arbete, och kan leda till betydande resursbesparingar. Ett generellt problem är att polisens rutiner och processer i samband med hantering av bildmaterial, måste organiseras bättre. I de exempel där detta gjorts, har också resultaten på brottsuppklaringen varit mycket goda.

Vi har också jämfört den svenska rättspraxisen på området, med den som utvecklats på EU-nivå, där Europadomstolens vägledande domar visat att det är *spridandet* av bildmaterial från ett övervakningssystem, som utgör ett hot mot den personliga integriteten, snarare än kamerasystemet i sig. Svensk praxis utgår ifrån att en integritetskränkning automatiskt sker i den stund som en kamera installeras på en allmän plats, oavsett om någon granskar bildmaterialet eller inte. Denna strikta definition av den personliga integriteten är dock knappast skriven i sten, när man beaktar införandet av Ipred- och FRA-lagstiftningen där den personliga integriteten inte ansågs väga särskilt tungt i förhållande till upphovsrättsintresset.

Ny forskning behövs

Den nuvarande situationen, där man förlitar sig på den brittiska forskningen, innebär att politiker och myndigheter i hög grad gör avvägningar och baserar sina beslut på en felaktig grund. Ny och relevant forskning som utvärderar fler effekter av, och användningsområden för kameraövervakning i typiska svenska kontexter behövs därför. Sådan forskning bör vara tvärvetenskaplig, och inkludera fler forskningsansatser som ett komplement till de kvantitativa och statistiska metoder som idag dominerar.

Referenser

Andrén, S. (2009) Fler kameror minskar inte brotten, *Dagens Nyheter*, 22 september.

Alexandrie, L. (2014) "Säkerhetshål i lagstiftningen hotar svensk rättssäkerhet", *SecurityUser.com*, nr. 4, 8.

Axberger, H.-G. (2009) Integritetsskydd i perspektiv, *Svensk Juristtidning*, nr. 1, 468-480.

Barrett, D. (2013) One surveillance camera for every 11 people in Britain, says CCTV survey, *The Telegraph*, 10 juli, http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

Big Brother Watch (2012) The Price of Privacy: How local authorities spent £515m on CCTV in four years, A Big Brother Watch report, http://www.bigbrotherwatch.org.uk.

Blixt, M. (2003) *Kameraövervakning i brottsförebyggande syfte*. Stockholm: BRÅ.

Brå-rapport dömer ut övervakning (2008) *Svenska Dagbladet*, 15 januari, http://www.svd.se/nyheter/inrikes/bra-rapport-domer-ut-overvakning_773335.svd.

Doyle, A., Lippert, R. K., & Lyon, D. (2012) *Eyes Everywhere: The Global Growth of Camera Surveillance*, Oxon: Routledge.

En ny kameraövervakningslag: Betänkande av 2008 års kameraövervakningsutredning. (2009) SOU 2009:87.

Eriksson, Björn & Svensson, Leif (2014) "Det är obegripligt att Datainspektionen tillåts stoppa ett effektivt användande av övervakningskameror", *Sydsvenskan*, 9 september.

Gallagher, C. (2004) CCTV and human rights: The fish and the bicycle? An examination of Peck v. United Kingdom (2003) 36 EHRR 41, *Surveillance & Society*, 2 (2/3).

Gerrard, G., Parkins, G., Cunningham, I., Jones, W., Hill, S., & Douglas, S. (2007) *National CCTV Strategy*, London: Home Office.

Gill, M., & Spriggs, A. (2005) *Assessing the impact of CCTV. Home Office research study 292*, London: Home Office Press.

Gras, M. L. (2004) The legal regulation of CCTV in Europe, *Surveillance & Society*, 2 (2/3), 216-229.

Groombridge, N. (2008) Stars of CCTV? How the Home Office wasted millions–a radical 'Treasury/Audit Commission'view, *Surveillance and Society*, 5 (1), 73-80.

Johansson, H. S., Kindgren, J., & Marklund, F. (2013) *Kameraövervakning på Stureplan och Medborgarplatsen: Delrapport 1 – implementering och utgångsläge*, Stockholm: BRÅ.

Kameraövervakningslag (2013), SFS 2013:460.

Kindgren, J., & Marklund, F. (2014) *Kameraövervakning på Stureplan och Medborgarplatsen: Delrapport 2 (Rapport 2014:12)*, Stockholm: BRÅ.

Klart nej till ny fildelningslag (2009) *Svenska Dagbladet*, 17 mars. http://www.svd.se/nyheter/inrikes/klart-nej-till-ny-fildelningslag_2604781.svd.

Kroener, I. (2013) 'Caught on Camera': The media representation of video surveillance in relation to the 2005 London Underground bombings, *Surveillance & Society*, 11 (1/2), 121-133.

Lag (1998:150) om allmän kameraövervakning.

Larsson, S., & Runesson, P. (red.) (2014) DigiTrust: Tillit i det digitala: Tvärvetenskapliga perspektiv från ett forskningsprojekt, Pufendorfinstitutet, Lunds universitet.

Lindahl, E. (2009) *Kameraövervakning i Landskrona: En utvärdering*, Stockholm: BRÅ.

McCahill, M., & Norris, C. (2002) CCTV in Britain. Centre for Technology and Society, Urbaneye Working Paper nr. 3, Berlin: Technical University of Berlin.

McCahill, M., & Norris, C. (2003) Estimating the Extent, Sophistication and Legality of CCTV in London I M. Gill (red.) *CCTV*, Leicester: Perpetuity Press Ltd.

Mick Neville at ST13 Newcastle (2013) *Professional Security Magazine Online* http://www.professionalsecurity.co.uk/news/interviews/mick-neville-at-st13-newcastle/.

'More support' for CCTV after riots (2011) *The Independent*, 25 oktober, http://www.independent.co.uk/news/uk/crime/more-support-for-cctv-after-riots-2375768.html.

Norris, C., & Armstrong, G. (1999) *The maximum surveillance society: The rise of CCTV*, Oxford: Berg.

Norris, C., McCahill, M., & Wood, D. (2004) The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space, *Surveillance & Society*, 2 (2/3), 110-135.

Norris, C. (2003) From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control, i D. Lyon (red.), *Surveillance as social sorting: Privacy, risk, and digital discrimination*, London: Routledge.

Silberstein, M. (2013) "Effekten är nästan noll", *Arbetarbladet*, 23 juli, http://www.arbetarbladet.se/gastrikland/gavle/effekten-ar-nastan-noll.

Norris, C. (2010) Closed-Circuit Television: A Review of its Development and its Implications for Privacy i S. G. Shoham, P. Knepper, & M. Kett (red.), *International Handbook of Criminology*, CRC Press.

Norris, C. (2012) Reflections on the global growth of CCTV surveillance i A. Doyle, R. K. Lippert, & D. Lyon (red.), *Eyes Everywhere: The Global Growth of Camera Surveillance*, Oxon: Routledge.

Owen, K., Keats, G., & Gill, M. (2006) *A short evaluation of the (economic) benefits of the Milton Keynes CCTV System in managing police resources*, Leicester: Perpetuity Research Ltd.

Paulson, H. (2012) Stort stöd för säkerhetskameror bland Malmöbor, *SecurityUser* nr 1.

Smith, G. J. D. (2004) Behind the screens: Examining constructions of deviance and informal practices among CCTV control room operators in the UK, *Surveillance and Society*, 2 (2/3), 376-395.

Smith, G. (2012) On the moribundity of camera networks in the UK I A. Doyle, R. K. Lippert, & D. Lyon (red.), *Eyes Everywhere: The Global Growth of Camera Surveillance*, Oxon: Routledge.

Strömkvist, S. (2012) Kamerorna inte avskräckande, *Sydsvenskan*, 22 maj, http://www.sydsvenskan.se/sverige/kamerorna-inte-avskrackande/.

Säkerhetskameror på offentliga platser är trygghetsskapande (2014) *SecurityUser*, 29 april, http://www.securityuser.com/se/news_archive_.asp?newsType=1&newsid=6811&area=0&newsYear=2014&nav=1.

Söderlund, H. (2014) Polisen struntar i att utreda bensinstölder, *SecurityUser*, nr 4.

Svahn Starrsjö, Kristina (2014) Det finns en övertro på kameraövervakning, *Svenska Dagbladet*, 1 maj.

Von Sivers, Tom (2009) Hård kritik mot kameralagen och Datainspektionen på Trygghetskamerans dag, *SecurityUser*, nr 3.

Webster, W. R. (2004) The diffusion, regulation and governance of closed-circuit television in the UK, *Surveillance & Society*, 2 (2/3), 230-250.

Webster, W. (2009) CCTV policy in the UK, *Surveillance & Society*, 6 (1), 11.

Welsh, B. C., & Farrington, D. P. (2007) *Kameraövervakning och brottsprevention: En systematisk forskningsgenomgång*, Stockholm: BRÅ.

Welsh, B. C., & Farrington, D. P. (2009) *Making public places safer: Surveillance and crime prevention*, Oxford: Oxford University Press.

Wiklund, I. (2010) Fel filformat förstör för polisen, *SecurityUser*, 24 mars, http://www.securityuser.com/se/news.asp?newsid=2244.

Överviktsprincipen – vad är det? (2013) *Integritet i fokus*, nr. 3-4.

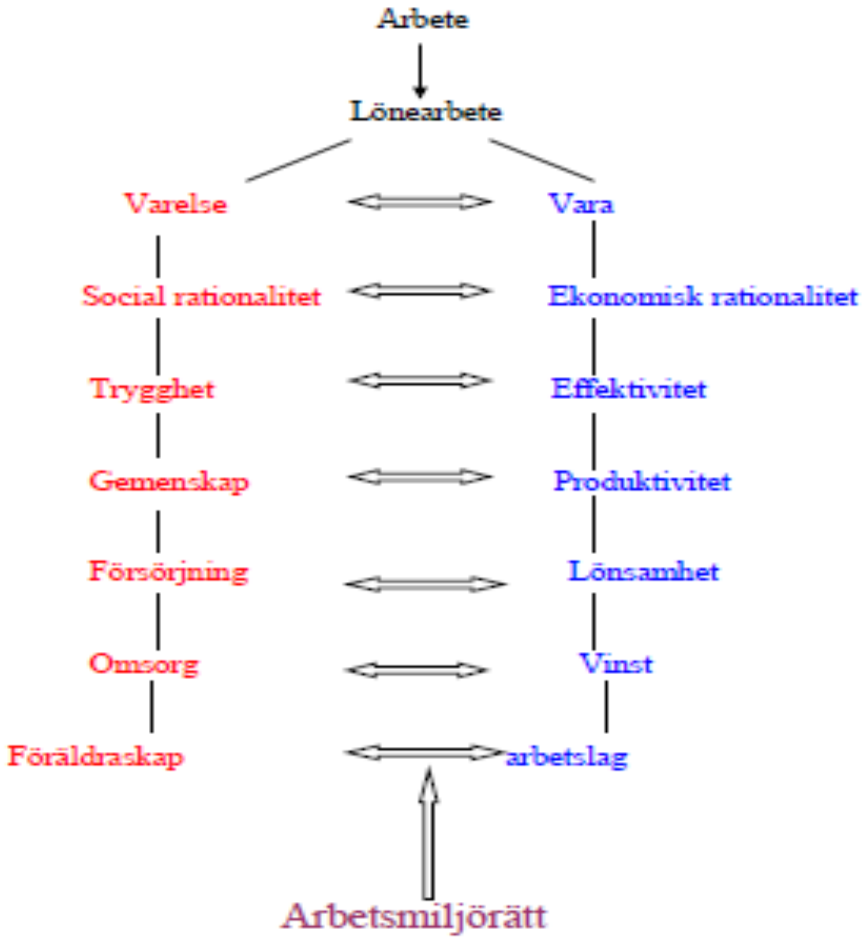
Måste vi ta det onda med det goda eller går det att välja? Om övervakning som samhällsproblem.

Håkan Hydén och Marcin de Kaminski

Övervakning är ett postmodernt problem med paralleller till t ex miljöförstöring, vilket börjar anta allt större proportioner. Det föreligger dock avgörande skillnader mellan dem. Miljöproblemen är en negativ extern effekt av något som vi bejakar och vill ha. Vi vill ha en materiell behovstillfredsställelse genom en effektiv industriproduktion. Men kopplat till detta får vi miljöproblem på köpet. De hänger samman. Men parallellen till övervakning är enbart skenbar. Övervakning har alltid funnits i en eller annan form (Foucalt 2003). Traditionellt har övervakning använts av polisen för att följa upp kriminella och av säkerhetspolisen för att följa personer som klassas som säkerhetsrisker. Med ny teknik har dock massövervakning möjliggjorts som inte bara övervakar redan utpekade personer utan mer eller mindre alla med syfta att hitta potentiella riskpersoner. De är inte nu längre bara storebror, staten, som ser dig utan idag kan även enskilda övervaka varandra (Hadley-Kamptz 2011). Stater som vill övervaka sina medborgare brukar hävda att övervakning minskar piratkopiering, våld, förtal, ekonomisk brottslighet, hatbrott och annan brottslighet. Övervakning som samhällsproblem hänger samman med den teknikutveckling som den digitala tekniken för med sig. Teknikutvecklingen ger upphov till olika möjligheter. Den kan användas för olika syften. I detta samhällsskede är samhällsproblemen mer en fråga om val av framtidsalternativ än kompromisser inom ramen för ett alternativ. Vi står här med övervakning som exempel inför ett kvalitativt nytt regleringsfenomen.

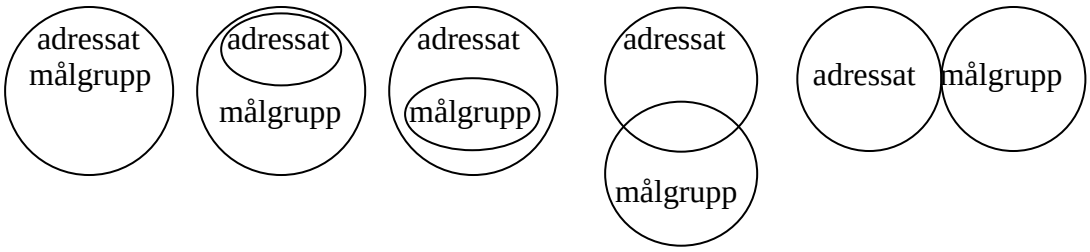
Det senmoderna samhällets regleringsproblem

Det finns paralleller mellan övervakning å ena sidan och sentida fenomen som anställnings- och arbetsmiljöskydd, konsumentskydd och miljöskydd å andra sidan. Under 1970-talet växte det fram lagstiftning till skydd mot exploatering av arbetstagare, konsumenter och allmänhet. Denna lagstiftning hade till funktion att balansera olika intressen, framförallt sociala och ekologiska intressen mot ekonomiska, där det sistnämnda alltid har haft ett outtalat tolkningsföreträde. De ekonomiska intressena har inte behövt något politiskt stöd förmedlat genom lagstiftning. Det har haft sin naturliga utvecklingskraft ändå. När industrisamhället emellertid nått sin kulmen börjar de negativa externa konsekvenserna av den ekonomiska modellen successivt bli alltmer påtagliga. Överexploatering riskerar att hämma ekonomins egen utveckling. Konsumtionen riskerar att minska om konsumenterna känner sig lurade. Det kräver rättsliga remedier mot de företag som missbrukar marknadsföring och kontraktsvillkor. På samma sätt hämmar överexploatering av arbetskraften produktionen. Lagstiftningens funktion blir att kompromissa mellan berörda intressen. Jämför följande figur:



Lagstiftning är således något som behövs för att stärka det intresse som är utsatt för exploatering av de ekonomiska normerna. Dessa i sin tur kräver inte något rättsligt stöd annat än i form av äganderättsliga och associationsrättsliga regler om innehav, organisation och liknande. Arbetsrätten kan ses som en intervenerande lagstiftning som kännetecknas av att den syftar just till att påverka en viss verksamhet i samhället (Hydén 2006). Denna lagstiftning har sin särskilda egenhet i det att den måste implementeras genom någon för ändamålet upprättad myndighet eller annan aktör. På arbetsrättens område spelar fackföreningar en stor roll när det gäller att bevaka arbetstagarnas rättigheter. I själva verket är det så i den svenska modellen att det är fackföreningarna som i stor utsträckning är bärare av dessa rättigheter. Men här finns också en särskild domstol, arbetsdomstolen, och myndigheter av typen Arbetsmiljöverket som har till uppgift att medverka till att upprätthålla arbetstagarnas intressen.

Den amerikanska sociologen och spelteoretikern James Coleman har infört en distinktion mellan normens adressater och de som drar nytta av normen, normens målgrupp (*targets* respektive *beneficiaries*). För de fall då dessa sammanfaller talar Coleman om gemensamma normer (*conjoint norms*) och då de är skilda åt för icke gemensamma normer (*disjoint norms*) (Coleman 1990). Däremellan räknar Coleman med ett antal mellan former i enlighet med följande figur :



a b c d e

Gemensamma normer ***Icke gemensamma normer***

Gemensamma normer föreligger då de intressen som gynnas genom normen och de som missgynnas berör samma aktörer eller aktörskategori. Var och en tillhör i dessa fall samtidigt både gruppen adressater och normens målgrupp. Icke-gemensamma normer är de normer som gynnar en grupp av aktörer, målgruppen, medan den missgynnar eller i vart fall riktar sig till en annan grupp i samhället, normens adressater. Normens adressater och dess målgrupp tillhör således olika aktörskategorier.

Coleman menar att man i sociala sammanhang lika lite som i ekonomiska kan tala om optimala lägen utan att beakta den existerande fördelningen av rättigheter och resurser. Om skillnaden är stor, dvs. om vissa gruppers intressen tillmäts mycket större betydelse än andra gruppers, finns det en möjlighet att den gruppen med mest makt kan framtvinga icke-gemensamma normer som styr handlandet hos den gruppen som saknar makt. Coleman framhåller att möjligheten att analysera dessa normer i termer av social optimalitet förutsätter att man tar den ojämlika fördelningen av makt för given. Denna typ av normer kräver oftast att tvång kan utövas över den svagare gruppen eller att den ojämna maktfördelningen är en del av den existerande samhällsstrukturen, såsom i extremfallet med gruppen slavar. De exempel Coleman nämner handlar om kvinnors ställning i olika samhällssystem.

Mellan de här två extremfallen av gemensamma och icke-gemensamma normer finns det olika blandformer som figuren visar. Behovet av en norm enligt Coleman uppkommer när en parvis relation eller annat handlande medför konsekvenser för andra än de närmast inblandade. I parvisa relationer antas i utgångsläget vardera parten ha tillgång till resurser som gör det möjligt att förhindra uppkomsten av negativa externa effekter på en själv. Så är inte situationen i en relation som innefattar tre och fler aktörer.

Gemensamma normer är sådana där lagens adressat och de som drar nytta av normen kan växla över tid. Om vi tar straffrätten som exempel så riktar den sig till oss alla med krav på att vi avhåller oss vissa handlingar, såsom våld, lurendrejeri, etc. samtidigt som vi alla också drar nytta av normerna i det att vi slipper bli utsatt för våld eller lurendrejeri. Samma sak gäller för civilrättens område. Regler om avtal, t ex att avtal ska hållas, är ett krav som gäller oss alla som slutit ett avtal, samtidigt som vi kan dra nytta av att känna den trygghet det innebär att vi kan lita på att avtal ska hållas. Det finns därför all anledning att i fråga om gemensamma normer räkna med en form av naturlig eller spontan efterlevnad av normerna. Det kan ändå behöva finnas rättsliga normer som slår fast ”den naturliga ordningen” av det skälet att man alltid får räkna med att det finns vissa i samhället som tar chansen att försöka skaffa sig fördelar eller av andra skäl bryter mot reglerna. Vi kallar dessa individer för avvikare, något

som är föremål för kriminologins intresse. Ser vi till icke-gemensamma normer kännetecknas dessa av att de riktar sig till en grupp i samhället, t ex rökare till gagn för en annan grupp, icke-rökare, som slipper att utsättas för passiv rökning och obehaglig lukt. I dessa fall kan vi inte räkna med att normerna upprätthålls spontant. De som normerna riktar sig mot har ju inget omedelbart eget intresse av att följa reglerna, tvärtom innebär det många gånger en belastning för dem. Samtidigt finns det en annan grupp i samhället, de vars intressen normerna avser att gynna eller skydda. Denna grupp kan i varierande grad göra sin röst hörd och utöva sociala, ekonomiska eller politiska påtryckningar för att reglerna ska tillämpas, något som studeras inom rättssociologin.

Intersystemkonflikter – dubbla normativa budskap

På arbetslivets område har vi just icke-gemensamma normer, regler som riktar sig mot arbetsgivarna till gagn för arbetstagarna. De sistnämnda har ansetts behöva skydd mot exploatering i olika sociala och ekonomiska hänseenden. Det har för det första tagit sig uttryck i olika rättigheter till skydd för ett kollektivt agerande. Vi talar här om förenings- och förhandlingsrätt, något som arbetstagarna tillskansade sig under första delen av 1900-talet. Dessa rättigheter har sedermera utvidgats genom införande av Medbestämmandelagen. Genom ett kollektivt uppträdande har arbetarrörelsen kunna utöva starkare fackliga och politiska påtryckningar mot motparten, arbetsgivarna. Så småningom ställdes krav på anställningsskydd, vilket infördes genom krav på saklig grund för uppsägning, något som kunde och kan underkastas rättslig prövning. Denna reglering framstår som tämligen långtgående krav på arbetsgivarna och tillika skydd för arbetstagarna. Regleringens ingrepp i arbetslivets maktförhållanden lindrades dock av att arbetsbrist alltid utgör saklig grund. Det innebär att ekonomiska och organisatoriska argument har företräde framför arbetstagarnas socialt färgade argument om rätten till arbete.

Ett annat område som tidigt fick sina skyddsregler är arbetsmiljöns område. Här infördes skyddsregler genom lag redan i slutet av 1800-talet något som successivt har byggts ut bl. a. genom att den särskilda myndigheten, Arbetsmiljöverket (tidigare Arbetarskyddsstyrelsen), i lag getts rätten att utfärda mer eller mindre konkreta skyddsregler generellt och inom olika branscher. Eftersom man inte kan räkna med att dessa icke-gemensamma regler följs spontant på samma sätt som vid gemensamma normer, så har det redan från början en särskilt myndighet, i detta fall arbetsmiljöinspektionen (tidigare yrkesinspektionen) inrättats för att kontrollera tillämpningen av dessa skyddsregler. Arbetstagarna kan också i särskild ordning vända sig till denna myndighet för att påkalla dess stöd och kontroll.

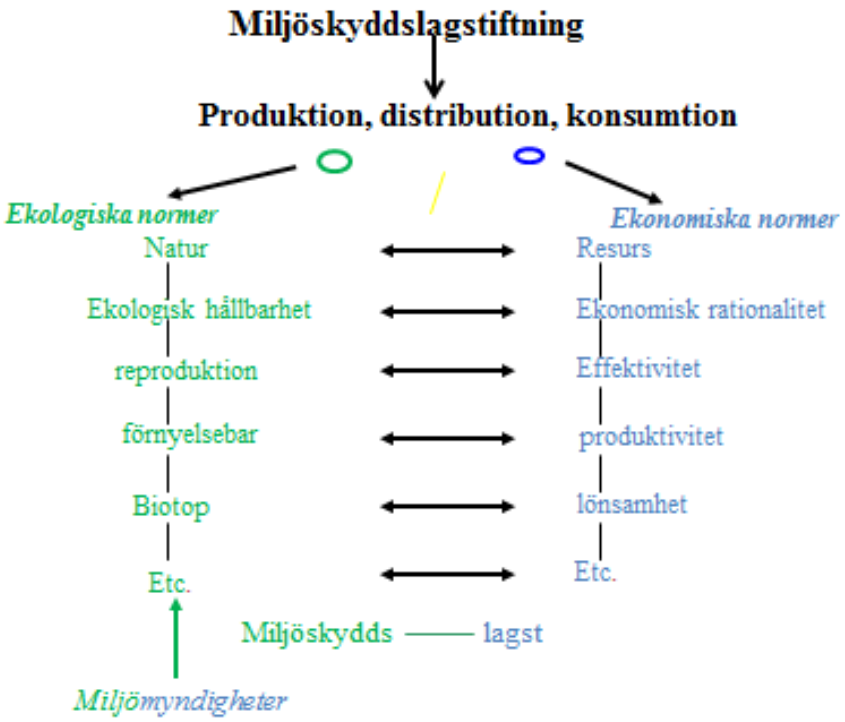
På konsumentskyddsområdet tar sig reglerna till skydd för konsumenterna delvis drastiska uttryck. Jämför följande bestämmelse hämtad från konsumentköplagen (1990:932) 18 §:

> *Vara är felaktig, om den säljs i strid mot ett förbud enligt 27 eller 36 § produktsäkerhetslagen (2004:451) eller mot ett annat försäljningsförbud som har meddelats i författning eller av myndighet väsentligen i syfte att förebygga att den som använder varan drabbas av ohälsa eller olycksfall eller för att annars hindra användning av vara som inte är tillförlitlig från säkerhetssynpunkt eller är så bristfällig att dess användning medför påtaglig fara för liv eller hälsa. (Lag 2008:492)*

Nog måste man i ett framtida historiskt perspektiv ställa sig undrande inför vad som kännetecknade den tid som kallades välfärdssamhället. På den tiden hade man bestämmelser varigenom det slogs fast att man inte fick sälja vara som var förbjuden eller att man riskerade

att skadas av varan när man använder den. För säkerhets skull föreskrev man att det skulle anses vara fel på en vara om dess användning medförde påtaglig risk för liv eller hälsa. Eftervärlden måste tro att vi var spritt språngande galna som sålde sådana produkter. Dessa regler handlar inte om straffbestämmelser gentemot dem som avviker från en i övrigt etablerad norm. Nej, vi är inne på civilrättens område, där det som regleras normalt inte är uttryck för något extremt beteende.

När det gäller miljöskyddslagstiftning gör sig liknande avvägning gällande som på arbetsrättens område. Här är det dock avvägningen mellan ekonomi och ekologi som står på spel. Jämför följande figur:



Under kapitel 2 i Miljöbalken (MB) med rubriken ”Allmänna hänsynsregler”, §§ 1 – 6, står det att man skulle vidta försiktighetsmått av olika slag, liksom att man skall hushålla med råvaror och energi. I 2 kap. 7 § kan man läsa följande:

> *Kraven på hänsyn enligt 2 – 6 §§ gäller i den utsträckning det inte kan anses orimligt att uppfylla dem. Vid denna bedömning skall särskilt beaktas nyttan av skyddsåtgärder och andra försiktighetsmått jämfört med kostnaderna för sådana åtgärder.*

MB 2 kap. 9 § 2 stycket föreskriver vidare:

> *En verksamhet eller åtgärd får inte bedrivas eller vidtas om den medför risk för att ett stort antal människor får sina levnadsförhållanden väsentligt försämrade eller miljön försämras avsevärt.*

Det är således ganska uppseendeväckande avvägningar som förväntas äga rum, där Naturvårdsverk, länsstyrelser och lokala miljöskyddsförvaltningar ska agera till skydd för människor som kan antas vara utsatta för miljöstörningar. Detta intryck förstärks ytterligare genom bestämmelsen i MB 2 kap. 10 §. Där föreskrivs följande:

> *Om en verksamhet eller åtgärd är av synnerlig betydelse från allmän synpunkt kan regeringen tillåta denna, även om förutsättningarna är sådana som anges i 9 § 2 stycket.*

Regeringen kan således bestämma att trots att människors levnadsförhållanden eller miljön förstörs så skall verksamheten tillåtas om det är av synnerlig betydelse. I samma paragraf föreskrivs ytterligare:

> *Detta gäller dock inte om verksamheten eller åtgärden kan befaras försämra det allmänna hälsotillståndet.*

Det som hittills beskrivits kännetecknas av att olika (handlings)system i människornas praxis kolliderar med varandra eller att de ställer oförenliga krav på varandra, varvid ett systems krav uppfattas som främmande för ett annat. Det uppstår då vad vi kan kalla för en inter-systemkonflikt, dvs. en konflikt mellan system.[68] I dessa situationer kan vi tala om att det föreligger normkonflikter. Så länge de olika handlingssystemen får leva sitt eget liv och var och en bestämma aktörernas handlande är det inga problem. Det kan på sin höjd ge upphov till intra-systemkonflikter, dvs. konflikter inom ett och samma system. Dessa kan hanteras inom ramen för varje handlingssystem för sig. Intersystemkonflikter, däremot, uppstår när handlande bestämt av ett system har konsekvenser för handlandet med stöd av ett annat system, dvs. när handlingssystemen kolliderar i mänsklig praxis, t.ex att det ekonomiska systemet har konsekvenser för det sociala eller ekologiska systemet på sätt som vi talade om ovan.

Situationen blir särskilt allvarlig om dessa kollisioner har en sådan frekvens och styrka att de hotar eller i vart fall stör de olika handlingssystemens reproduktion. Det är vad som kännetecknar det övermogna industrisamhället från 1970 och framåt. Då det i människornas praxis uppstår normkonflikter av det slag som beskrivits, hotas handlingssystemens reproduktion och krav ställs på rättsliga ingripanden. Även om rätten inte förmår att lösa det egentliga, underliggande problemet så har den ett högt symbolvärde som kan utnyttjas för att hålla samman samhället när det är utsatt för spänningar. Denna situation uppstår då det förekommer strukturella motsättningar mellan olika handlingssystem, dvs. då ett systems handlingsanvisningar systematiskt tenderar att komma i konflikt med ett annat systems normer, när de berör samma del av mänskliga praxis. Genomgående uppkommer i dessa situationer motsättningar och konflikter mellan individen, å ena sidan och något system, å andra sidan. Detta återspeglas i konflikter mellan olika normer.

Under en övergångsperiod får vi ta det goda med det onda. Så småningom tycks dock det onda ta överhanden och då uppkommer frågan: Måste vi ta det onda med det goda eller går det att sätta stopp? Går det att välja bort?

Övervakning som samhällsfenomen

Om vi ser till övervakning som samhällsfenomen så återfinns liknande avvägningar i den lagstiftning som växt fram på nationell basis. 2 kap 6 § i Regeringsformen:

[68] Distinktionen mellan inter- och intra-systemkonflikter görs av den norske fredsforskaren Johan Galtung (1970).

Var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp även i andra fall än som avses i 4 och 5 §§. Var och en är dessutom skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Utöver vad som föreskrivs i första stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten (understruket här), om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Lag (2010:1408).

Det finns ett principiellt skydd för den personliga integriteten som kan användas till skydd mot övervakning, i vart fall mot det allmänna, dvs. stat och kommun. Men skyddet handlar ”bara” om betydande intrång och att det rör den enskildes personliga förhållanden. Båda dessa inskränkningar i det personliga integritetsskyddet lämnar tämligen stort och svårbestämt tolkningsutrymme. Regleringen påminner om miljöskyddets ovan redovisade reglering i Miljöbalken.

Även i Europarådet konvention om mänskliga rättigheter finns det bestämmelser om skydd för privat- och familjeliv som har med skyddet mot övervaktning att göra. Artikel 8 i denna konvention föreskriver följande:

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

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

Den brasklapp som andra stycket innebär öppnar för omfattande inskränkningar i den personliga integriteten. Det ska visserligen ske med stöd av lag, men ändå. Observera att myndigheterna i dessa fall inte opererar till skydd för individen och dennes integritet utan tvärtom representerar det överordnade, ”hotande intresset”, övervakning. Det sker främst genom den civila myndigheten Försvarets Radioanstalt, (FRA). FRA har till uppgift att skydda Sverige och svenska intressen. Det sker dels genom att olika uppdragsgivare ges unik information om viktiga utländska förhållanden av betydelse för svensk utrikes-, säkerhets- och försvarspolitik, dels genom arbete med att stärka informationssäkerheten hos samhällsviktig verksamhet.

Signalspaning sker på uppdrag av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och/eller Rikskriminalpolisen. FRA:s signalspaning kräver tillstånd från Försvarsunderrättelsedomstolen och granskas löpande av Siun, Statens Inspektion för försvarsunderrättelseverksamheten. Det finns ett uttryckligt förbud i lagen för FRA att inhämta signaler där både avsändare och mottagare befinner sig i Sverige.

Försvarsunderrättelsedomstolen beslutar om tillstånd för att FRA ska få inhämta trafik. Domstolen bedömer om det är förenligt med lagstiftningen och regeringens nationella inriktning. Domstolen beslutar om vilka sökbegrepp eller kategorier av sökbegrepp som får användas. Domstolen beslutar också om vilka fibertrådar eller signalbärare som FRA ska få tillgång till.

Siun är det huvudsakliga granskningsorganet för FRA och de verkställer även domstolens beslut och ger FRA tillgång till signalbärare enligt tillstånden. Siun ska granska FRA:s verksamhet och se till att lagen följs. Kontroll görs av bland annat de sökbegrepp som

används, hur förstöringspliktig information förstörs och hur rapporteringen sker. Siun ger FRA tillgång till de kablar som omfattas av tillstånden. Siun:s granskningar av FRA resulterar i flertalet fall inte i någon synpunkt eller åtgärd. I en del fall kan Siun ge olika former av kommentarer. De sträcker sig från förslag till förbättringar av rutiner till i ett fall påpekande av en brist i personuppgiftshanteringen vid FRA.

Datainspektionen granskar hanteringen av personuppgifter. Myndigheten granskar behandlingen av personuppgifter inom FRA. I ett särskilt uppdrag under 2010 granskade inspektionen verksamheten ur ett integritetsskyddsperspektiv. Utöver ovanstående instanser har en parlamentarisk kommitté (Signalspaningskommittén) att följa signalspaningen via FRA ur ett integritetsskyddsperspektiv, med fokus på hur den nya lagen tillämpas, vilket redovisades 8 februari 2011.

Datalagringsdirektivet har kommit att bli en allt tydligare konflikthärd mellan rättsliga och nätsliga normsystem. I sig syftar direktivet till att ålägga internetoperatörer och leverantörer av digitala lagringstjänster att lagra uppgifter om användares aktivitet. Direktivet har på grund av sin pro-aktivitet och allt för breda omfång underkänts i Europeiska domstolen för de mänskliga rättigheterna (ECHR), men då det hunnit ratificeras i flera medlemsstater – däribland Sverige – är lagringen lagstadgad på flera håll i Europa. Detta har skett i tid i två näst intill parallella processer.

Dels har flera svenska internetleverantörer med Tele2 och Bahnhof i spetsen tydligt försökt opponera sig mot den påtvingade lagringen. Tele2 var under en tid i hätsk debatt med Rikspolisstyrelsen som presenterade ett narrativ där internetleverantörerna obstruerade rättsvårdande myndigheters arbete mot grov och organiserad brottslighet. Med tiden gav Tele2 upp striden och sällade sig till gruppen leverantörer som datalagrar enligt rådande svensk lagstiftning. Bahnhof å sin sida fortsatte motsätta sig lagringen under lång tid, bland annat genom att överklaga beslut rörande detta till högre rätt. När Post- och Telestyrelsen PTS ålade Bahnhof ett kännbart vite om man inte följde uppmaningar att datalagra valde Bahnhof istället att ansluta alla sina kunder till en stiftelseägd anonymiseringstjänst som på så sätt är tänkt att garantera användarintegriteten.

Dels gruppanslöt branschorganisationen Svenska Stadsnätsföreningen ett stort antal internetleverantörer till ett avtal med en svensk aktör på datalagringsarenan, Maintrac, med huvudsakligt argument att mindre leverantörer inte har kapacitet eller ekonomi att själva stå för infrastrukturen. Parallellt med detta ingick även Säkerhetspolisen SÄPO samarbete med Maintrac om att underlätta uthämtning av information för att undslippa den fördröjning mellan krav och utlämning som av rättsvårdande myndigheter ofta argumenteras mot som försvårande. Detta strider dock mot gällande svensk lag. Samarbetet avbröts efter publicitet och avslöjanden av bland annat Sveriges Radio.

Övervakning förekommer också genom kameror (Ström 2003). Denna verksamhet är omgärdad av särskild lagstiftning. Den s k Kameraövervakningslagen föreskriver bl.a. följande:

> *7 § Kameraövervakning ska bedrivas lagligt enligt god sed och med tillbörlig hänsyn till enskildas personliga integritet.*

Denna reglering förefaller vara en kapitulering inför problemet. Passusen att kameraövervakning ska bedrivas lagligt ter sig som överflödig i en lagparagraf. Det borde tas för givet. Tillägget att det ska ske enligt god sed antyder att det skulle finnas något som är lagligt utan att följa god sed, vilket framstår som märkligt. Uttrycket, rekvisitet som juristerna kallar det, ”med tillbörlig hänsyn till enskildas integritet”, är just vad saken handlar om. Det

är bra om det fanns någon form av innehållslig bestämning av vad detta innebär. Uttrycket tillbörlig hänsyn förekommer i en del rättsliga sammanhang där avvägningar förväntas ske, såsom i Väglagen där det bl.a. föreskrivs att vid byggande av väg ska tillbörlig hänsyn tas till allmänna och enskilda intressen. I Kameraövervakningslagen (2013:460) anges dock inte i vilka situationer som kameraövervakning ska anses legitim, dvs. vilket värde i avvägningen som ska tillmätas kameraövervakningen versus den personliga integriteten. Det är något som får avgöras i det särskilda fallet i samband med att det ställs krav på tillstånd för kameraövervakning i de fall en övervakningskamera ska sättas upp på sådant sätt att den kan riktas mot en plats dit allmänheten har tillträde. Tillstånd prövas (läs ges) av länsstyrelsen i respektive län.

I kameraövervakningslagen 9 § får vi lite vägledning om vilka villkor som krävs. Där föreskrivs att ”(t)illstånd till kameraövervakning ska ges om intresset av sådan övervakning väger tyngre än den enskildes intresse av att inte bli övervakad.” Av detta påstående blir man inte mycket klokare. Vi får emellertid ytterliga vägledning i 9 § 2 st som föreskriver att ”(v)id bedömningen av intresset av kameraövervakning ska det särskilt beaktas om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller andra därmed jämförliga ändamål.” Ytterligare föreskrivs i st. 3 att ”(v)id bedömningen av den enskildes intresse av att inte bli övervakad ska det särskilt beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas.”

Det problem som kvarstår är väl närmast att förutse och beakta de oavsiktliga integritetskränkningar som kan uppstå i samband med kameraövervakning, dvs. de fall som är indirekta och oförutsedda. Efter anmälan får övervakningskamera enligt Kameraövervakningslagen 12 § sättas upp för kameraövervakning i en banklokal, en lokal hos ett kreditmarknadsföretag eller ett postkontor eller i området omedelbart utanför in- och utgångar till en sådan lokal, eller vid uttagsautomater eller liknande anordningar, allt i syfte att förebygga, avslöja eller utreda brott. För säkerhets skull föreskriver lagen att kameraövervakning inte får avse omklädningsrum, provhytter, toalettutrymmen eller liknande utrymmen. Vad som gäller i övrigt är i brist på reglering oklart.

Övervakning som postindustriellt problem

Övervakning som samhällsproblem hänger samman med den teknikutveckling som den digitala tekniken för med sig. Teknikutvecklingen ger upphov till olika möjligheter. Den kan användas för olika syften. I detta samhällsskede är samhällsproblemen mer en fråga om val av framtidsalternativ än kompromisser inom ramen för ett alternativ. Biotekniken är ett exempel. Genmodifiering har alltid förekommit, men med den nya digitala tekniken förändras förutsättningarna radikalt, både i förhållande till människan och till naturen. Ska vi beträda bioteknikens mark eller inte? Det finns egentligen inte mycket annat än ett val att göra. Inte desto mindre har reglerna om genmodifiering införts som ett kapitel i Miljöbalken, som om det vore en fråga om kompromisser. Användning av genmodifierad teknik förutsätter tillstånd. När ska tillstånd ges enligt Miljöbalken (13 kap)? Svaret är, när det är etiskt försvarbart!

Vi finner här samma regleringskapitulation som vi såg ovan rörande övervakning. Som när Försvarsunderrättelsedomstolen beslutar om tillstånd för att FRA ska få inhämta trafik. Domstolen har då att bedöma om det är förenligt med lagstiftningen och regeringens

nationella inriktning. Eller som när länsstyrelserna ska ta ställning till tillstånd för kameraövervakning eller inte. Är kameraövervakningen laglig enligt god sed och sker den med tillbörlig hänsyn till enskildas personliga integritet? Det är lite som att förutsätta det som borde bevisas.

Medan det senmoderna samhället i ett skede då industrisamhället har nått sin höjdpunkt och inte längre entydigt producerar nytta möter regleringsproblem i form av behovet av kompromisser inom ramen för den befintliga tekniken, mellan det vi vill ha och det vi inte vill ha, de negativa – kontraproduktiva – effekterna som alltmer med nödvändighet gör sig påminda. Men vi kan inte både ha kakan kvar samtidigt som vi äter upp den. Vi står med övervakning som exempel inför ett kvalitativt nytt regleringsfenomen. Här gäller det att välja vilken kaka eller del av kakan vi vill ha. Internet i sig är ett exempel. Grundprincipen för Internet är att det ska vara öppet och fritt för alla. Lawrence Lessig talar om ”the norm of open code” (Lessig 2006). Denna syn på användningen av Internet konkurrerar med en annan användning. Den som handlar om övervakning och begränsning av Internet för olika ändamål. Den teknikutveckling som ligger bakom framväxten av det vi kallar informationssamhället tenderar att i ett första skede anammas och användas inom ramen för det tidigare samhällets logik. Det är där makt och resurser finns. Övergången från ett samhälle till ett annat leder till utmaningar för de styrande, de med makt, inom samhällets alla delar. Dessa får ett ökat behov av att kontrollera sina medborgare. Vetenskapen har sitt *peer review*-system som framstår som ett legitimt sätt att kontrollera, medan andra system tvingas till mer klandestina åtgärder. Övervakning tillhör denna kategori.

Går det då inte att reglera? Kan man inte tänka sig att samhällsfenomenet övervakning så småningom når en ”mognad” där man kan urskilja olika intressen som kan lägga grunden för reglerande kompromisser. Redan det hittills sagda antyder svårigheterna. Till detta kommer två tendenser i fråga om informationssystem för övervakning som ytterligare understryker svårigheterna och det principiellt annorlunda när det gäller regleringen av övervakning. Det handlar om att (1) systemen för övervakning integreras horisontellt. De sprider sig utan överordnade beslut mellan och inom olika samhällen. Vidare och delvis som en följd av det först nämnda (2) minskar kopplingen till nationalstaten. I båda fallen försvåras ansvarsutkrävande.

Den norske rättssociologen Thomas Mathiesen menar att vi befinner oss i en situation som han med paralleller till Lex Mercatoria på affärslivets område kallar för *Lex Vigilatoria*. Han talar på samma sätt om en lag utan stat på ett internationellt plan, dvs. en det internationella övervakningssamhällets rätt (Mathiesen 2008). Mathiesen tycker sig se en utveckling mot ett globalt kontrollsystem som lever sitt eget liv. Han ser två mekanismer som gör sig gällande. En som handlar om en fortlöpande integration av olika kontrollsystem som samtidigt blir alltmer sammanflätade. Mathiesen ställer sig frågan om inte en form av sedvanerätt håller på att växa fram på det internationella planet, där olika kontrollsystem, när de väl är etablerade, tenderar att utvidga sig genom att sammankopplas med andra kontroll- och informationssystem. Detta sker genom allehanda informella överenskommelser och arrangemang som följer en slags sociologisk logik. Den andra mekanismen består i det frigörande från nationalstaten och dess demokratiska processer som kan iakttas.

Det tycks således som om övervakning snarare vinner rättsligt stöd än underkastas begränsningar. Som exempel hänvisar Mathiesen till nyligen införda möjligheter att begära ut information av tredje land med stöd av olika övervakande kontrollmekanismer. *Principle of availability* (Hague Programme) innebär att polismyndigheter inom EU kan utbyta

information från olika nationelle register. *The Prym Treaty*, känt också som Schengen III, innehåller bestämmelser som gör det möjligt att för de medlemsstater inom EU som undertecknat konventionen att utbyta och samla information från databaser om terrorism, fingeravtryck och bilregistreringsdata.

Det tycks, menar Mathiesen, som om den horisontella utbredningen av kontrollsystemen på ett internationellt plan i motsvarande grad minskar systemens koppling till nationalstatliga kontrollmekanismer, politiskt och rättsligt. Istället blir det systemfunktionärer som är en del av systemet som utan insyn och kontroll utvecklar tekniken för övervakning. Det framstår som tveksamt att förlita sig på rättslig reglering. Om man ska reglerna måste man sätta upp tydliga gränser för utrymmet för övervakning. Det går inte att låtsas som om det kan vara föremål för rättsliga kompromisser och överväganden i individuella fall. Det rör sig inte om negativa externa effekter i enskilda fall, den typ av rättslig reglering vi har vant oss vid. Det handlar istället om att vi har att göra med en ny teknik som kan användas för goda eller onda syften. Problemet måste därför underkastas demokratisk kontroll varigenom man definierar vad som är gott och vad som är ont i sammanhanget. Med denna utgångspunkt kan man måhända sätta upp spelregler som kan göra anspråk på att kontrollera fenomenet övervakning.

Ett alternativ som kan prövas under tiden, som vi ser det, är att ställa krav på den som utvecklar tekniken, vilket är något som tagits upp i flera parallella diskussioner under tidigt 2010-tal. Framförallt relaterat till omvärldshändelser såsom den så kallade Arabiska våren samt den högljudda debatt kring övervakning som främst relateras till avslöjanden av Wikileaks och den amerikanske visselblåsaren Edward Snowden. Men även i och med granskningar av svenska företag i telekomsektorns förehavanden i såväl post-Sovjetiska stater som i andra icke-demokratiska regimer.

Frågan är inte enkel. Exempelvis har dåvarande utrikesministern Carl Bildt uttryckt stöd för att svenska telekomföretag bör agera även i ofria stater, eftersom utbyggnaden av internetinfrastruktur också ger politiska frihetsrörelser större möjlighet att kommunicera fritt och brett. Företagen menar därtill att de negativa konsekvenserna av deras verksamhet är bortom deras kontroll, exempelvis i konfliktområden där det geopolitiska läget generellt är komplicerat eller i stater där lagstiftning medger att säkerhetstjänst aktivt registrerar och övervakar nätlig aktivitet. Dock har diskussionen medfört att flera stora kommersiella aktörer, däribland svenska Ericsson, inlett ambitiösa arbeten med konsekvensutvärderingar ur ett mänskorättsperspektiv gällande deras aktivitet i svåra miljöer. Flera internetleverantörer, med svensk-finska Telia-Sonera i spetsen, publicerar numera regelbundet vad de kallar transparensrapporter där de sammanställer vilken typ av påverkan statliga aktörer har på deras verksamhet.

Det rör sig om civil infrastruktur som har som huvudsyfte att agera möjliggörare. Gemensamt med flera typer av hårdvarulösningar kallas det *dual-use* teknologi, för att synliggöra de dubbla användningsområdena. Flera myndigheter har börjat se över möjligheterna att mer systematiskt kunna utvärdera detta, bland annat Exportrådet och Exportkreditnämnden. Vad gäller mer utpräglat offensiva, *single-use* teknologier av övervakningsart finns en internationell diskussion om möjligheten att klassificera vissa sådana lösningar som ett aktivt vapenslag och därmed föra in dem i den redan existerande Wassenaar-överenskommelsen om vapenexport.

Här finns dock ytterligare försvårande omständigheter. Framförallt rör detta sig om hur dubbelheten i tekniken ska hanteras. Det är möjligt att det inte är särdeles enkelt att skilja på

dual-use och *single-use* teknologier. Samma tekniska lösningar som kan användas för att söka efter sårbarheter i offensiva syften kan vara nödvändiga för att söka efter svagheter i egna system. Det knyter också an till den diskussion som växt fram post-Snowden, om hälsoläget för vår samhälleliga digitala infrastruktur. I en tid när övervakning upptäcks i lager efter lager av nät som vi gjort oss alltmer beroende av är trygghet och social stabilitet i riskzonen. Exempelvis menas enligt en av de läckor som Edward Snowden tagit ära för att amerikansk säkerhetstjänst aktivt försvagat de kryptografiska nycklar som det stora flertalet tekniska lösningar lutar sig mot. Om detta stämmer kan man anta att det finns okända säkerhetshål inte enbart i det vi känner som internet utan även i såväl våra banktransaktioner som digitala hälsosystem och andra samhällsbärande nätverk.

Referenser

Coleman, J. S. (1990) Foundations of Social Theory, Cambridge Mass: Harvard University Press.

Foucault, Michel (2003) Övervakning och straff: fängelsets födelse, 4. översedda uppl., Lund: Arkiv.

Galtung, Johan (1970) Fredsforskning, 3. uppl, Stockholm: Prisma.

Hadley-Kamptz, Isobel (2011) Frihet och Fruktan. Tankar om liberalism, Stockholm: Natur & Kultur.

Hydén, Håkan (2002) Normvetenskap, Lund Studies in Sociology of Law.

Lessig, Lawrence (2006) ".commons" i John N. Drobak, Norms and the Law, Cambridge University Press.

Mathiesen, Thomas (2008) Lex vigilatoria: Global control without a state? i Deflem, Mathieu (red.) Surveillance and Governance: Crime control and beyond, Sociology of crime, law and deviance, vol.10.

Ström, Pär (2003) Övervakad. Elektroniska fotspår och snokarsamhället, Kristianstad: Liber

Demokratins skydd eller självmål? En sammanfattande diskussion

Wilhelm Agrell

> *Bakom Winstons rygg fortsatte telescreenen att rabbla något om tackjärn och nionde treårsplanens rekord. Telescreenen både sände och upptog. Varje ljud som Winston gav ifrån sig utöver den svagaste viskning togs upp, och så länge han höll sig inom det fält som metallplattan behärskade kunde han även ses. Det var naturligtvis omöjligt att vet om man iakttogs i ett visst ögonblick. Man fick gissa hur ofta och enligt vilka principer tankepolisen kopplade in varje enskild individs nät. Det var en ren omöjlighet att den iakttog varenda människa hela tiden (Orwell 1964:6).*

Redan på de första sidorna i Orwells klassiska dystopi *1984* konfronteras läsaren med den totalitära statens övervakningssystem. Eller för att vara mer exakt, ett av dem. Utanför fönstret hörs ljudet av en helikopter, en patrull som flyger runt och tittar in genom fönstren. Men det är inget som oroar Winston, han arbetar på Sanningsministeriet och vet att det enda han verkligen måste frukta är tankepolisen. Det är därför han ger akt på telescreenen, försöker lista ut dess prestanda och hur den används. Han föredrar att stå vänd bort från den men vet att inte heller det är ofarligt eftersom också en ryggtavla kan avslöja mycket. Winston Smith är en lojal arbetsmyra i yttre partiet som lever ett i alla avseenden torftigt liv i Ledarens tjänst. Men av en slump råkar telescreenen i hans lägenhet vara lite felinstallerad i förhållande till planlösningen och han upptäcker att det finns en död vinkel inne i en alkov där dess optiska sensor inte har täckning. Tillfället gör som bekant tjuven och det lilla obevakade området föder tanken på att begå ett ohyggligt brott, att börja föra en alldeles egen hemlig dagbok.

Rent tekniskt uppvisar Orwells science fiction-uppfinning telescreen betydande likheter med det projekt Petrus Bolin beskriver i sitt bidrag och som fått namnet *En virtuell kompis*, ett system som är avsett att ge kassapersonal en ökad trygghet genom närvaron av en operatör på en larmcentral. Kassörskan som vinkar till sin virtuella kompis, eller snarare beskyddare, är den psykologiska motsatsen till den förskrämde Winston Smiths ryggtavla eller kurande inne i den (förhoppningsvis) döda vinkeln. Här är det snarare det oönskade klientelet i butiken som aktualiserar paralleller. Dessa håller sig undan när de väl blivit uppmärksamma på den preventiva övervakning som finns framme vid kassan, något som är inte bara detta utan det stora flertalet övervakningssystems syfte.

Men här börjar också problemen dyka upp. Ett omedelbart sådant är att den önskade effekten kanske inte uppnås. Det kan som Per Gustafson beskriver i sitt kapitel bero på att utrustningens tekniska prestanda helt enkelt är för låga eller att den, likt telescreenen i Winston Smiths lägenhet, är felmonterad. Men orsaken kan också vara mer komplex och handla om satsningar på övervakningssystem som politiska symbolhandling och om ordningsstörandets socialpsykologi. De brittiska forskningsresultat som Benjamin Weaver och Markus Lahtinen redogör för ger en på många sätt förvånande bild av övervakningens begränsade brottspreventiva effekter utanför specifika objekt som parkeringsplatser, där presumtiva förövare väljer icke-övervakade platser så långt detta är möjligt.

I princip innebär detta att man genom olika tekniska övervaknings- och skyddssystem, t.ex. för kontanthantering, kan reducera eller i vissa fall eliminera specifika brottstyper. Processen

är dock dynamisk och som med annan brottslighet kan aktörerna välja alternativa mål, tillgripa motmedel som maskering eller ändra brottsupplägg. Processen avstannar inte utan är ständigt pågående så länge för brottslig verksamhet eller ordningsstörning som fenomen fortgår.

Kameratekniken, eller snarare bildbehandlingens digitalisering, har dessutom öppnat ökade möjligheter för att utreda begångna brott, eller bedriva efterspaningar. Weaver och Lahtinen diskuterar betydelsen av övergången från analog till digital teknik i Storbritannien och exemplifierar utredningspotentialen med identifierandet av gärningsmännen i terrorattentaten i London 2005 och deltagare i uppploppen 2011. Man kan här tillfoga kameramaterialets betydelse i efterspanandet av gärningsmannen från attentatet i Köpenhamn 14 februari 2015. Weaver och Lahtinen pekar här på ett från andra samhällsfrågor välbekant fenomen, att framtida användning av system diskuteras med utgångspunkt från forskning på tillämpningar av äldre och idag överspelad teknik

Utveckling och användning av övervakningssystem är inte enbart en fråga om förhållandet mellan förväntad nytta och tekniska prestanda och investeringar. Detta kan vara fallet i avgränsade sammanhang som i industriella processer men inte vid användning som berör allmänheten eller som har en kontrollerande funktion gentemot individer. Graden av tvång och intrång spelar här en viktig roll. Ett system som kan aktiveras och deaktiveras av den övervakade har inte samma innebörd som ett system som är utanför vederbörandes kontroll och vars aktivitet inte kan följas - se till exempel betydelsen av den ”demonstrationsmonitor” många livsmedelsbutiker har i entrén. Ett mycket selektivt system med en stor och hemlig insamlingspotential kan upplevas som mer hotfullt än ett tekniskt mer begränsat system som i själva verket samlar in mer information. Graden av hotfullhet är i grunden subjektiv. FRA:s oreglerade signalspaning i de satellitburna telekommunikationerna före tillkomsten av lagen om signalspaning i försvarsunderrättelseverksamheten upplevdes inte som ett integritetsproblem av allmänheten av det enkla skälet att verksamhetens existens överhuvudtaget inte var känd. Men av detta kan man inte dra slutsatsen att den tidigare oreglerade kommunikationsspaningen *inte* var ett integritetsproblem och saknade en potential att påverka allmänhetens tillit.

Den upplevda övervakningens art och omfattning är bara en del av problematiken. Acceptansen är också i hög grad beroende av åtgärdernas syfte, eller snarare hur detta syfte uppfattas och om det betraktas som legitimt i förhållande till ett upplevt eller fruktat integritetsintrång. De undersökningar Weaver och Lahtinen hänvisar till exemplifierar lägen där människor på allmän plats upplever en större trygghet med kameraövervakning - något som inte nödvändigtvis behöver korrelera med en motsvarande faktisk säkerhet. För flertalet (men inte självklart alla) framstår då övervakningen som legitim. Här har då en säkerhetskultur etablerats på det sätt Per Gustafson beskriver, i detta fall med en övervikt för acceptans gentemot en upplevelse av integritetskränkning.

Acceptansen är i sin tur beroende av graden av tillit. Om samma system skulle ha en sidoanvändning, eller en uppenbar potential för sådan, skulle förmodligen acceptansen sjunka drastiskt. De kraftiga opinionsrörelserna i samband med FRA-lagsdebatten är ett exempel på detta. Misstron mot myndigheternas goda vilja visade sig vara betydande och acceptansen för övervakningsåtgärderna blev därför låg, trots hänvisning till rikets säkerhet och behovet att förebygga allvarliga samhällshot som terroristbrott. Problemet med fenomen som acceptans och tillit är att de är starkt beroende av ett större politiskt och socialt sammanhang, liksom av snabba förändringar i opinioner och av reaktioner på individnivå. Samhällsinstitutionernas

legitimitet har således en stor betydelse för tilltron till utsagor om övervakningens omfattning och syfte. Snowden-debatten belyser hur medial uppmärksamhet av övervakning kan påverka både acceptans och tillit - i extremfallet till hela infrastrukturen för elektronisk kommunikation.

Rent mjöl i fel påse? Kontroversen kring metadata

Övervakning har alltså både en subjektiv upplevd sida och en objektiv materiell som hänger samman med vilken information som kan samlas in, som faktiskt samlas in, som vidarebefordras och lagras och hur sedan denna information tolkas och används, alltså den informationscykel som till stor del liknar eller är identisk med underrättelsecykelns flödes- och processtänkande. En sådan koppling till underrättelsecykeln hjälper också att synliggöra var i en process de problematiska punkterna finns. Mycket av debatten om övervakningssystem är inriktad på själva åtkomsten och insamlandet av informationen. Detta gällde debatten kring FRA-lagen, där fokus låg på signalspaningens åtkomst till och sökning i de elektroniska flödena. Mycket mindre uppmärksamhet ägnades informationens betydelse i en fortsatt underrättelseprocess och dess innebörd som underlag för beslut och åtgärder, både i närtid och i en svåravgränsad framtid med permanent lagrade dataset.

Den omfattande internationell debatten kring NSA:s och GCHQ:s insamling och lagring av ospecificerade metadata (*Bulk Access*) har däremot i hög grad handlat om informationens innebörd i den fortsatta underrättelseprocessen. Myndigheterna har i sitt försvar av insamlingen hävdad att metadata definitionsmässigt utgör ett mindre integritetskänsligt material än själva innehållet i kommunikationen och att insamling och lagring därmed är mindre problematisk än avlyssning i traditionell mening. I USA har denna tolkning haft stor betydelse eftersom den inneburit att de ansvariga instanserna inte ansett metadata åtnjuter samma skydd enligt konstitutionens fjärde tillägg. Men också i svensk rättspraxis har det skett en glidning som öppnat för det Markus Naarttijärvi beskriver som ett separat lagtekniskt spår avseende metadata.

Denna tolkning har starkt ifrågasatts i post-Snowden debatten, inte bara på rent rättsliga grunder utan också utifrån beskrivningen av metadatas relativa harmlöshet, något som samtidigt kontrasterar mot NSA:s stora investering i program för just insamling av bearbetning av metadata. Debatten om metadata förefaller både i USA och i Europa ha ett inslag av samma slags eftersläpningsfenomen som återfinns kring kameraövervakning. Ett tidigare fokus på telefonavlyssning färgar av sig, trots att metadata, precis som kameraövervakningen, har genomgått ett kvantsprång i fråga om informationsinnehåll och därmed fortsatt analyspotential.

En av de punkter där den av president Obama tillsatta översynsgrupp riktat skarpast kritik mot insamlingen av material från elektronisk kommunikation gäller just synen på metadata (Liberty and Security in a Changing World 2013). Gruppen pekar på att den kvalitativa skillnaden mellan innehåll och metadata minskar i takt med den tekniska utvecklingen. Andra har gått betydligt längre och pekat på att metadata i själva verket kan vara viktigare än innehållet, beroende på för vilket syfte den insamlade och bearbetade informationen används. Metadata spelar således en central roll som underrättelseunderlag för USA:s användning av drönare för utomrättsliga avrättningar, eller som förre NSA-chefen general Hayden har uttryckt saken i ett försvar av insamlingsprogrammet: Vi dödar folk på basis av metadata (Cole 2014).

Ett motsvarande ifrågasättande som det amerikanska av den vidare innebörden av metadata återfinns, som Naarttijärvi diskuterar, i EU-domstolens principiellt viktiga underkännande 2014 av datalagringsdirektivet. EU-domstolen tar här sikte på själva potentialen i det insamlade och lagrade informationen och möjligheterna att kartlägga enskilda personers liv, en kartläggning som kan bli mycket omfattande och inträngande och vars innebörd inte går att fastlägga på förhand.

Diskussionen kring metadata har tydligare än andra frågor lett till ett ifrågasättande av den fortfarande ofta åberopade tesen om ”rent mjöl i påsen”, alltså att den som inte har några brottsliga avsikter inte heller har något att frukta, att det rena mjölet per definition kommer siktas genom processens filter. Intressant i sammanhanget är den kritiska bild den amerikanska granskningsgruppen ger av myndigheternas metod att utnyttja metadata för att åstadkomma kontaktkluster i flera led från ett misstänkt telefonnummer, något som oundvikligen leder till att en stor mängd ovidkommande personer granskas och registreras. Ju större datamängder som sammanställs, desto större är risken för slumpmässiga korrelationer som kan få dem att framstå som misstänkta.

Att förhålla sig till teknikens potential och konsekvenser

Här någonstans, i teknikens mångtydiga innebörd och integritetens både konkreta och samtidigt djupt subjektiva karaktär, finns det bärande tema som löper genom de olika bidragen i denna antologi, ett tema som trots, eller kanske snarare tack vare, bidragens olika upplägg och fokus knyter dem samman. Det är som om varje diskussion på temat övervakning och integritet förr eller senare kör ner i denna problematik och de ändlösa svårigheterna att åstadkomma en avdömning mellan motstående intressen.

Den amerikanska debatten på 1970- och 80-talen om fenomenet Survelliance Technology var starkt fokuserat på själva teknikutvecklingen, dess dynamik och potential (Electronic Surveillance 1985). Debatten fördes i en större teknikkritisk kontext där det positiva värdet av ny teknik ifrågasattes med hänvisning till kapprustning, miljöproblem och upplevd resurs- och energiknapphet, men också utifrån statens övervakning av medborgarna och urholkandet av deras konstitutionella skydd. Delvis kan denna teknikkritiska debatt ses som en reaktion på 1950- och 60-talens teknikoptimism och tro på storskalig teknik som lösningen på olika samhällsproblem. Ungefär samtidigt som den informationsteknologiska utvecklingen på allvar tog fart från senare delen av 1980-talet avstannade dock debatten om övervakningsteknologin. Till en del kan detta förmodligen förklaras med de förändrade hotbilderna och därmed också övervakningsteknologins bärare. Staten och dess kontrollfunktioner var under 1990-talet på tillbakagång på en rad plan, en utveckling som i viktiga avseenden bröts efter 2001, samtidigt om den i andra fortsatte och fördjupades.

Övervakningen är, skriver Håkan Hydén och Marin de Kaminski, ett kvalitativt nytt regleringsfenomen. Det avviker på ett grundläggande sätt från andra samhällsområden som format regelverk och normsystem för avvägningar. Hydén och Kaminski sätter frågetecken för möjligheterna att här alls bygga upp sådana regelverk, framförallt till följd av globalisering och teknikspridning. Systemen ligger i många fall ovan och bortom nationalstaten och dess demokratiska processer.

Janne Flyghed diskuterar i sitt bidrag denna horisontella spridning utifrån säkerhetssektorns privatisering och därmed de minskande möjligheterna för medborgarna att överblicka och utöva kontroll. Den amerikanska debattens fokus på myndigheternas potential att övervaka medborgarna som det huvudsakliga problemet har här sin omvändning i en praxis där medborgarna möjligheter att få insyn och utkräva ansvar av myndigheter minskar eller försvinner. Naarttijärvi ger ett exempel på detta i den ovan berörda glidningen i fråga om metadata, en glidning som i tiden sammanfaller med telemarknadens avreglering och överflyttandet av regelverket till den privata marknaden. Den kontrovers som följt i Sverige på EU-domstolens beslut att underkänna legaliteten i datalagringsdirektivet har som Julia Branting tar upp inneburit att privata aktörer aktivt motsatt sig krav från myndigheterna på att tillgängliggöra metadata. Frågan är hur detta påverkar förutsättningarna för medborgarnas tillit, och inte minst tillit till vad och vem.

Tilliten påverkas inte bara av dessa strukturella förändringar utan också och mera direkt av den glidning i lagstiftningen och myndigheternas verksamhet som både Branting och Naarttijärvi beskriver och diskuterar i sina respektive bidrag. I grunden ligger den metod som lagstiftarna använt för att ta ställning till olika former av övervakningsmetoder, först inom ramen av den brottsutredande verksamheten men alltmer inom en växande och svåravgränsad underrättelsedomän, i praktiken en förskjutning i syftet från utredande av begångna brott till proaktiv arbete mot möjliga brott och samhällshot. En slags preventiv logik har därmed etablerats där en diffus potentiell nytta ställs mot svårdefinierade och följaktligen tänjbara integritetshänsyn.

Den stora restriktivitet som däremot präglat tillståndsgivningen kring övervakningskameror som Per Gustafson ger exempel på skulle kunna tolkas som ett i reglerings- och kontrollsammanhang inte ovanligt fenomen där lagstiftare och myndigheter lägger ner oproportionerligt stor möda på att granska och kringskära övervakningssystem med begränsad användbarhet eller små effekter på den personliga integriteten. Orsaken kan helt enkelt vara att man här kan reglera, medan de stora och verkligt betydelsefulla genombrotten glider förbi i det tysta därför att de är för svåra att få grepp om eller, som Flyghed skriver, till följd av internationalisering och privatisering helt enkelt i många fall inte längre är gripbara.

Branting och Naarttijärvi tecknar en bild där lagstiftarnas metod att göra avvägningar mellan samhällsnytta och integritetsintrång framstår som i bästa fall förenklad och schablonmässig och i värsta fall som rättslig regndans. Den faktiska målsättningen blir där snarare att krångla lagstiftarna ur ett besvärligt och politiskt känsligt dilemma så snabbt och smärtfritt som möjligt men utan att egentligen angripa de etiska och samhälleliga dilemman som bara växer i takt med teknikutveckling och glidningar i rättspraxis. En möjlig väg vidare är då Helen Nissenbaums teori om ett kontextberoende integritetsbegrepp, alltså att man varken ser till tekniken eller informationen som sådan utan till det större sammanhanget och hur detta påverkas av ett förändrat flöde av personuppgifter. Nissenbaums teori pekar på värdet att gå från en statisk teknik- och uppgiftsfokusering till en värdering utifrån hela processen för informationshantering. Julia Branting ger i sitt kapitel två konkreta exempel på hur teorin kan användas för en mer kvalificerad typ av avvägning än den schablonmässiga och hur utfallen skiljer sig.

Självcensur och demokratins självmål

Det stora problemet är kanske inte att de enskilda besluten kan ifrågasättas. Det är något som alltid kommer att kunna vara fallet, oberoende av vilken metod för avvägning som används. Istället är det den samlade oavsedda effekt som kan uppstå på samhällsnivå som tornar upp sig. President Obamas granskningsgrupp tar upp samma risk som EU-domstolen skriver om i sitt utslag om datalagringsdirektivet, nämligen att medborgarna kan komma att ålägga sig självcensur och begränsa sin användning av elektronisk kommunikation av fruktan för övervakning. Effekten är inte bara att teknikens effektivitetsvinster riskerar att reduceras. Självcensur skulle framförallt innebära att yttrandefriheten och i förlängningen demokratin undermineras. Den preventiva effekt som många mer begränsade brottsförebyggande övervakningssystem strävar efter att uppnå skulle här kunna uppstå på samhällsnivå och leda till en pacificering av medborgarna av samma slag som i totalitära system. Medborgarna skulle då i överförd mening börja söka efter den eventuella döda vinkel som Winston Smith tror sig ha hittat i alkoven i sin lägenhet. Att dessa frågor på allvar börjat diskuteras i post-Snowden debatten är en indikation på att detta slags demokratins självmål inte är en fråga om hypotetiska dystopiska framtidsvisioner.

Referenser

Cole, David (2014) ”We Kill People Based on Metadata”, *New York Review of Books Blog,* 10 maj.

Electronic Surveillance and Civil Liberties (1985) Washington*:* Office of Technology Assessment.

Liberty and Security in a Changing World (2013) Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 12 december.

Om författarna

Håkan Hydén är seniorprofessor i Rättssociologi vid Lunds universitet och ledamot av The World Academy of Arts and Sciences

Janne Flyghed är professor i kriminologi vid Stockholms universitet.

Julia Branting är Malmö Stads förre chefstrateg.

Marcin de Kaminskin är doktorand i rättssociologi vid Lunds universitet och nätforskare vid Lunds universitets Internetinstitut. Han är även ämnesföreträdare för yttrandefrihet/ICT vid Sida.

Per Gustafson är säkerhetschef vid Lunds universitet med trettio års erfarenhet av att arbeta med säkerhetsrelaterade frågor. Han är även doktorand i sekuritetshantering och initiativtagare till att etablera ett säkerhetsvetenskapligt centrum vid Lunds universitet för såväl grundutbildning som forskning i syfte att utveckla och akademisera sekuritetsområdet.

Petrus Bolin är koncernsäkerhetschef på Handelsbanken, före detta polis och med femton års erfarenhet som säkerhetschef inom både detaljhandel och bank.

Markus Lahtinen och Benjamin Weaver är båda forskare inom LUSAX-gruppen på Institutet för ekonomisk forskning vid Lunds universitet. De studerar där de övergripande effekterna av digitalisering på den fysiska säkerhetsbranschen.

Markus Naarttijärvi är universitetslektor vid juridiska institutionen på Umeå universitet. Han disputerade i rättsvetenskap 2013 på en avhandling om konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel.

Tobbe Petterson är lärare och forskare i underrättelseanalys vid Lunds universitet.

Wilhelm Agrell är författare och professor i underrättelseanalys vid Lunds universitet.