Nya aktörer och ny teknik i kontrollandskapet[1]

> *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[2], 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

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

2 Se t.ex. Säkerhetskommissionen 2003:87-95 samt Flyghed 2011.

personliga integriteten;[3] 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 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 2006,31). 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 2009,23).

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 2007:4). 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 2003:68). 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 2009,19). 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

3 Angående definitionsproblematiken kring personlig integritet se Branting i denna volym.

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 2009,150-51).

En kontrollteknologisk förändring som påbörjade långt innan 11 september 2001, är den explosionsartade ökningen av övervakningskameror, 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.[4] Till kameranyheterna hör utvecklandet av 3D-bilder. Detta är möjligt genom att låta två parallella kameror ta bilder, Biometric Optical Surveillance System (BOSS) (Keenan 2014,31). 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” (Ibid.).

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, 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.

4 Den brottspreventiva effekten av Closed Circuit TeleVision (CCTV), motivet till att de från början sattes upp, har starkt ifrågasatts. (För Sverige se t.ex. BRÅ 2012 och 2014.) 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. Enligt en intern rapport från Metropolitan Police 2009, bidrog CCTV till att lösa ett brott per 1000 kameror och år (Hughes 2009). David Davis (former shadow Home Secretary) kommenterade rapporten på följande vis: ”It should provoke a major and long overdue rethink on where the Home Office crime prevention budget is being spent. CCTV leads to massive expense and minimum effectiveness. It creates a huge intrusion on privacy, yet provides little or no improvement in security” (Ibid.).

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.[5]

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 2007,5). 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 2014,13,120).

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

5 Omfattande insamling och lagring av information sker även hos operatörer som Google, Facebook, Yahoo m.fl. (Se vidare Cleland & Brodsky 2012 och Keenan 2014:32ff.). En närmare belysning av hur dessa bl.a. kommersiellt exploaterar insamlade bilder m.m. faller dock utanför ramarna för denna framställning. För en studie av sociala medier som kontroll, se Trottier 2015, särskilt kap.3-5.

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 2003,78f.; Andersson 2007; SOU 2012:44,223f.). 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” (Ibid.:48) som riskerar att ”´infiltrera´ det lagliga samhället” (Ibid.: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.[6] 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 2000:47-69).

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 o annan lagstiftning	
Säkerhets -industrin	Effektiv kontrollav 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

6 De 5 aktörerna är inte rangordnade eller viktade på något sätt. Se vidare Flyghed 2007.

				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 1996:370ff). En sådan organisationsrationalitet är inget unikt för polisen utan gäller alla byråkratier (Emsley 1997:2).

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.[7] 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.

7 Se Mueller 2006 för en beskrivning av orons betydelse i dessa sammanhang.

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 hamnar sådan verksamhet främst under rubriken Forensic.[8] 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 2011:1). Även Securitas tillhör de större med en verksamhet i 40 länder och med drygt 240 000 anställda (Ibid.:26). I Sverige har G4S och Securitas omkring 4000 respektive 9000 anställda (Berndtsson & Stern 2011:409). 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 2011:41).

8 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.

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 2009:177-178; Arwinge 2015:39f). 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.[9] 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.

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

9 Om inte annat sägs är uppgifterna i detta avsnitt hämtat från Flyghed 2014.

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 1997:206).

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 2000:183).

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[10] 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[11].

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 2012:61ff). O´Reilly och Ellison nämner hur McDonalds använt privata säkerhetsföretag för att infiltrera och delta i protestgruppers möten (O´Reilly & Ellison 2006:648). 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

10 ”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/.

11 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 2009,64). 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).

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 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 2013:295).

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. Säkerhetschefen för Jernhusen AB, Leif Svensson, anklagade Datainspektionen (DI) för att inte respektera brottsoffrens integritet då DI överklagat ett antal beviljade tillstånd att sätta

upp övervakningskameror.[12] ”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 140505).[13] 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.

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.

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

13 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 (Rapport 2014:12) av kameraövervakningen på Stureplan och Medborgarplatsen och som visade högst marginella effekter av övervakningskameror.

Litteratur

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 2008:8. *Otillåten påverkan mot brottsoffer och vittnen*, Stockholm: Brottsförebyggande rådet.

Brå 2013:13. *Kameróvervakning på Stureplan och Medborgarplatsen*, Stockholm: Brottsförebyggande rådet.

Brå 2014:12. *Kameróvervakning på Stureplan och Medborgarplatsen. Delrapport 2*, Stockholm: Brottsförebyggande rådet.

Cleland, S & Brodsky, I (2012) *Search & Destroy. Why we can´t trust Google Inc*, Telescope books.

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, pp.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* 140505.

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. S. 73-97 i Flyghed, J & Hörnqvist, M (red) (2003): *Laglöst land. Terroristjakt och rättssäkerhet i Sverige*, Ordfront förlag.

Flyghed, J (2007): Kriminalitetskontroll – baserad på tro eller vetande? *Svensk Jurist Tidning*, 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, pp. 203-220 in *Commissions of Inquiry and National Security: Comparative Approaches*, Stuart Farson and Mark Phythian (eds.). Praeger/ABC-CLIO.

Flyghed, J (2014) Privat område? Revisionsbyråers och säkerhetsföretags polisarbete, s.131-146 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* 2/2009,76-82.

Green, A. (2013) Skanskas ursäkt pr-strategi, *Arbetaren* nr.42/2013 s.6.

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

Hughes, M (2009) "CCTV in the spotlight: one crime solved for every 1000 cameras", *The Independent*, 25 August 2009. http://www.independent.co.uk/news/uk/crime/cctv-in-the-spotlight-one-crime-solved-for-every-1000-cameras-1776774.html#

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, pp. 177-200 in Sheptycki, James (ed.) *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, pp.641-660.

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

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* 140429.

Trottier, D. (2015) *Social Media as Surveillance. Rethinking Visibility in a Converging World*, Ashgate.

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 2005, pp187-211.