Olle Abrahamsson

Kriminalitetsbekæmpelse og integritet

Kriminalitetsbekæmpelse og integritet

Rättschef *Olle Abrahamsson,* Justitiedepartementet, Sverige[1]

Till värdegemenskapen mellan de nordiska länderna hör uppfattningen att staten inte bara skall tillförsäkra medborgarna fred och frihet utan också ta ett övergripande ansvar för deras välstånd och trygghet. I samhällen som i första hand strävar efter att tillgodose medborgarnas behov av välstånd och att skydda dem mot brott, kan värnet av allas rätt till personlig integritet inte samtidigt ges högsta prioritet. Väsentligt är emellertid att behovet av en effektiv brottsbekämpning inte tillåts inskränka medborgarnas privata sfär mer än nödvändigt. I detta avseende finns åtskillig kritik att rikta mot den svenska lagstiftningen och de motiv som bär upp denna. Dessvärre har debatten om effektivitet i brottsbekämpningen kontra ett godtagbart integritetsskydd alltför mycket kännetecknats av brist på analys och rationella överväganden, både från deras sida som hävdar att ett demokratiskt samhälle har rätt att ta till i princip alla medel för att försvara sig mot sina fiender och från dem som menar att demokratin vittrar sönder inifrån om den tillåter sig att bekämpa brottsligheten med odemokratiska metoder. I referatet framställs fyra teser som, om de tas ad notam av lagstiftaren, kan bidra till att bättre än i dag tillgodose både behovet av effektivitet i brottsbekämpningen och skyddet för den personliga intregriteten.

1. Generell övervakning och kontroll är från integritetsskyddssynpunkt mer problematisk än åtgärder som sätts in vid misstanke om brott.

Hemlig rumsavlyssning (buggning) har sedan tidigare varit tillåtet i Danmark och Finland och har nyligen införts som straffprocessuellt tvångsmedel också i Norge och Sverige. Det har skett under viss vånda och till ackompanjemang av högljudda protester. Kritikerna har visserligen ofta bejakat polisens behov av effektiva hjälpmedel och metoder i kampen mot den grova och organiserade brottsligheten men invänt att buggning i alltför hög grad kränker rätten till personlig integritet, särskilt för oskyldiga som råkar befinna sig på fel plats. Till och med en normalt så återhållsam instans som Riksdagens Justitieombudsman (JO) tog i ett remissyttrande i december 2005 skarpt avstånd från den svenska regeringens lagförslag i ämnet. JO framhöll att buggning är ett utomordentligt långtgående ingrepp i den enskildes integritet och lade i sitt yttrande särskild vikt vid den misstänksamhet som kan uppstå hos allmänheten på grund av blotta vetskapen att polisen får använda sig av buggning. Att döma av flera opinionsundersökningar som gjordes vid denna tid synes misstänksamheten dock ha varit begränsad; i genomsnitt ansåg ca 90 procent av de tillfrågade att polisen borde ges rätt att bugga.

[1] Rättschef i Justitiedepartementet och ordförande i 2004 års parlamentariska integritetsskyddskommitté.

Vid ungefär samma tid aktualiserades i Sverige frågan huruvida Försvarets radioanstalt (FRA) skulle ges rätt att bedriva så kallad signalspaning via tråd och kabel. Regeringen föreslog en lagreglering som innebar en kraftig ökning av FRA:s tillgång till integritetskänslig information. I princip all tele- och internetkommunikation som passerade landets gränser skulle enligt förslaget kunna fångas upp och analyseras av myndigheten. Några garantier för att inrikes trafik, t.ex. i form av vanliga lokala telefonsamtal eller e-postmeddelanden, inte skulle komma att avlyssnas eller avläsas gavs inte. Tvärtom framgick av förslaget att det i praktiken inte skulle vara möjligt att sortera bort inrikes trafik från gränsöverskridande sådan.

Jämfört med propositionen om buggning väckte förslaget om utvidgad signalspaning liten uppmärksamhet. Remissinstanserna ansåg i allmänhet inte att hänsynen till skyddet för den personliga integriteten utgjorde något hinder för det senare förslaget. Medierna, som i buggningspropositionen nära nog hade sett det totala övervakningssamhället på väg att förverkligas, intresserade sig till en början inte nämnvärt för regeringens ungefär samtidigt presenterade förslag om att FRA skulle ges rätt att tappa inte bara etern utan också signalkablar på information. Om reaktionerna hade grundats på överväganden utifrån respektive förslags samlade skadeverkningar med avseende på den personliga integriteten, borde utfallet enligt min mening ha blivit det omvända. Från integritetsskyddssynpunkt borde alltså förslaget om buggning ha varit lättare att acceptera än förslaget om utvidgad signalspaning. Jag skall förklara varför.

Å ena sidan har vi att göra med ett hemligt processuellt tvångsmedel, buggning, som får tillgripas endast i fall då någon är misstänkt för ett grovt brott. För polisen är buggning mycket resurskrävande och av logistiska skäl ofta svår att genomföra. Arbetsmetoden kräver ett omfattande förspaningsarbete, teknisk utrustning och specialutbildad personal. Domstol måste i varje särskilt fall först ge sitt tillstånd, och verksamheten granskas i efterhand av en särskild nämnd med parlamentariska inslag. Under sådana premisser är och förblir buggning en ganska marginell företeelse i den polisiära verksamheten. Den inhämtade informationsvolymen är relativt liten och antalet drabbade personer högst begränsat. I själva verket synes den vanlige medborgaren inte ha någon rationell anledning att oroa sig för att han skall bli hemligt avlyssnad av polisen. Risken för att han någonsin kommer att få sin integritet kränkt på grund av buggning bör från hans synpunkt framstå som i det närmaste försumbar.

På den andra sidan står en verksamhet, signalspaning, som omfattar enormt stora informationsmängder och som möjliggör hemlig avlyssning av praktiskt taget landets hela befolkning. Beslut av domstol behövs inte och inhämtning får ske alldeles oberoende av om det finns brottsmisstankar eller inte. Telefonsamtal kan avlyssnas, in- och utgående e-post kan avläsas och det är möjligt att exakt följa vilka webbsidor en Internetanvändare besöker. Naturligtvis har FRA varken resurser eller intresse av att övervaka och kartlägga vad varje medborgare har för sig, men för bedömningen av verksamhetens samlade integritetsskadliga effekter är detta förhållande inte avgörande. Redan existensen av ett system som tillåter hemlig avlyssning utgör ett hot

mot dem som träffas av lagstiftningen, framhöll Lagrådet i sitt yttrande över förslaget och fortsatte: ”Detta hot slår med nödvändighet mot den frihet att kommunicera som bör finnas mellan människor som använder telekommunikationstjänster. Det utgör därför i sig själv ett intrång i såväl privatliv som korrespondens”.

De båda exemplen ger stöd för att bedömningen av en åtgärds integritetsinskränkande verkan bör ta sin början hos den enskilda människan. Lagstiftaren riskerar att komma till felaktiga slutsatser om han inte i främsta rummet ställer frågan vad den ordinäre samhällsmedborgaren har anledning att bekymra sig för i sin vardag. Om man tar den frågan som utgångspunkt inser man också att åtgärder som generellt inskränker den privata sfären och som därmed berör hela eller stora delar av ett lands befolkning, får mer djupgående negativa återverkningar, inte minst på det folkpsykologiska planet, än åtgärder som sätts in enbart vid misstanke om att brott har begåtts eller i varje fall kommer att begås.

Ytterligare två exempel skall ges för att visa på skillnaden mellan å ena sidan riktad övervakning och kontroll samt å andra sidan generell kartläggning av befolkningen som helhet. Under den lagstiftningsmässigt dynamiska tiden kring år 2005 diskuterades i Sverige ett förslag som innebar att polisen skulle ges möjlighet att använda hemlig teleavlyssning, hemlig kameraövervakning och postkontroll i brottsförebyggande syfte. Förutsättningen var att det fanns anledning anta att en person skulle begå ett allvarligt brott av visst angivet slag samt att en domstol i varje särskilt fall medgav att det aktuella tvångsmedlet skulle få användas. Förslaget, som numera har resulterat i lagstiftning, angreps häftigt av dem som ville försvara integritetsskyddsintresset. Exempelvis framhöll Justitiekanslern (JK) att det var fråga om en mycket ingripande lagstiftning som innebar ett stort avsteg från grundläggande rättsprinciper. Tillsammans med ett flertal andra remissinstanser tog JK avstånd från förslaget. I medierna beskrevs förslaget som ett stort och ödesdigert steg på vägen mot Storebrorssamhället.

Det uttalade syftet med förslaget var att ge polisen ytterligare ett verktyg i kampen mot terrorism, spioneri och annan allvarlig, ofta systemhotande brottslighet, som äventyrar stora samhällsvärden och utgör ett hot mot enskilda människors liv och hälsa. Den föreslagna nya möjligheten att begagna hemliga tvångsmedel skulle alltså ingalunda tillgripas vid alldagliga eller mer ordinära former av brottslighet utan vara reserverat för en ganska exklusiv kategori av mycket allvarlig kriminalitet. De personer som drabbades skulle naturligtvis kunna åsamkas integritetsförluster, till och med svåra sådana. Från den vanlige medborgarens perspektiv måste emellertid varje rimlig och rationellt grundad bedömning ha talat emot att han själv eller någon närstående skulle råka ut för en integritetsförlust på grund av tvångsmedelsanvändning i förebyggande syfte.

Det andra exemplet, som jag vill ställa i kontrast mot det förra, avser EG-direktivet om lagring av trafikuppgifter, som antogs våren 2006 och som skulle ha varit genomfört i medlemsstaterna den 15 september 2007. Även Norge och Island kommer sannolikt att införa motsvarande lagstiftning. Medlemsstaterna skall enligt

direktivet ålägga teleoperatörerna att lagra alla uppgifter om meddelanden som överförs via fast och mobil telefoni, Internettelefoni och Internetbaserad e-post och om Internetåtkomst. Det innebär en kraftigt utökad skyldighet för operatörerna, eftersom de i dag åläggs en sådan skyldighet endast i de relativt fåtaliga fall då en domstol ger tillstånd till hemlig teleövervakning. Enligt direktivet skall däremot samtliga teletrafikuppgifter sparas i upp till två år. Alla användare av Internet och av fast och mobil telefoni kommer att beröras. Några undantag för t.ex. samtal som omfattas av tystnadsplikt och källskydd kommer inte att ges. Inte heller kommer det att gälla något krav på att brott har begåtts eller att det skall finnas en skäligen misstänkt person.

Det är uppenbart att direktivet och den därpå grundade nationella lagstiftningen kommer att förstärka den känsla som många redan har av att leva i ett övervakningssamhälle. Vetskapen om att information om i princip varje medborgares strängt privata angelägenheter kontinuerligt lagras och görs tillgänglig för myndigheterna kommer att ge upphov till en frätande ovisshet om vad som sker med denna information, nu och i framtiden. Många kommer att oroas över att en så kraftigt ökad informationsvolym hos teleoperatörerna också innebär större risk för läckage av känsliga uppgifter till obehöriga och för så kallad ändamålsglidning, dvs. att informationen småningom används för något annat samhällsnyttigt ändamål än den varit avsedd för.

Den dag lagstiftningen träder i kraft och det står klart för medborgarna vad den innebär för dem personligen kommer deras beteendemönster att förändras. I stället för att koppla upp sig på sin egen dator kommer många av försiktighetsskäl att anlita webbcaféer och datorer på bibliotek. Somliga kommer att undvika att tala med vissa personer per telefon. E-postmeddelanden som är känsliga i förhållande till chefer eller närstående, blir kanske inte längre skrivna och postade när det blir allmänt känt att alla uppgifter om e-posttrafiken lagras för att vid behov tas fram och undersökas närmare.

De psykologiska och attitydskapande effekterna av den direktivbaserade lagstiftningens föreskrifter om skyldighet att lagra datatrafikuppgifter kan förväntas bli långt mer omfattande än effekterna av de förut nämnda reformerna på tvångsmedelsområdet – buggning samt hemlig tvångsmedelsanvändning i preventivt syfte – vilka den vanlige medborgaren saknar grundad anledning att bekymra sig för. Ändå ifrågasattes trafikdatalagringsobligatoriet, som Sverige tillsammans med tre andra medlemsstater tog initiativ till inom EU, nästan inte alls från integritetsskyddssynpunkt medan det ännu fanns tid att påverka direktivets innehåll. Den huvudsakliga förklaringen tror jag är en bristande insikt i hur skadliga generella övervaknings- och kontrollåtgärder är från integritetsskyddssynpunkt. Sådana åtgärder är i själva verket till sin typ långt allvarligare än åtgärder som, även om de är skarpa och djupt integritetskränkande i det enskilda fallet, kommer till användning endast när det finns en specifik misstanke om brott.

För att undvika missförstånd bör tilläggas att jag är väl medveten om att lagringsobligatoriet av tele- och datatrafikuppgifter kan bli ett förnämligt hjälpmedel i

den brottsbekämpande verksamheten. Redan i dag, när teleoperatörerna av debiteringsmässiga skäl sparar vissa uppgifter, har polisen tack vare detta i åtskilliga fall kunnat förhindra planerade terroristangrepp och ingripa mot människosmuggling, tvångsprostitution, narkotikahandel och annan grov organiserad kriminalitet, som på senare år gynnats av att gränskontrollerna inom EU till stor del har upphört. Hänsynen till brottsoffren är ett utomordentligt relevant skäl för att tvinga teleoperatörerna att undantagslöst lagra trafikuppgifter. Jag ifrågasätter heller inte detta, utan vill endast framhålla att de integritetsskadliga effekterna härav har underskattats samt rikta fokus på det allmänt sett föga uppmärksammade spörsmålet om vad som är värst från integritetsskyddssynpunkt: generell övervakning, kontroll och kartläggning eller åtgärder som sätts in enbart när syftet är att avslöja eller förhindra ett brott. Det är en allvarlig brist i den politiska beslutsprocessen att sådana överväganden ofta inte finns med vid bedömningen av vilka brottsbekämpande åtgärder och metoder som bör vara tillåtna och vilka begränsningar som bör gälla för verksamheten.

2. En integritetsinskränkning uppkommer i och med att känslig information om individen *görs tillgänglig* för polisiära eller andra myndigheter, inte först när informationen utnyttjas. Staten bör därför vara restriktiv med att inhämta känslig information, men när informationen väl är tillgänglig bör den utnyttjas på ett brottsbekämpnings-effektivt sätt.

En gängse utgångspunkt för lagstiftningen är att myndigheterna har rätt att inhämta uppgifter om den enskildes privata förhållanden om det behövs för verksamheten men också en skyldighet att se till att informationen inte missbrukas. Informationen får inte i hamna i orätta händer och inte heller användas för andra ändamål än den var tänkt för. Myndigheterna har givits rätt att samla in en stor mängd individanknuten information samtidigt som ändamålsbestämmelser och restriktiva hanteringsregler avsetts ge tillräckligt skydd åt medborgarnas privata förhållanden. Så länge den känsliga informationen inte når längre än till behöriga personer inom myndigheten eller till andra personer som är bundna av tystnadsplikt, anses inte någon integritetsförlust ha skett. Detta synsätt är djupt rotat men kan ifrågasättas både från effektivitets- och integritetsskyddssynpunkt. Jag skall ge några i sig banala men belysande exempel.

Polisen för sedan 1992 ett anmälningsregister, där uppgifter om bland annat namn på misstänkta personer införs i takt med att anmälda brott utreds. Registret innehåller stora mängder information, däribland uppgifter om personer som aldrig blivit dömda för det som de var misstänkta för. I kampen mot grov och organiserad brottslighet skulle det innebära en stor vinst för polisen om registret fick användas i underrättelseverksamheten och samköras mot andra dataregister. Ett så vidsträckt bruk av anmälningsregistret är emellertid till följd av den av integritetshänsyn uppburna lagstiftningen inte tillåtet. Redan personuppgiftslagens grundläggande krav på att varje behandling av en personuppgift skall vara nödvändig för det tänkta ändamå-

let utesluter möjligheten att ge polisen carte blanche att fritt förfoga över registeruppgifterna, och sekretesslagstiftningen hindrar att uppgifterna samkörs med andra myndigheters register utan att en sekretessprövning har gjorts i varje särskilt fall. Polisen har inte heller fått lov att kopiera informationen till det vanliga kriminalunderrättelseregistret, eftersom Datainspektionen sagt nej med hänvisning till integritetsskyddsriskerna.

Situationen kan alltså beskrivas så, att information som polisen lagenligt har inhämtat inte får användas på effektivast möjliga sätt i den brottsutredande verksamheten. En effektiv användning av den inhämtade informationen kommer nämligen i konflikt med bestämmelser som syftar till att ge skydd för den personliga integriteten. Någon integritetsskyddskonflikt har däremot inte ansetts uppkomma vid själva inhämtandet av informationen, när det sker för ett i lagstiftningen godkänt ändamål.

Ett annat exempel avser det förhållandet att Skatteverket samlar in en mängd uppgifter om skattskyldiga, för övrigt även uppgifter om förmögenhetsinnehav och annat som strängt taget inte behövs för den fiskala verksamheten. I många fall kan Skatteverket tydligt se att om Försäkringskassan hade tillgång till uppgifter som finns hos verket skulle felaktiga utbetalningar av sjukpenning och andra bidrag förhindras, exempelvis när det av uppgifterna framgår att en bidragstagare inte längre vistas i landet. Ändamålsbestämmelser i sekretesslagen, vilka tillkommit för att skydda den personliga integriteten, förbjuder emellertid Skatteverket att självmant förse Försäkringskassan med uppgifter vid misstanke om bidragsfusk. Kassan kan visserligen på begäran få ut uppgifterna i enskilda fall, men det är tidsödande och ineffektivt jämfört med om man utan eget initiativ försågs med underrättelser om misstänkta oegentligheter. I praktiken innebär detta att ett omfattande bidragsfusk, som i många fall uppfyller kriterierna för bedrägeri och årligen uppgår till mångmiljardbelopp, kan fortgå år efter år utan att myndigheterna kan göra mycket åt saken.

Jurister förtrogna med EU:s dataskyddsdirektiv och den nationella data- och sekretesslagstiftningen ser förmodligen ingenting i grunden konstigt med dessa konsekvenser. Direktivet, som visserligen formellt inte gäller på EU:s straffrättsliga och polisiära samarbetsområden, bärs ju upp av gemensamma europeiska värderingar vilka också återspeglas i Europakonventions krav på att staterna får inskränka medborgarnas rätt till respekt för privatlivet bara när detta är ”nödvändigt” (artikel 8). Från denna synpunkt sett skulle en generell möjlighet att utbyta information myndigheter emellan inkräkta på det integritetsskydd som nödvändighetskravet är avsett att garantera. Detta gäller även om informationsutbytet begränsas till att avse endast de brottsbekämpande myndigheterna inbördes. Ett radikalt förslag i den riktningen, i form av en allmänt hållen sekretessbrytande bestämmelse inom brottsbekämpningen, lades för några år sedan faktiskt fram i ett utredningsbetänkande (SOU 2005:117) men fick kritik under remissbehandlingen och har inte föranlett lagstiftning.

I stort sett förefaller det råda enighet både på det politiska planet och inom juristkåren om att gällande sekretesslagstiftningen skapar en balans mellan effektivitet

och integritet, på så sätt att den dels ger tillräckliga möjligheter till informationsutbyte inom och mellan myndigheter, dels är tillräckligt restriktiv för att uppfylla dataskyddsdirektivets och personuppgiftslagens krav på nödvändighet. Men integritetsskyddsdiskussionen har nästan helt och hållet gällt frågan om hur den hos myndigheterna tillgängliga informationen får behandlas, inte det förhållandet att informationen alls görs tillgänglig för myndigheterna.

Uppfattningen att den personliga integriteten utsätts för fara först när en myndighet *begagnar sig av* inhämtad information om medborgarna är både grundmurad och vitt utbredd. Det är inte bara det allmänna som resonerar i dessa banor utan också företrädare för det civila samhället. Man ser påfallande ofta hur intresseorganisationer, medier och enskilda debattörer under åberopande av integritetsskyddsintresset kräver att myndigheterna skärper sina interna rutiner så att inte känslig individrelaterad information missbrukas eller kommer på avvägar, medan man däremot utan vidare godtar att informationen görs tillgänglig för myndigheten.

Enligt min mening är detta allmänna synsätt grundat på en otillräckligt insikt om vad som konstituerar en integritetsinskränkning. Den avgörande inskränkningen inträffar redan när informationen görs tillgänglig för staten. Från den tidpunkten har den medborgare som informationen rör, förlorat kontrollen över hur denna i fortsättningen kommer att användas. I varje ögonblick härefter måste medborgaren räkna med möjligheten att informationen kan komma att utnyttjas och att det kan ske när som helst. Han kan inte heller utesluta att informationen används för andra ändamål än den varit avsedd för.

Vetskapen om att någon annan människa kan komma att ta del av informationen utgör i sig en integritetsbegränsning och en mycket påtaglig sådan. Det spelar härvid inte någon roll om den människan är en behörig företrädare för en myndighet eller inte. Min personliga integritet kan kränkas lika mycket genom att en åklagare eller en domare läser sekretessbelagda handlingar om mig som genom att en närstående eller obekant person utan lov gör samma sak. När en människa ständigt måste hålla i minnet att känslig information om henne finns tillgänglig hos myndigheterna, har hon i själva verket redan till stor del intecknat den ytterligare integritetsförlust som uppkommer om och när informationen sedan verkligen utnyttjas.

Om min tes stämmer, att den avgörande integritetsförlusten uppkommer redan när känsliga uppgifter inhämtas oavsett ändamålet, bör det få till konsekvens att den information som gjorts tillgänglig hos myndigheterna i större utsträckning än i dag används i den brottsbekämpande verksamheten. Utbyte av information bör i högre grad tillåtas både mellan och inom myndigheter och polisen bör ha rätt att använda tillgängliga arkiv och register både i utrednings- och spaningsverksamhet. Samkörning av registerdata bör oftare få ske som ett led i kampen mot grov brottslighet men också för att stävja sådant som skatte- och bidragsbedrägerier. En från integritetsskyddssynpunkt positiv sidoeffekt av att redan inhämtad information utnyttjas i högre grad än tidigare skulle bli att polisen inte lika ofta behöver ansöka om att få använda hemlig teleavlyssning eller andra integritetsbegränsande tvångsmedel.

En radikal omläggning av rådande system, ett ”paradigmskifte”, är en utopi. Men redan ett måttligt ökat utnyttjande av sådan information om medborgarna som redan finns tillgänglig för myndigheterna stöter på problem. Dels sätter inom sitt tillämpningsområde dataskyddsdirektivet och ytterst även Europakonventionen gränser för ett utvidgat bruk av befintlig information. Dels är det ingen enkel sak att förändra synen på en nationell sekretessreglering som enligt de flestas åsikt innefattar en någorlunda god balans mellan effektivitets- och integritetshänsyn. Under inga förhållanden får det tillåtas att integritetsskyddet försvagas, sett till den samlade effekten. Mer generösa regler om informationsanvändning måste därför balanseras, inte i första hand genom nya ändamålsbestämmelser utan genom en minskning av den totala volymen känsliga personrelaterade uppgifter som görs tillgänglig för myndigheterna.

Det är tydligt att system vilkas själva idé är att kolossala mängder integritetskänslig information görs tillgänglig för myndigheterna medan bara en liten bråkdel härav utnyttjas i brottsbekämpningen, passar dåligt in i den här skisserade omläggning av synen på vad som utgör en integritetskränkning. Exempel på system som inte passar in utan går i rakt motsatt riktning är det förut nämnda EG-direktivbaserade trafikdatalagringsobligatoriet och FRA:s föreslagna möjlighet att signalspana via kabel. I båda fallen är poängen att enorma informationsmängder görs tillgängliga i fullt medvetande om att den alldeles övervägande delen av materialet fullkomligt saknar intresse för myndigheterna och aldrig någonsin kommer att användas i brottsbekämpningen. I båda fallen saknas dessvärre också insikt om de omfattande integritetsskador som blir följden av den sortens massövervakning och storskalig kartläggning av ett lands hela befolkning.

3. Allmän kameraövervakning och DNA-registrering är exempel på metoder som är kostnadseffektiva och som få människor upplever som integritetskränkande. Metoder som dessa bör därför användas mer i den brottsbekämpande verksamheten.

I Sverige har integritetsskyddsdebatten till betydande del ägnats frågan i vad mån buggning bör vara tillåten och under vilka förutsättningar teleavlyssning och andra hemliga tvångsmedel bör få användas i den polisiära verksamheten. Denna debatt har varit principiellt intressant och väl på sin plats, eftersom användning av hemliga straffprocessuella tvångsmedel kan innebära djupgående integritetsförluster för dem som drabbas. Verksamheten är emellertid förenad med åtskilliga svårigheter och mycket resurskrävande, bland annat behöver specialutbildad personal tas i anspråk, ofta under lång tid. Som förut nämnts kan användningen av de hemliga tvångsmedel redan av det skälet knappast få mer än marginell betydelse i polisens utredande och förebyggande arbete.

Parallellt har det förts en diskussion rörande omfattningen av systemet med fast monterade övervakningskameror på gator och torg och på andra platser där

allmänheten vistas. Denna debatt har följt ungefär samma spår som diskussionen om tvångsmedelsanvändningen. De som av integritetsskäl har varit emot buggning och användning av hemliga tvångsmedel i preventivt syfte har med i stort sett samma argument haft invändningar också mot en utbyggnad av systemet med allmän kameraövervakning. Antalet ansökningar om att få installera kameror på offentliga platser har emellertid stadigt ökat. Som skäl har åberopats sådant som att busschaufförer blivit misshandlade av passagerare, att mobbning förekommit i skolor och sexuella trakasserier i simhallar och att kyrkor blivit plundrade på kollekt och egendom. De myndigheter som har tillsyn och kontroll över verksamheten (länsstyrelserna, Datainspektionen och JK) har emellertid betonat integritetsskyddsaspekterna och intagit en restriktiv hållning till bruket av allmän kameraövervakning.

Inte bara myndigheterna utan också en stor del av landets politiska och intellektuella elit har ställt sig skeptiska till en ytterligare utbyggnad av systemet med allmän kameraövervakning. De som velat framhäva riskerna för den personliga integriteten har inte dragit sig för att åkalla George Orwells framtidsskildring *1984*, där interaktiva teleskärmar övervakar medborgarna vilka framlever sina liv inför ”Storebrors” allseende öga, eller Karin Boyes *Kallocain*, som skildrar ett samhälle där människorna är fråntagna varje möjlighet till privatliv och där kameraövervakning är obligatorisk i varje hem.

Det är intressant att jämföra denna elitistiska negativism med gemene mans inställning till allmän kameraövervakning. Integritetsskyddskommittén som jag var ordförande i, lät häromåret Statistiska centralbyrån utföra en enkätundersökning avseende medborgarnas attityder till bland annat olika integritetskänsliga metoder som används i den brottsbekämpande verksamheten. Undersökningen gav ett entydigt utfall när det gällde användning av allmän kameraövervakning. 97 procent av de tillfrågade ansåg att sådan övervakning bör vara tillåten på allmän plats om det kan förhindra grov brottslighet. 90 procent menade att kameraövervakning bör få ske även om syftet bara är att folk skall känna sig tryggare. Över huvud taget var det tydligt att de tillfrågade uppfattade allmän kameraövervakning som en väsentlig trygghetsskapande faktor i vardagstillvaron.

Inom forskningen finns ingen entydig bild av hur effektiv den icke hemliga kameraövervakningen är i brottsbekämpningens tjänst. De studier som gjorts tycks visa att företeelsen har en avsevärd brottsförebyggande effekt i stadskärnor och parker och på parkeringsplatser, medan resultaten är mindre tydliga och säkra på andra platser (Brottsförebyggande rådets tidskrift Apropå 4/2007). Självfallet har kameraövervakningen härjämte en brottsuppklarande betydelse, även om den sidan av saken inte tycks ha intresserat forskningen i samma utsträckning. Vad som emellertid står klart är att övervakning av offentliga platser med fast monterade och väl skyltade kameror är en effektiv brottsbekämpande metod i förhållande till de kostnader och de personella resurser som krävs.

Allmän kameraövervakning är alltså en kostnadseffektiv metod som en överväldigande majoritet av befolkningen inte upplever som nämnvärt integritetskränkande.

Mot den bakgrunden framstår det som svårbegripligt att utnyttjandet av detta brottsförebyggande instrument och brottsutredande hjälpmedel möter så hårt motstånd. Det kan knappast bero på att allmän kameraövervakning i viss mening kan sägas vara generell till sin natur, om än i så lågintensiv form att människor inte känner sig nämnvärt besvärade av den. Sådana överväganden gjordes knappast ens när frågan gällde de mer högintensiva övervaknings- och kartläggningsformerna obligatorisk trafikdatalagring och FRA:s signalspaning. Också statsmakterna har visat stor försiktighet med att utvidga systemet med kameraövervakning samtidigt som man från det allmännas sida har bedrivit ett energiskt och omfattande rättsligt reformarbete i syfte att på annat sätt ge polisen tillgång till mer integritetskänslig information, bland annat genom ökad användning av hemliga tvångsmedel och just krav på lagring av uppgifter om tele- och datakommunikation.

Sedan några år är det i Sverige tillåtet att i ett register föra in uppgifter om DNA-analyser avseende personer som har dömts till annan påföljd än böter. Det har också gjorts möjligt att i ett nyinrättat utredningsregister föra in analysuppgifter för eventuellt framtida bruk, förutsatt att personen i fråga är skäligen misstänkt för brott på vilket fängelse kan följa. Bakgrunden är att jämförande DNA-analyser har visat sig vara en effektiv och säker metod, användbar både för att klara upp brott och för att avskriva oskyldigt misstänkta och andra ovidkommande personer från brottsutredningar. Reformen går längre än vad som är tillåtet enligt Europarådets rekommendation i ämnet och bemöttes med åtskillig kritik. Advokatsamfundet menade i sitt remissyttrande över den utredning som låg till grund för reformen att en korrekt avvägning inte hade gjorts mellan reformens positiva effekter och dess negativa verkningar med avseende på den personliga integriteten. Flera riksdagspartier röstade av integritetsskäl mot regeringens proposition i ämnet.

På samma sätt som beträffande allmän kameraövervakning är motståndet mot en utbyggnad av systemet med DNA-registrering svårt att förklara i den mån det motiveras utifrån hänsyn till de registrerades personliga integritet. En del av förklaringen ligger förmodligen i den ganska vanliga missuppfattningen att de så kallade DNA-profilerna kan användas till annat än identifiering. Det borde emellertid framstå som uppenbart att integritetsförluster som uppkommer i samband med provtagning och användning av analysmaterialet är närmast försumbara vid jämförelse med de positiva effekter som tekniken med registrering av DNA-analyser har visat sig få i brottsförebyggande och i synnerhet i brottsuppklarande hänseende. Härtill kommer att tekniken är kostnadseffektiv och kan bespara många människor obehag och lidande.

Denna bild av DNA-registrering som ett användbart och från integritetsskyddssynpunkt ganska harmlöst verktyg i brottsbekämpningens tjänst stämmer väl överens med medborgarnas allmänna uppfattning i frågan. Endast tre procent av de tillfrågade i den nyss nämnda attitydundersökningen ansåg att brottsmisstänkta personer inte borde DNA-registreras. Över hälften ansåg, måhända något överraskande, att ”även om många människor upplever det som integritetskränkande bör hela befolkningen DNA-registreras”.

Mot denna bakgrund är den relevanta frågan inte så mycket om den nuvarande ordningen med DNA-registrering är godtagbar från integritetssynpunkt utan snarare varför inte registret tillåts bli än mer omfattande. Den samlade effekten av en ytterligare utbyggnad skulle närmast få till resultatet att integritetsskyddet stärktes, dels därför att de mer ingripande hemliga processuella tvångsmedlen skulle behöva utnyttjas i mindre utsträckning, dels därför att ett snabbt och säkert uppklarande särskilt av grövre brott ofta i sig innebär integritetsvinster på flera plan.

Vad som sammanfattningsvis är av vikt är att inte alla integritetspåverkande metoder i brottsbekämpningen skärs över en kam, utan att de så analytiskt och lidelsefritt som möjligt placeras in på en skala som sträcker sig från starkt integritetsskadliga metoder till sådana som är harmlösa från integritetssynpunkt. Denna skala bör sedan jämföras med en som visar graden av olika åtgärders effektivitet och användbarhet från brottsbekämpningssynpunkt, varvid även en sådan faktor som polisens resurstillgång bör vägas in och beaktas. Först då blir det möjligt att på ett rationellt sätt, med tillvaratagande av både brottsbekämpnings- och integritetshänsyn, bedöma vilka metoder som bör prioriteras i den brottsbekämpande verksamheten respektive användas i begränsad utsträckning eller inte alls.

Den framlagda tesen – att brottsbekämpande metoder som är kostnadseffektiva och föga integritetskränkande bör användas mer *et vice versa* – har allmän giltighet och är alltså inte begränsad till exemplen med allmän kameraövervakning och DNA-registrering. Ett exempel av annat slag på vart ett rationellt ställningstagande leder är den situation som uppkommer när valet står mellan att utsätta en misstänkt brottsling för hemlig teleavlyssning och att söka på hans namn i register och arkiv som redan finns tillgängliga hos polisen och hos andra myndigheter. Ett sökande i register och arkiv är som regel mindre integritetskränkande än hemlig teleavlyssning, ändå återspeglas inte detta basala förhållande i lagstiftningen.

4. Proportionalitetsprincipen tillämpas inte på ett korrekt sätt vid integritetsbegränsande lagstiftning på brottsbekämpningsområdet.

Den svenska regeringsformen innehåller i 2 kap. 12 § en uttrycklig proportionalitetsprincip av innebörd att viss rättighetsinskränkande lagstiftning aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Motsvarande princip finns i artikel 8 i Europakonventionen och formuleras där som att vars och ens rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens inte får inskränkas annat än om det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa angivna motstående intressen. Inskränkningar i integritetsskyddet får göras endast om det motstående intresse som skall tillgodoses är så starkt och integritetsskyddsintresset så förhållandevis svagt att inskränkningen framstår som proportionerlig. Ett krav på nödvändighet och proportionalitet vid behandling av personuppgifter genomsyrar också EU:s dataskyddsdirektiv och den på direktivet baserade nationella lagstiftningen.

För att rätt kunna bedöma proportionaliteten av en viss åtgärd krävs självfallet kännedom inte bara om behovet och de positiva effekterna av åtgärden i fråga utan också om de motstående intressena och åtgärdens negativa effekter för dessa. I detta avseende bör sägas att behovet av nya integritetskänsliga brottsbekämpningsåtgärder ofta utreds och redovisas ganska väl av lagstiftaren. Som exempel kan nämnas regeringens proposition 2005/06:178 där det polisiära behovet av att kunna använda buggning belystes på ett bra sätt. Ett genomgående drag i lagstiftningsprocessen är däremot att det saknas noggranna och vederhäftiga redovisningar och analyser av de negativa verkningar från integritetsskyddssynpunkt som lagstiftningen kan medföra.

I de fall då någon som helst beskrivning förekommer av ett lagförslags integritetsbegränsande effekter, framstår denna redogörelse inte sällan som schablonartad och substanslös. Illustrativa exempel på vad en person kan tänkas råka ut för till följd av att integritetsskyddet sätts ur spel lämnas så gott som aldrig. Ett typiskt tillvägagångssätt i de skrivna motiven till lagstiftningen är att fördelarna med en föreslagen integritetsbegränsande åtgärd sammanfattningsvis anges vara så stora att hänsynen till integritetsskyddet måste vika, utan att det närmare förklaras vari integritetsskadorna består och vilka effekter de kan beräknas få till art och omfattning.

Denna summariska metod kan exempelvis ta sig följande uttryck: ”Användande av hemliga tvångsmedel kan i och för sig inkräkta på tredje mans integritetsintresse, t.ex. en person som talar i telefon med en presumtiv gärningsman. De behovs- och effektivitetsskäl på det brottsförebyggande området som talar för förslaget väger emellertid så tungt att tredje mans integritetsintresse i viss mån måste få stå tillbaka i dessa fall” (prop. 2005/06:177).

Men även när beredningsunderlaget i och för sig kan synas vara tillräckligt för att möjliggöra en fullödig proportionalitetsbedömning görs denna ofta – oavsett om termen ”proportionalitet” används eller inte – på ett alltför klichéartat sätt. 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.

Ett nödvändigt moment i en proportionalitetsbedömning är att lagstiftaren undersöker vilka alternativa och mindre ingripande metoder som kan finnas för att uppnå syftet med en föreslagen åtgärd samt därefter omsorgsfullt prövar hur långt det går att komma med sådana alternativa åtgärder, varvid eventuella nackdelar med dessa åtgärder från annat än effektivitetssynpunkt måste beskrivas och värderas. Denna typ av resonemang, som ständigt återkommer i EG-domstolens avgöranden, finns nästan inte alls i motiven till svensk lagstiftning på integritetsskyddsområdet.

De invändningar jag har mött från dem som sysslat med att utarbeta förslag till integritetsbegränsande lagstiftning på brottsbekämpningsområdet är att det är svårt att närmare bedöma och kvantifiera en åtgärds betydelse med avseende på den personliga integriteten, särskilt som de subjektiva upplevelserna av en kränkning kan variera kraftigt. Enligt min mening är dessa svårigheter överdrivna och invändningen ett utslag av brist på ambition och inlevelseförmåga. När förslag till ny lagstiftning

utarbetas bör det vara fullt möjligt att ta fram ett underlag beträffande integritetsskyddet som svarar mot beskrivningen av fördelarna med förslaget. En rad relevanta frågor kan ställas och bli belysta i det sammanhanget: Vad kännetecknar de integritetsförluster som kan uppkomma, dvs. vilken typ av förluster rör det sig om; hur stor är risken för olika kategorier av medborgare att råka ut för integritetsförluster; vilken omfattning kan skadorna väntas medföra; drabbas alla medborgare eller bara de som tillhör en viss grupp; vad kan de tillämpande myndigheterna och medborgarna själva göra för att begränsa respektive skydda sig mot integritetsförlusterna; hur allvarliga är integritetsförlusterna i förhållande till andra integritetsskador?

För att öka graden av konkretion borde lagstiftaren gå ännu ett steg längre och redovisa fallstudier över inträffade eller tänkta intrång i privatlivet. Fallstudier är vanliga för att påvisa de brottsbekämpningsmässiga fördelarna med integritetsbegränsande lagstiftning men förekommer nästan inte alls för att illustrera nackdelarna från integritetsskyddssynpunkt.

Det kan heller inte godtagas att man i lagstiftningsarbetet underlåter att göra och noggrant redovisa proportionalitetsbedömningar med hänvisning att det till sist ändå alltid är lagstiftarens sammanvägda bedömning som avgör. Det sistnämnda är visserligen ett korrekt konstaterande, men genom att pröva idéer och uppkast gentemot proportionalitetsprincipen tvingas lagstiftaren att aktivt och allsidigt tänka igenom sina förslag innan de presenteras, till gagn för kvaliteten i den integritetsbegränsande lagstiftningen. Som professor Mikael Hidén framhöll i sitt referat till ämnet ”Brottsbekämpning och grundrättigheterna” inför Nordiska juristmötet 2005 behöver balanspunkterna mellan integritetsskyddet och andra berättigade intressen ständigt prövas på nytt i en pågående offentlig diskussion. Lösningar ges inte en gång för alla och står heller inte att finna i givna formler, utan det är just genom att ställa och söka svaret på de frågor som följer med proportionalitetsprincipen och dess krav på analys och värdering av argumenten för och emot som de rätta balanspunkterna uppnås – eller konstateras inte ha uppnåtts.

Den tid borde vara förbi, även för svenskt vidkommande, då lagstiftaren på ett självtillräckligt sätt struntar i att redovisa egna proportionalitetsbedömningar med hänvisning till att domstolarna ändå är skyldiga att döma enligt lagen som den är skriven. Denna inställning är desto mindre hållbar som domstolarna och för övrigt också andra rättstillämpande myndigheter kan sätta integritetsinskränkande lagstiftning ur spel genom att hänvisa till proportionalitetsprincipen, en realitet som blivit allt mer påtaglig till följd av europarättens utveckling och ökade genomslag i den nationella rätten. Det borde därför ligga i lagstiftarens eget intresse att utförligt redovisa sina väl grundade överväganden för att härigenom övertyga domstolarna om att en proportionerlig avvägningen har gjorts mellan brottsbekämpnings- och integritetsskyddsintresset.

Frånvaron av proportionalitetsresonemang i lagförarbetena behöver inte betyda att det är något fel på själva lagstiftningen. Men det räcker inte att motstående intressen *är* väl balanserade i lagstiftningen, denna måste också *framstå* som väl balanserad. Det har ett stort värde att lagstiftaren noggrant, uppriktigt och med pedagogisk klarhet re-

dovisar sina skäl och värderingar. I de nordiska länderna bjuder traditionen att dessa överväganden redovisas i förarbeten till lagstiftningen, i första hand i propositioner och utskottsbetänkanden som sin tur kompletteras av det utredningsmaterial som föregår departementsbehandlingen. En betydande del av det motstånd mot integritetsbegränsande lagstiftning, inte minst när det gäller buggning och tvångsmedelsanvändning i brottspreventiv syfte, som kommit till uttryck i den allmänna debatten kan förmodligen förklaras just av att proportionalitetsresonemangen inte har utvecklats tillräckligt väl i motivskrivningarna och därmed också har haft svårt att få genomslag i medierna och i den rättspolitiska diskussionen.

Utan en noggrann redovisning av de proportionalitetsbedömningar som ligger till grund för lagstiftningen försämras också möjligheterna att i efterhand utvärdera lagstiftningen. En korrekt utvärdering måste utgå från de prognoser som vid lagstiftningens tillkomst gjordes beträffande åtgärdernas effektivitet och förväntade inverkan på den personliga integriteten. Om lagmotiven inte innehåller den typen av bedömningar går det inte att senare studera hur väl den faktiska verkan av lagstiftningen uppfyller de mål som uppställdes vid lagstiftningens tillkomst.

5. Sammanfattande teser

a) Generell övervakning och kontroll är från integritetsskyddssynpunkt mer problematisk än åtgärder som sätts in vid misstanke om brott.

Det finns en stor, inte minst folklig förståelse för att de brottsbekämpande myndigheterna behöver använda sig av även kraftigt integritetsinskränkande metoder, såsom buggning och andra hemliga tvångsmedel, för att utreda eller förhindra grova brott som har begåtts eller som misstänks vara under planläggning. Generell övervakning och kartläggning som inbegriper hela befolkningen och vars enda syfte är att inhämta information för eventuellt framtida bruk, riskerar däremot att få djupgående negativa återverkningar och inger medborgarna känslan av att leva i en övervaknings- och kontrollstat.

b) En integritetskränkning uppkommer redan i och med att känslig information om individen görs tillgänglig för polisiära eller andra myndigheter.

Staten bör därför vara restriktiv med att utan samtycke inhämta sådan information. När informationen väl är tillgänglig saknas rationella skäl att inte använda den på ett brottsbekämpningseffektivt sätt. Den ytterligare integritetsförlust som själva användningen innebär är nämligen till stor del redan intecknad och bokförd av den som informationen rör.

c) Allmän kameraövervakning och DNA-registrering är exempel på metoder som endast i mindre grad upplevs som integritetskränkande.

I den allmänna debatten och även från myndigheternas sida har emellertid dessa och andra måttligt integritetsbegränsande metoder på ett olyckligt sätt jämställts med hemliga tvångsmedel, obligatorisk lagring av teletrafikuppgifter och andra mycket

integritetskänsliga metoder som används i brottsbekämpande syfte. Eftersom allmän kameraövervakning och DNA-registrering är relativt harmlösa från integritetsskyddssynpunkt och dessutom effektiva i förhållande till de resurser som krävs för att begagna dem, bör de komma till ökad användning i brottsbekämpningen. Om så sker kan bruket minska av hemliga tvångsmedel och andra mer påtagligt integritetsinskränkande metoder.

d) Proportionalitetsprincipen tillämpas ofta inte på rätt sätt när integritetsbegränsande lagstiftning utarbetas på brottsbekämpningsområdet.

Inskränkningar i integritetsskyddet får göras bara om syftet inte kan uppnås på annat sätt och om vinsterna för den brottsbekämpande verksamheten är så stora och förlusterna för integritetsskyddet så förhållandevis små att inskränkningarna framstår som berättigade. För att bedömningar av denna typ skall kunna göras i lagstiftningsarbetet räcker det inte med utredning om det brottsbekämpande behovet, utan det krävs också fullgod utredning om lagstiftningens negativa verkningar med avseende på den personliga integriteten. I de flesta lagstiftningsärenden saknas emellertid underlag som gör det möjligt att närmare bedöma integritetsskadorna, vilket innebär risk för felaktiga ställningstaganden och äventyrar lagstiftningens trovärdighet.