10 Ljudupptagning, bildupptagning och lokalisering av person

10.1 Bakgrund

10.1.1 Upptagning av ljud

Dold kroppsmikrofon och liknande

Mikrofoner används för att i hemlighet spela in eller för att låta någon annan direkt ta del av samtal som t.ex. en polis själv deltar i. Metoden innebär att någon eller några av de personer som deltar i samtalet är ovetande om inspelningen eller avlyssningen. Metoden ska därför inte förväxlas med olovlig avlyssning enligt 4 kap. 9 a § BrB, där samtliga personer som deltar i samtalet är ovetande om avlyssningen (se även lagen om hemlig rumsavlyssning).

Utrustningen fästs på tjänstemannens kläder eller direkt på kroppen. Det förekommer också att utrustningen bärs av en annan person som den brottsbekämpande myndigheten samarbetar med, t.ex. en målsägande som är utsatt för ett utpressningsförsök. En dold mikrofon behöver inte fästas på kläderna utan kan även bäras i en väska eller monteras i ett rum eller i en bil.

Dold kroppsmikrofon används i högst hundratalet fall årligen, främst i förundersökningar rörande grov organiserad brottslighet. Det finns huvudsakligen tre syften med användningen. Metoden kan utgöra ett skydd för tjänstemannen. Den kan också användas för att den som leder en viss spaningsoperation ska, av rättssäkerhetsskäl eller av operativa skäl, ha möjlighet att följa händelseutvecklingen. Uppgifter som kommer fram vid användning av dold kroppsmikrofon kan vidare användas som underlag för spaning och som bevis inför domstol.

Utrustningen finns endast tillgänglig på ett fåtal platser i landet. Vissa myndigheter har föreskrifter om framför allt beslutsfattandet.

Besluten fattas av högre polischef, exempelvis länskriminalchef eller dennes ställföreträdare efter skriftlig begäran. Besluten liksom användningen av utrustningen dokumenteras.

Säkerhetspolisen har redogjort för en restriktiv användning av kroppsmikrofoner men samtidigt understrukit att kroppsmikrofoner är ett betydelsefullt verktyg för tjänstemän som noggrant behöver dokumentera samtal som de deltar i. Dolda kroppsmikrofoner används också för att förbättra tjänstemännens säkerhet i vissa situationer.

10.1.2 Upptagning av bild

Kikare

Kikare används i stor omfattning i de brottsbekämpande myndigheternas spaningsverksamhet.

Handmanövrerad kamera

Övervakning med kamera kan ske genom användning av fjärrmanövrerade kameror. Sådan övervakning är reglerad i lagen (1998:150) om allmän kameraövervakning och i 27 kap. RB om hemlig kameraövervakning (jfr även lagen om åtgärder för att förhindra vissa särskilt allvarliga brott). Övervakning kan också ske genom s.k. handmanövrerad kamera. Den sistnämnda metoden är inte lagreglerad. Den lagstiftning som reglerar behandling av personuppgifter begränsar dock i viss utsträckning den praktiska användningen av digitala kameror (se avsnitt 3.1.6).

Det kan också nämnas att det i 28 kap. 14 § RB finns bestämmelser om att den som är anhållen eller häktad bl.a. kan fotograferas och videofilmas. Närmare bestämmelser finns i förordningen (1992:824) om fingeravtryck m.m. Även annan person än den som är anhållen eller häktad får filmas på det sättet, om det behövs för att utreda ett brott på vilket det kan följa fängelse (jfr JO 1999/2000 s. 91). De nu nämnda åtgärderna ska alltid ske öppet i förhållande till den enskilde.

Det är mycket vanligt att de brottsbekämpande myndigheterna använder sig av filmning med handmanövrerad kamera i en spaningsoperation, oavsett om det sker i förundersökning eller i underrättelseverksamhet och oberoende av brottslighetens svårhetsgrad.

Metoden kan i stort sett inte planeras utan måste situationsanpassas. Oftast filmas enskilda misstänkta och personer som dessa träffar. Även filmning in i eller strax utanför bostäder eller andra privata utrymmen förekommer. Vanligast är dock att filmningen äger rum i offentliga miljöer. Även stillbildskameror används. Beslut om att använda handmanövrerad kamera fattas av den enskilde polis- eller tulltjänstemannen och någon särskild dokumentation över användningen görs inte. Privatpersoner upplåter ibland utrymmen för att spaningsinsatsen ska kunna genomföras. För det fall bilderna har betydelse för utredningen redovisas de i förundersökningsprotokollet och används som bevis i rättegång.

Säkerhetspolisens användning av handmanövrerade kameror skiljer sig inte från den som förekommer inom polisen i övrigt. Säkerhetspolisen har också framhållit att metoden är viktig för att på ett tillförlitligt och säkert sätt dokumentera de iakttagelser som exempelvis spaningspersonal gör i sitt arbete.

10.1.3 Utröna lokalisering

Positionsbestämning (s.k. pejling)

Positionsbestämning (ofta benämnd pejling) är en metod som innebär att den brottsbekämpande myndigheten spårar ett föremål genom att en elektronisk sändare fästs på föremålet, t.ex. ett fordon eller en container. Det kan också vara fråga om väskor, t.ex. när dessa har hittats i narkotika- eller vapengömmor, eller paket med narkotika som ska levereras till någon mottagare. Däremot förekommer det inte att sändare i hemlighet fästs i kläder. Positionsbestämning kan ske med radiopejling eller via satellit. Information ges om var föremålet befinner sig och om det rör sig.

Positionsbestämning används i några hundra fall årligen i såväl förundersökning som underrättelseverksamhet. Metoden används vid grov organiserad brottslighet, ofta sådan allvarlig brottslighet där straffvärdet överstiger fängelse två år (t.ex. mord, grova narkotikabrott, grova rån, människohandel och grova smugglingsbrott rörande vapen, cigaretter, narkotika eller alkohol). Många gånger används positionsbestämning i en förundersökning som ett komplement till hemlig teleavlyssning eller andra hemliga tvångsmedel.

Brottslingarnas många gånger extrema vaksamhet liksom medvetenheten om de brottsbekämpande myndigheternas spanings-

metoder gör användningen av positionsbestämning helt nödvändig. Genom metoden går det att se t.ex. hur fordon eller något annat objekt rör sig. Därigenom kan slutsatser dras om rekognoseringar, var möten äger rum, mönster i körningar, klarläggande av avlämningsplatser och lagerplatser samt var medgärningsmän befinner sig utan att spanare riskerar att upptäckas.

Det är av kvalitetsskäl endast ett fåtal brottsbekämpande myndigheter som har tillgång till den tekniska utrustning som behövs. Beslut om att använda metoden fattas inom polisen av högre polischef, exempelvis länskriminalchef eller dennes ställföreträdare, och i vissa fall (t.ex. nattetid) av annan polischef efter delegation. En liknande ordning finns inom tullen. Besluten fattas som utgångspunkt efter skriftlig begäran. Många gånger behöver dock besluten fattas mycket snabbt, t.ex. när en smuggellast upptäcks vid en tullkontroll och det beslutas att låta fordonet fortsätta färden till en okänd mottagare. Besluten och användningen av utrustningen dokumenteras. Även utvärderingar och uppföljningar förekommer. En och samma insats kan pågå i allt från någon dag upp till tidsperioder om flera månader. Besluten omprövas med jämna mellanrum, oftast månadsvis. Vid några myndigheter finns föreskrifter som reglerar främst beslutsfattandet.

Säkerhetspolisens användning av den tekniska utrustningen skiljer sig något från den övriga polisens genom att myndighetens uppdrag gör att den inte har samma behov av att följa exempelvis smuggellasters färd till en mottagare. Utrustningen används istället främst i arbetet med att kartlägga rörelsemönster för att se exempelvis var möten äger rum. Användningen av utrustningen är mycket betydelsefull då den sällan kan ersättas med andra metoder för inhämtning av de aktuella uppgifterna.

Montering och demontering av utrustning sker ibland på andra platser än helt offentliga, t.ex. parkeringsgarage som används av allmänheten. Privatpersoner används ibland för att bereda myndigheten tillgång till sådana platser.

Det har för utredningen påtalats ett stort behov hos de brottsbekämpande myndigheterna av att göra intrång i skyddade utrymmen för att placera den utrustning som ska användas vid positionsbestämningen och för att demontera den. I avsaknad av lagreglering är det dock inte tillåtet för den brottsbekämpande myndigheten att öppna t.ex. en bil för att bättre kunna dölja utrustningen. Det skulle strida mot ändamålsprincipen att i en sådan situation genomföra en husrannsakan, eftersom en sådan åtgärd inte kan beslutas för ett

sådant syfte (jfr 28 kap. 1 och 3 §§ RB). Det finns också behov av att kunna flytta ett fordon tillfälligt i samband med att utrustningen ska monteras eller demonteras. Ibland kan det också finnas behov av att återta utrustning som inte längre är placerad på föremålet.

Det ska i det sammanhanget nämnas att Utredningen om utvärdering av vissa hemliga tvångsmedel bedömt att en tillfällig förflyttning av ett fordon i syfte att installera avlyssningsutrustning utgör ett avsevärt mindre ingrepp i den enskildes integritet än själva avlyssningen och att det därför är rimligt att den myndighet som ska verkställa ett beslut om hemlig rumsavlyssning får möjlighet att flytta det fordon i vilket avlyssningsutrustningen ska installeras. Utredningen nämnde också att även säkerhetsskäl ibland kan motivera att fordonet flyttas (se vidare SOU 2009:70 s. 153).

Det förhållandet att positionsbestämning har använts redovisas ofta inte i förundersökningen och uppgifterna används normalt inte som bevis i rättegång.

10.2 Internationell utblick

10.2.1 Danmark

I Danmark finns sedan år 1999 en särskild reglering om observation i 791 a § retsplejeloven. Utgångspunkten för lagstiftningen är att observation, med eller utan tekniska hjälpmedel, på en plats som är tillgänglig för allmänheten är tillåten utan särskilt lagstöd. Detsamma gäller observation med blotta ögat, dvs. utan optiska hjälpmedel, varhelst den äger rum. I den ovan nämnda bestämmelsen regleras därför endast sådan observation som sker på platser dit allmänheten inte har tillträde och där optiska instrument används.

Polisen kan, enligt 791 a § första stycket retsplejeloven, med hjälp av kikare eller annan apparat fotografera eller iaktta personer som befinner sig en plats som inte är fritt tillgänglig (observation). Som villkor för en sådan observation gäller att åtgärden måste vara av väsentlig betydelse för efterforskningen och att efterforskningen rör en lagöverträdelse som kan medföra frihetsstraff. Denna typ av observation kan beslutas av polisen.

I andra stycket samma lagrum behandlas observation som sker med hjälp av fjärrstyrda eller automatiska tv-kameror, fotografiapparater eller liknande apparater. Som villkor för sådan observa-

tion uppställs att efterforskningen avser ett brott på vilket det kan följa fängelse i ett år och sex månader eller däröver. Rätten beslutar om sådan observation med möjlighet för polisen att fatta interimistiskt beslut.

I tredje stycket behandlas sådan observation där den person som observeras befinner sig i en bostad och där observationen sker med hjälp av fjärrstyrd eller automatisk tv-kamera, fotografiapparat eller liknande apparat eller med hjälp av en apparat som används i bostaden eller ”husrummet”. För att en sådan observation ska få genomföras gäller att det finns bestämd grund till att anta att bevis kan erhållas genom åtgärden, att åtgärden är av avgörande betydelse för efterforskningen och att det rör sig om ett brott på vilket fängelse i sex år eller däröver kan följa eller annars vid vissa särskilt angivna brott. Även i dessa fall gäller att observation ska beslutas av rätten, men att polisen har rätt att fatta interimistiskt beslut.

En målsägande som råder över den plats som ska observeras kan ge sitt samtycke till observation, vilket medför att de förutsättningar som beskrivs ovan inte behöver vara uppfyllda.

Rättens tillstånd till observation anses innefatta ett tillstånd att placera nödvändig utrustning i de lokaler som är aktuella (jfr Lovforslag L 177 1997-98).

Användningen av dolda kroppsmikrofoner och inspelning av telefonsamtal i vilka polisen, eller den som polisen samarbetar med, själv deltar är oreglerad i Danmark (se SOU 2003:74 s. 99).

Vad gäller positionsbestämning var denna metod uppe till bedömning i samband med tillkomsten av den ovan nämnda lagstiftningen. I propositionen (L 177 1997-98) anförs att positionsbestämning inte ger möjlighet till avbildning eller avlyssning, utan att metoden närmast har karaktären av skuggning med hjälp av teknisk utrustning. Metoden ansågs därför inte vara av så ingripande karaktär att den bör jämställas med andra metoder enligt lagen. Vidare hänvisades till ett avgörande i Vestre Landsret år 1996 där domstolen fann att positionsbestämning inte var att anse som ett straffprocessuellt tvångsmedel som krävde lagstöd eller domstolens tillstånd (se SOU 2003:74 s. 99).

10.2.2 Finland

Bestämmelser om tekniska spaningsmetoder infördes i Finland i mitten av 1990-talet och är intagna i dels polislagen, dels tvångsmedelslagen. Tvångsmedelslagen är tillämplig vid förundersökning, medan polislagen gäller polisens arbete även i samband med förebyggande av brott. Tvångsmedelslagen tillämpas enligt principen om lex specialis, dvs. om det rör sig om utredning av ett brott gäller denna lag framför polislagen.

Vad gäller handmanövrerad kamera innehåller finsk lagstiftning dels bestämmelser om allmän övervakning, dels bestämmelser om s.k. optisk övervakning.

Enligt polislagen (7.4.1995/493) får polisen på allmän plats bedriva teknisk övervakning i syfte att bl.a. upprätthålla allmän ordning och säkerhet eller förebygga brott (29 §). Härmed avses att polisen fortlöpande eller upprepat iakttar eller avlyssnar allmänheten, fordonsförare, fotgängare eller fordon med hjälp av en teknisk anordning samt automatisk upptagning av ljud eller bild (28 §).

Polisen får vidare bedriva teknisk observation (31 §). I det begreppet täcks tre förfaranden in; ”teknisk avlyssning” (avlyssning av person och upptagning av ljud), ”optisk övervakning” (iakttagande och avbildande av en person) och ”teknisk spårning” (spårning av hur ett fordon eller en vara förflyttas). En polisman får enligt bestämmelsen utföra teknisk observation av en person som inte befinner sig i ett utrymme som används som bostad eller av fordon eller varor, om det finns grundad anledning att anta att observationen kan ge uppgifter som behövs för att avvärja ett brott. Polisen får ta sig in i utrymmen där teknisk observation är tillåten, om observationen förutsätter detta och för att installera eller avlägsna anordningen. För optisk övervakning och teknisk spårning förutsätts att det på grund av en persons uppträdande eller annars finns grundad anledning att anta att han eller hon gör sig skyldig eller medverkar till ett brott för vilket det föreskrivna strängaste straffet är fängelse i mer än sex månader. Beslut om optisk övervakning och teknisk spårning fattas av en polisman som tillhör befälet eller som har förordnats till undersökningsledare (32 §).

Även i tvångsmedelslagen (30.4.1987/450) finns bestämmelser om teknisk observation. I lagen definieras optisk övervakning som att en viss person eller plats där en misstänkt kan antas befinna sig fortlöpande eller upprepade gånger fotograferas eller observeras i hemlighet med kikare, kamera, videokamera eller någon annan så-

dan anordning eller metod (5 a kap. 1 § 3 b). Det betraktas enligt förarbetena inte som optisk övervakning, om den som misstänks för ett brott fotograferas eller iakttas med kikare enstaka gånger i vissa enskilda situationer. Optisk övervakning får enligt tvångsmedelslagen användas när någon är skäligen misstänkt för ett brott för vilket det strängaste straffet är mer än sex månaders fängelse. Övervakningen får riktas mot den misstänkte eller mot en viss plats där han kan antas befinna sig. Som en allmän förutsättning gäller att övervakningen får genomföras endast om de uppgifter som därmed fås kan antas vara av synnerlig vikt för utredningen av brottet. Optisk övervakning får riktas mot den misstänkte endast när denne inte befinner sig i en bostad (5 a kap. 4 a §).

I tvångsmedelslagen definieras teknisk spårning som att ett kommunikationsmedel eller en vara spåras med hjälp av en radiosändare som har fästs vid kommunikationsmedlet eller varan eller med hjälp av någon annan sådan anordning eller metod (5 a kap. 1 § 3 c). Teknisk spårning får ske om någon är skäligen misstänkt för ett brott för vilket det strängaste straffet är mer än sex månaders fängelse och spårningen får riktas mot det fordon som den misstänkte använder eller det varuparti som utgör föremål för brottet. Polisen har rätt att i hemlighet gå in i ett fordon för att avlägsna anordningen (5 a kap. 4 b §).

Beslut om optisk övervakning och teknisk spårning enligt tvångsmedelslagen fattas av undersökningsledaren. Beslut av domstol krävs för optisk övervakning som innebär att avlyssnings- eller övervakningsanordning fästs i ett fordon som används av den misstänkte eller i ett utrymme där den misstänkte befinner sig (5 a kap. 5 §).

Användningen av dolda kroppsmikrofoner och möjligheten att spela in telefonsamtal som polisen, eller den som polisen samarbetar med, själv deltar i är oreglerad i Finland. Metoderna anses dock vara tillåtna (se SOU 2003:74 s. 96).

10.2.3 Norge

Användning av kroppsmikrofon och liknande utrustning är tillåten i Norge enligt 216 l § straffeprosessloven. Enligt bestämmelsen får polisen efter beslut av åklagare genom teknisk utrustning avlyssna eller göra upptagningar av telefonsamtal eller andra samtal mellan en misstänkt och polisen eller någon som har gett samtycke till åtgärden. Misstanken ska röra brott som kan ge fängelse.

Handmanövrerad kamera ses som ett spaningshjälpmedel. Användningen är tillåten utan någon särskild reglering.

Även positionsbestämning genom pejling är tillåten. Enligt 202 b § straffeprosessloven får teknisk pejlingsutrustning placeras på fordon, gods och liknande i syfte att klarlägga var saken eller den misstänkte befinner sig. Metoden benämns teknisk spårning och får beslutas av åklagare när någon är skäligen misstänkt för ett brott för vilket är föreskrivet 5 års fängelse eller mer eller det är fråga om vissa uppräknade brott.

Skulle det vara fråga om brott som kan medföra tio års fängelse eller mer, alternativt vissa andra uppräknade brott, kan rätten enligt 202 c § straffeprosessloven ge polisen tillstånd att placera pejlingsutrustningen även i kläder eller annat som den misstänkte bär på sig och i väskor eller annat handbagage som den misstänkte bär med sig. Finns misstanke om sådana allvarliga brott kan polisen också få rättens tillstånd att bereda sig tillträde till utrymmen för att placera utrustningen, även i de fall som framgår av föregående paragraf (t.ex. ett fordon). Interimistiskt beslut kan ges av åklagare. Tillståndstiden får vara högst fyra veckor åt gången. Den misstänkte ska underrättas om åtgärden efter att den är genomförd. Från den huvudregeln finns undantag föreskrivna, bl.a. när det är ”strängt nödvändigt för utredningen” av vissa angivna brott.

10.3 Behovet av en reglering

Bedömning: Ljudupptagning, bildupptagning och lokalisering av person med hjälp av teknisk utrustning är åtgärder som idag används av de brottsbekämpande myndigheterna och som det fortsatt kommer att finnas ett stort behov av att använda. Med hänsyn till utvecklingen av Europadomstolens praxis och den beslutade ändringen av 2 kap. 6 § RF, finns det skäl att lagreglera användningen av dessa åtgärder. Den nuvarande användningen kan visserligen inte anses stå i strid med varken Europakonventionen eller den nya lydelsen av regeringsformen. Enligt utredningens mening finns det dock skäl att eftersträva en ordning som på ett tydligare sätt och med viss marginal uppfyller de krav som följer av internationella åtaganden eller av regeringsformen.

En utgångspunkt för utredningens bedömning av behovet av en reglering är att åtgärderna ljudupptagning av samtal, bildupptagning av hem eller korrespondens samt lokalisering av person är så viktiga för den brottsbekämpande verksamheten att något annat än ett fortsatt användande av dem är uteslutet.

Möjligheterna för de brottsbekämpande myndigheterna att använda teknisk utrustning för att ta upp ljud, bild och för att lokalisera en person är i princip oreglerad. Vad gäller ljudupptagning kan förenklat sägas gälla att endast ljudupptagning av samtal mellan andra är reglerad. I denna del finns ett grundläggande förbud i 4 kap. 9 a § BrB som kompletteras med en reglering av de brottsbekämpande myndigheternas rätt att använda bl.a. hemlig teleavlyssning och hemlig rumsavlyssning. Rätten att uppta ett samtal i vilket man själv deltar (eller vid vilket någon deltagare samtyckt till åtgärden) är emellertid, förutom de allmänna befogenheterna i polislagen, i princip oreglerad.

När det gäller bildupptagning finns en reglering avseende allmän och hemlig kameraövervakning, men upptagning med annat än fjärrstyrda kameror är oreglerad, förutom genom de allmänna principerna i polislagen. Vad gäller lokalisering av person råder en mer generell avsaknad av särskilda regler.

Som framgått av praxisgenomgången (se bilaga 3–4 avsnitt 6.5) har Europadomstolen funnit att upptagning av ljud, oavsett om någon av de personer som deltar i samtalet vet om upptagningen eller inte, innefattar ett intrång i den enskildes rättigheter på samma nivå som sker vid hemlig teleavlyssning. I genomgången sägs att det går att argumentera för att det uppstår olika nivå på intrånget t.ex. beroende på om upptagningen sker i hemmet eller utanför detsamma, men samtidigt kan resultatet av en upptagning utanför hemmet bli att myndigheten får tillgång till en större mängd överskottsinformation än annars. Slutsatsen i praxisgenomgången är att det i princip bör finnas en enhetlig reglering för upptagning av ljud och att den regleringen ska motsvara de principiella krav som Europadomstolen uppställer när det gäller hemlig teleavlyssning (se bilaga 3–4 avsnitt 6.5).

Vad gäller bildupptagning visar praxisgenomgången att det inte är själva bildupptagningen i sig som kan komma att innebära ett intrång i en skyddad rättighet enligt Europakonventionen, utan den efterföljande behandlingen av bilderna. Även om bildupptagningen i sig därför inte behöver ha särskilt lagstöd blir det praktiska resultatet att myndigheterna, så snart en bild är tagen, behöver särskilt

lagstöd för den fortsatta behandlingen av bilden (se bilaga 3–4 avsnitt 5.3.2).

När det gäller åtgärder som innefattar lokalisering av person visar praxisgenomgången att en sådan åtgärd innefattar ett intrång i den övervakades rättigheter. När det däremot gäller annan lokalisering än lokalisering av person är slutsatserna i praxisgenomgången mer osäkra (se bilaga 3–4 avsnitt 5.3.4). Det får dock anses föreligga betydande skillnader i graden av integritetsintrång vid en jämförelse mellan lokalisering av person och annan lokalisering. Detta återspeglar sig enligt utredningen också när det gäller behovet av uttrycklig reglering.

Härutöver bör det nya andra stycket som den 1 januari 2011 införs i 2 kap. 6 § RF uppmärksammas (se prop. 2009/10:80). I stycket föreskrivs följande.

> Utöver vad som föreskrivs i första stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

I författningskommentaren till denna bestämmelse (se prop. 2009/10:80 s. 250) utvecklas innebörden av bestämmelsen på följande sätt.

> I *andra stycket*, som inte har någon tidigare motsvarighet, finns en bestämmelse som utvidgar skyddet mot intrång i den personliga integriteten. Bestämmelsen innebär att enskilda, vid sidan av vad som redan följer av första stycket, är skyddande mot åtgärder från det allmännas sida som innefattar betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Bestämmelsen träffar inte åtgärder som en enskild vidtar i förhållande till en annan enskild. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp. Uttrycket ’enskilds personliga förhållanden’ avses här ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400). Vid bedömning av vilka åtgärder som kan anses utgöra ett ’betydande intrång’ ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Även åtgärdens ändamål och andra omständigheter kan ha betydelse vid bedömningen. Bestämmelsen omfattar endast sådana intrång som på grund av åtgärdens intensitet eller omfattning eller av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter innebär ett betydande ingrepp i den enskildes privata sfär.

Även om det kan diskuteras vad som omfattas av den föreslagna bestämmelsen står det klart att bestämmelsen kan komma att innebära att lagstöd åtminstone i vissa fall fordras beträffande sådana tekniska åtgärder som här avses.

Sammantaget finner utredningen att det såväl utifrån konventionspraxis som med utgångspunkt i den nya grundlagsbestämmelsen finns skäl att reglera användningen av de nu diskuterade tekniska spaningsmetoderna. Den nuvarande användningen av dessa metoder kan visserligen inte sägas stå i strid med Europakonventionen eller regeringsformen, men det finns enligt utredningens mening skäl att eftersträva en ordning som på ett tydligare sätt och med viss marginal uppfyller de krav som följer av såväl internationella åtaganden som regeringsformens bestämmelser om fri- och rättigheter.

10.4 Närmare om åtgärderna

Bedömning: Ljudupptagning, bildupptagning och lokalisering av person är åtgärder som vad gäller integritetsintrång inte skiljer sig så mycket från varandra att det finns skäl att föreskriva olika förutsättningar för att åtgärderna ska få vidtas. Det kan emellertid finnas skäl att ställa krav på att beslut fattas av annan än den brottsbekämpande myndigheten i de fall där åtgärderna kan bedömas bli särskilt ingripande.

Vid en reglering av möjligheterna att uppta ljud och bild samt att använda teknisk utrustning för att lokalisera en person bör kraven för att vidta åtgärden anpassas efter den grad av integritetsintrång som åtgärden innebär. En sådan gradering kan sägas följa av proportionalitetsprincipen: ju mer integritetskränkande en viss åtgärd kan anses vara desto viktigare måste det intresse som motiverar åtgärdens användning vara. Det finns därför, enligt utredningens mening, skäl att här inleda med ett avsnitt i vilket de olika åtgärderna behandlas och relateras till varandra i just detta perspektiv. Genom att göra en bedömning av hur ingripande och integritetskränkande olika åtgärder typiskt sett kan anses vara kan man skapa en grund för en rationell och värderingsmässigt sammanhängande reglering.

De åtgärder som ska behandlas i detta kapitel är – vilket närmare utvecklas nedan – ljudupptagning i fall där företrädare för de brotts-

bekämpande myndigheterna deltar i det samtal eller sammanträde som upptagningen avser, bildupptagning med handmanövrerad kamera samt lokalisering av person med hjälp av teknisk utrustning.

När det gäller dessa åtgärder menar utredningen att det finns skäl att betrakta upptagning av ljud som en typiskt sett integritetskänslig åtgärd, framför allt med hänsyn till att en ljudupptagning direkt tar sikte på innehållet i en viss kommunikation. Detta återspeglas också i Europadomstolens praxis där det t.o.m. talas om att ljudupptagning innebär en integritetskränkning på samma nivå som vid hemlig teleavlyssning (se ovan avsnitt 10.3).

Som ovan angivits och som närmare utvecklas nedan avser utredningens överväganden emellertid endast ljudupptagningar avseende samtal eller sammankomster vid vilka en företrädare för myndigheten deltar. Det förhållandet att regleringen på detta sätt endast tar sikte på upptagningar som görs av någon som deltar i samtalet eller sammankomsten gör, enligt utredningens mening, att integritetsaspekterna måste anses göra sig gällande på ett annat och mindre tydligt sätt än vid t.ex. hemlig teleavlyssning, eftersom företrädaren endast dokumenterar uppgifter som berättas för honom eller henne. Allmänt sett gäller att man i relation till personer som deltar i ett samtal eller ett sammanträde aldrig kan vara helt garanterad att innehållet i samtalet ska förbli privat. Den som deltar har naturligtvis en direkt upplevelse av samtalet eller sammanträdet och det måste också hållas i minnet att varje deltagare i princip har rätt att göra en upptagning avseende samtalet eller sammankomsten.

Vidare innebär det förhållandet att upptagningen förutsätter deltagande av företrädare för myndigheten en praktisk begränsning av åtgärdens användbarhet vilket allmänt sett är ägnat att minska riskerna för en tidsmässigt utsträckt avlyssning eller upptagning.

Detta bör enligt utredningens mening återspeglas däri att sådan ljudupptagning bör kunna tillåtas i större utsträckning än hemlig teleavlyssning eller hemlig rumsavlyssning.

När det gäller bildupptagning visar praxisgenomgången (se bilaga 3–4 avsnitt 5.3.2) att det inte är själva bildupptagningen i sig, utan den efterföljande behandlingen, som kan utgöra ett intrång i den skyddade rättigheten. I linje med vad som där anges blir emellertid snart sagt varje efterföljande åtgärd med bilden att se som ett intrång. Det finns därför skäl att reglera bildupptagningen som sådan.

Bildupptagning (utan ljud) kan typiskt sett anses vara en åtgärd som är något mindre känslig från integritetssynpunkt än ljudupptagning, bl.a. därför att man genom bildupptagningen inte får tillgång

till innehållet i själva kommunikationen, men också därför att personer normalt (med undantag för vissa platser) inte har en grundad förväntan om att inte bli sedda. Hur integritetskänslig en bildupptagning är kan emellertid, och naturligtvis, variera påtagligt bl.a. beroende på vilka utrymmen bildupptagningen avser. Fotografering in i eller inne i någons hem eller andra liknande platser, liksom fotografering av korrespondens, måste sålunda anses utgöra en åtgärd som i inte obetydlig utsträckning kan vara integritetskänslig, medan annan fotografering kan framstå som relativt harmlös från integritetssynpunkt. I ett lagstiftningsperspektiv bör emellertid bildupptagning allmänt sett betraktas som en åtgärd som är mindre integritetskänslig än ljudupptagning.

Motsvarande kan sägas om lokalisering av person, dvs. att åtgärden normalt bör betraktas som en åtgärd som från integritetssynpunkt är mindre känslig än ljudupptagning. Detta kan i första hand sägas bero på att det genom lokalisering endast framkommer information om var ett visst föremål (och därigenom eventuellt var en viss person) befinner sig, dvs. informationsmängden är begränsad. Också vid lokalisering kan det emellertid i hög grad bero på omständigheterna hur integritetskänslig en viss åtgärd är. I fall där utrustningen placeras på eller i ett föremål som personen bär på sig eller har med sig måste lokalisering betraktas som en relativt ingripande åtgärd som kan möjliggöra en inte obetydlig kartläggning av personens aktiviteter. Motsvarande kan gälla om lokaliseringen är tänkt att pågå under lång tid.

Mot bakgrund av dessa överväganden finner utredningen att det visserligen – på ett allmänt plan – kan sägas föreligga en viss skillnad inbördes mellan de nu diskuterade åtgärderna vad gäller graden av integritetsintrång. Skillnaderna mellan de olika åtgärderna är emellertid inte stora. Vidare förhåller det sig så att en åtgärd som typiskt sett är mindre integritetskränkande i ett konkret fall kan medföra en högst påtaglig integritetskränkning och i andra fall är det i stället omvänt. Det framstår därför inte som självklart att det från regleringssynpunkt bör skiljas mellan ljudupptagning, bildupptagning och lokalisering i de angivna fallen. Det finns inte heller tillräckliga skäl att i relation till de olika åtgärderna som sådana ställa upp olika krav.

Utgångspunkten bör i stället vara en enhetlig reglering avseende alla de nu behandlade åtgärderna. Inom ramen för en sådan enhetlig reglering finns det emellertid – på ett liknande sätt som gjordes i utredningens delbetänkande när det gäller hemlig teleövervakning i

syfte att utreda vem som kan misstänkas för ett visst brott (se SOU 2009:1 s. 117 f.) – skäl att uppställa krav på att besluten fattas på en högre nivå när det gäller åtgärder som bedöms vara särskilt ingripande. Genomgående bör också göras skillnad mellan den reglering som tar sikte på förundersökning och den som tar sikte på underrättelseverksamhet.

10.5 Upptagning av ljud

10.5.1 Vad ska befogenhetsregleringen avse?

Förslag: De brottsbekämpande myndigheterna ska med tekniskt hjälpmedel för upptagning av ljud, dolt eller genom vilseledande, få ta upp

1. samtal där företrädare för myndigheten själv deltar, eller
2. sådant som avhandlas vid sammanträde eller sammankomst vartill allmänheten inte har tillträde om företrädare för myndigheten själv deltar i sammanträdet eller sammankomsten.

Bedömning: Dold eller vilseledande ljudupptagning som sker i annat syfte än brottsutredande eller för att förebygga, förhindra eller upptäcka brottslig verksamhet, dvs. sådan ljudupptagning som sker i t.ex. skydds- eller dokumentationssyfte, behöver inte regleras särskilt.

Enligt 4 kap. 9 a § BrB är det straffbart att olovligen med tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssna eller uppta tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten icke äger tillträde och som man själv inte deltar i eller som man obehörigen berett sig tillträde till. Bestämmelsen kan sägas innebära att var och en som deltar i ett samtal (eller i ett sammanträde) i princip kan förfoga över detsamma och tillåta t.ex. avlyssning eller ljudupptagning.

Detta återspeglas i att de nuvarande reglerna om hemlig teleavlyssning eller hemlig rumsavlyssning tar sikte på situationer där ingen av de som deltar i samtalet eller sammankomsten har samtyckt till avlyssningen eller upptagningen.

Det område som idag inte är reglerat på annat sätt än genom polislagens allmänna bestämmelser avser alltså sådana fall där en företrädare för de brottsbekämpande myndigheterna tar upp ljud (eller

tillåter att ljud tas upp av annan) vid ett samtal där företrädaren själv deltar eller vid ett sammanträde eller en sammankomst där företrädare deltar. Det är i första hand detta område som det kan finnas skäl att reglera särskilt.

Som ovan framgått omfattar kriminaliseringen av olovlig avlyssning i 4 kap. 9 a § BrB inte heller avlyssning eller upptagning i samband med sammanträden och sammankomster vartill allmänheten äger tillträde. Att bestämmelsen är utformad på detta sätt beror naturligtvis på att man vid dylika tillställningar måste räkna med att det som sägs sprids och kanske också når offentligheten. Enligt utredningens mening finns det, av motsvarande skäl, inte något behov av en reglering av dessa situationer. Det betyder att regleringsbehovet avser dels ljudupptagning avseende samtal i vilka företrädare för den brottsbekämpande myndigheten själv deltar, dels ljudupptagning avseende sammanträde eller sammankomst vartill allmänheten inte har tillträde och vid vilken företrädare för myndigheten själv deltar.

Annorlunda förhåller det sig enligt utredningen med sådana ljudupptagningar av samtal som visserligen sker dolt eller med vilseledande men där syftet inte är brottsutredande eller att förebygga, förhindra eller upptäcka brottslig verksamhet. Det handlar framför allt om sådana ljudupptagningar som sker i skyddssyfte t.ex. om en polis som arbetar under täckmantel av säkerhetsskäl behöver kunna omedelbart vidarebefordra vad som händer omkring honom eller henne. Det kan också röra upptagningar som sker i dokumentationssyfte men utan anknytning till en pågående förundersökning eller motsvarande. Ett exempel på det sistnämnda kan vara när en informatörshanterare träffar en informatör och behöver kunna skydda sig mot senare framförda falska påståenden.

När dolda ljudupptagningar sker i skydds- eller dokumentationssyfte enligt vad som framgår ovan gör sig kravet på lagreglering av åtgärderna inte lika starkt gällande. Det kan visserligen hävdas att integritetsintrånget av att bli utsatt för en sådan ljudupptagning inte blir mindre beroende på i vilket syfte upptagningen sker. Det förhållandet att upptagningen inte är avsedd att användas så att säga direkt i den brottsbekämpande verksamheten gör dock att behovet av lagreglering framstår som påtagligt mindre. Det kan här jämföras med att motsvarande åtgärder kan vidtas av privatpersoner utan något som helst rättsligt stöd. Någon särskild lagreglering av åtgärder som brottsbekämpande myndigheter vidtar i dessa syften

anser utredningen således inte behövs utan dessa kan även framöver vidtas med stöd av enbart bestämmelserna i polislagen.

10.5.2 När ska befogenheten få användas?

Förslag: I en förundersökning ska ljudupptagning få ske om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket det är föreskrivet fängelse i ett år eller däröver.

I underrättelseverksamhet ska ljudupptagning få ske om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver.

I båda fallen ska förutsättas att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Ljudupptagning i förundersökning

En förutsättning för att hemlig teleavlyssning och hemlig rumsavlyssning ska få användas är att det finns en skäligen misstänkt person (se 27 kap. 20 § RB och 3 § lagen om hemlig rumsavlyssning). Hemlig kameraövervakning får dock i vissa fall genomföras även utan att det finns någon som är skäligen misstänkt för det aktuella brottet. Syftet ska då vara att fastställa vem som är skäligen misstänkt (27 kap. 20 c § RB). Utredningen har i delbetänkandet (se SOU 2009:1 s. 113 ff.) föreslagit att även hemlig teleövervakning ska få användas i fall där det saknas en skäligen misstänkt person i syfte att kunna fastställa vem den personen är eller för att utröna annan omständighet av väsentlig betydelse för utredningen.

En ljudupptagning av det slag som här diskuteras kan förvisso innebära ett visst, inte obetydligt, integritetsintrång. I sammanhanget kan, utöver vad som sägs i praxisgenomgången, noteras att två ledamöter av Lagrådet i samband med straffbestämmelsens införande menade att straffskyddet enligt bestämmelsen om olaga avlyssning enligt 4 kap. 9 a § BrB blivit väl inskränkt. I Lagrådsyttrandet uttalades följande (Se NJA II 1975 s. 607)

> Särskilt betänkligt synes det vara att avlyssningen eller upptagningen enligt förslaget anses lovlig och därmed straffri, när t ex en utomstående förmår en av deltagarna i ett sammanträde att i fickan eller

> annat utrymme medföra en dold mikrofon. Från övriga deltagares synpunkt lärer det ligga lika nära till hands att betrakta den nämnde deltagaren så som medverkande i en hemlig avlyssning från den utomståendes sida som att betrakta honom så som den som gjort avlyssningen lovlig. Gentemot alla dem som inte känner till avlyssningen måste nämligen vid ett naturligt betraktelsesätt denna uppfattas som hemlig och innebära lika svårt angrepp mot den personliga integriteten som den avlyssning som sker utan någon enda deltagares vetskap.

Enligt utredningens mening påvisar uttalandet att ett synsätt enligt vilket all avlyssning eller upptagning som sker av, eller med samtycke av, någon som deltar i ett samtal skulle vara oproblematisk från integritetssynpunkt, inte kan anses hållbar.

Med hänsyn till att man vid ett samtal alltid måste räkna med att de personer som deltar i samtalet i en mening också förfogar över innehållet (t.ex. kan föra innehållet vidare) kan emellertid dylika åtgärder inte anses vara lika integritetskänsliga som hemlig teleavlyssning eller hemlig rumsavlyssning. Emellertid är det på det sättet att man vid kommunikation med andra alltid är tvungen att visa tillit till dem som deltar i samtalet, men att det också bör finnas en befogad förväntan om att andra personer inte självständigt ska kunna få tillgång till innehållet i samtalet.

Mot denna bakgrund gör utredningen bedömningen att beslut om ljudupptagning inom ramen för en förundersökning bör förutsätta att utredningen avser brottslighet av viss svårhet samt att ljudupptagningen kan förväntas ha viss betydelse för utredningen. Det förhållandet att regleringen endast tar sikte på upptagningar som görs av någon som deltar i samtalet eller sammankomsten gör emellertid, som ovan utvecklats, att integritetsaspekterna gör sig gällande med betydligt mindre styrka än vid t.ex. hemlig teleavlyssning, vilket också bör återspeglas i regleringen. Kraven för användande av åtgärden bör med andra ord inte sättas på en sådan hög nivå straffvärdemässigt som krävs för tillstånd till hemlig teleavlyssning.

Vad gäller brottslighetens svårhet framstår det enligt utredningen som rimligt att lägga gränsen för när åtgärden ska få användas vid brott som kan utgöra grund för häktning enligt 24 kap. 1 § första stycket RB, dvs. vid brott som kan föranleda fängelse i ett år eller mer. Härigenom utesluts dels rena bötesbrott, dels brott med ett maximistraff motsvarande fängelse i sex månader.

Med hänsyn till att det är fråga om åtgärder som är tillåtna för envar och med beaktande av att integritetshänsynen får en mer tillbakaskjuten roll än vid avlyssning som görs av någon som inte del-

tar i samtalet, bör åtgärden, enligt utredningens bedömning, kunna användas också när det inte föreligger skälig misstanke mot en viss person.

När det gäller frågan om betydelsen för brottsutredningen bör det krävas att det finns anledning att anta att en ljudupptagning kommer att ha betydelse på ett sätt som inte framstår som obetydligt. Detta kan lämpligen komma till uttryck genom att det föreskrivs att åtgärden får vidtas, om den kan antas vara av särskild betydelse för utredningen.

Ljudupptagning inom underrättelseverksamhet

När det gäller underrättelseverksamhet ter det sig som naturligt att anknyta till de krav som utredningen tidigare föreslagit vad gäller inhämtning av uppgifter om viss elektronisk kommunikation (se SOU 2009:1 s. 123 ff.), men samtidigt anpassa kraven med hänsyn till att det är fråga om en åtgärd som i princip är tillgänglig för envar. I nyss nämnda betänkande föreslogs att inhämtning av uppgifter om elektronisk kommunikation skulle få ske under förutsättning att det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar antingen brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller vissa särskilda uppräknade brott av allvarligare slag.

Uttrycket ”särskild anledning att anta” har tidigare använts för att ge uttryck för att fråga ska vara om en bedömning som inte bygger på spekulationer eller allmänna antaganden utan om en bedömning grundad på faktiska omständigheter. Denna tröskel framstår som lämplig att använda också i detta sammanhang (tröskeln har behandlats bl.a. i utredningens delbetänkande, SOU 2009:1; jfr citatet strax nedan). Det bör följaktligen uppställas krav på att det finns särskild anledning att anta att åtgärden, dvs. ljudupptagningen, kommer att ha betydelse för undersökningen.

Innebörden i kravet på särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka viss brottslighet, beskrevs i nämnda betänkande (se SOU 2009:1 s. 178) på följande sätt.

> Som en begränsning i möjligheten att inhämta uppgifter föreskrivs i paragrafen att det i en undersökning ska finnas särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upp-

täcka viss brottslighet. Att det ska finnas ”särskild” anledning att anta att uppgifterna på det sättet kan vara till nytta i undersökningen markerar att det inte kan vara fråga om en alltför extensiv bedömning av värdet av uppgifterna för undersökningen. Bedömningar av uppgifternas värde får inte bygga på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter.

På grundval av faktiska omständigheter ska bedömningen som görs av uppgifternas värde i undersökningen mynna ut i att de kan bidra till att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Med begreppet ”kan bidra” avses att uttrycka att uppgifterna på något sätt ska kunna antas bli av värde i undersökningen och föra denna framåt.

Kravet på visst underlag för bedömningen vad gäller åtgärdens framtida betydelse är uppställt med hänsyn till att underrättelseverksamhet bygger på bred informationsinhämtning. En reglering som bara skulle bygga på att det finns anledning att anta att en viss uppgift kan bidra till att förebygga, förhindra osv. skulle därför, enligt utredningens mening, bli alltför vidsträckt.

Med hänsyn till åtgärdens karaktär finns i detta fall inte skäl att uppställa så höga krav avseende brottslighetens svårhet som gjordes när det gäller inhämtning om uppgifter om elektronisk kommunikation. Det framstår, med hänsyn till de överväganden som tidigare gjorts angående åtgärdens betydelse i ett integritetsperspektiv, som rimligt att lägga tröskeln vid undersökningar inom underrättelseverksamheten vid brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, dvs. på en nivå som motsvarar den som föreslås gälla för förundersökning.

Proportionalitet vid åtgärderna

Åtgärder som innefattar intrång i enskilda personers rättigheter enligt Europakonventionen och regeringsformen måste enligt de allmänna principer som gäller avseende den statliga maktutövningen alltid användas med återhållsamhet och endast när åtgärden är nödvändig och står i rimlig proportion till vad som står att vinna med åtgärden. Dessa krav innefattas i den s.k. proportionalitetsprincipen. Enligt utredningens mening bör det vid reglering av de nu behandlade åtgärderna – på motsvarande sätt som när det gäller tvångsmedelsanvändning enligt bl.a. rättegångsbalken – uttryckligen föreskrivas att åtgärderna ska få användas endast när skälen för åtgärden uppväger det intrång eller men i övrigt som den innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Detta gäller även för bildupptagnings- och lokaliseringsåtgärder enligt detta kapitel.

10.5.3 Vem ska fatta beslut?

Förslag: I en förundersökning ska beslut om ljudupptagning fattas av undersökningsledaren.

I underrättelseverksamhet ska beslut om ljudupptagning fattas av chefen för den brottsbekämpande myndigheten.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller ljudupptagning som är särskilt ingripande ska frågor om ljudupptagning i förundersökning prövas av rätten på ansökan av åklagaren, med möjlighet för åklagaren eller polisman att fatta ett interimistiskt beslut. Ett interimistiskt beslut ska skyndsamt prövas av rätten.

I underrättelseverksamhet ska frågor om ljudupptagning som är särskilt ingripande prövas av Nämnden på ansökan av den brottsbekämpande myndigheten, med möjlighet för chefen för den brottsbekämpande myndigheten, polisman eller annan tjänsteman vid den brottsbekämpande myndigheten att fatta ett interimistiskt beslut. Ett interimistiskt beslut ska skyndsamt prövas av Nämnden.

Beslut i förundersökning

Beslut om hemlig teleövervakning prövas som huvudregel av rätten på ansökan av åklagaren. Med beaktande av att det här är fråga om upptagning som görs (eller tillåts) av en person som deltar i samtalet eller sammanträdet och med beaktande av att åtgärden är tillgänglig för envar framstår det emellertid som rimligt att som huvudregel lägga beslutanderätten på undersökningsledaren.

När det gäller ljudupptagning som kan anses vara av mer ingripande slag, t.ex. om det kan förutses att upptagningen kommer att bli mycket omfattande eller avse samtal som från integritetssynpunkt är särskilt känsliga, bör emellertid frågan prövas av rätten på ansökan av åklagaren. Frågan vad som ska bedömas vara en särskilt ingripande ljudupptagning får avgöras från fall till fall. En närmare

beskrivning av några typsituationer finns i författningskommentaren till 2 kap. 5 §, se avsnitt 15.1.

I båda fallen gäller emellertid att beslut om ljudupptagning kan behöva fattas i en snabbt uppkommen situation. Det framstår därför som nödvändigt att komplettera regleringen med en möjlighet till interimistiska beslut som kan användas i sådana situationer.

I sådana fall där det slutliga beslutet ska fattas av undersökningsledaren bör interimistiska beslut kunna fattas av en polisman.

När det sedan gäller fall där frågan ska prövas av rätten bör interimistiska beslut i första hand fattas av åklagaren, men också i detta fall måste sådana beslut – i fall där åklagarens beslut i sin tur inte kan avvaktas – kunna fattas av polisman. När det har fattats ett interimistiskt beslut i sådana ytterst brådskande fall där rätten normalt skulle fatta beslut bör krävas att åklagaren genast gör en skriftlig anmälan av åtgärden till rätten och att rätten sedan prövar ärendet. Detsamma bör gälla för interimistiska beslut som åklagaren fattat beslut om.

Beslut i underrättelseverksamhet

Som ovan utvecklats måste ljudupptagning anses vara en åtgärd som i inte obetydlig utsträckning innebär ett intrång i den enskildes integritet. Av skäl som också anförts ovan kan emellertid upptagning av ljud som sker av någon som deltar i ett samtal eller sammanträde inte anses vara en lika integritetskänslig åtgärd som t.ex. hemlig teleavlyssning. I likhet med vad som i det tidigare delbetänkande föreslogs när det gäller inhämtning av uppgifter om elektronisk kommunikation menar utredningen därför att beslutanderätten ska ligga kvar hos de brottsbekämpande myndigheterna, men att beslutsnivån bör preciseras på så sätt att beslutanderätten tillkommer myndighetschefen. Denne bör dock ges möjlighet att delegera beslutanderätten till andra personer på chefsnivå.

När det sedan gäller ljudupptagning som är av mer ingripande slag bör frågan prövas av Nämnden, med möjlighet för chefen för polismyndigheten eller – i särskilt brådskande fall – en polisman att fatta interimistiskt beslut. I denna del bör, på motsvarande sätt som inom ramen för en förundersökning, ett eventuellt interimistiskt beslut anmälas till Nämnden för prövning.

10.6 Bildupptagning av hem och korrespondens

10.6.1 Vad ska befogenheten avse?

Förslag: De brottsbekämpande myndigheterna ska med teknisk utrustning för upptagning av bild, dolt eller genom vilseledande, få ta upp

1. bild i bostad, annat hus eller rum som inte är tillgängligt för allmänheten,
2. sådan bild som avses i 1 genom särskilt inriktad bildupptagning som sker från annan plats, eller
3. bild av korrespondens genom särskilt inriktad bildupptagning.

Bildupptagning med handhållen kamera är, som ovan framhållits, endast reglerad genom polislagens allmänna befogenhetsbestämmelser. Samtidigt framgår av praxisgenomgången att bildupptagning och framför allt den efterföljande behandlingen av bilden på olika sätt kan innebära ett intrång i den enskildes rättigheter enligt Europakonventionen. När det gäller bildupptagning som visar någons hem framkommer t.ex. av praxisgenomgången att intrånget i rätten till respekt för den skyddade rättigheten blir så stort att en reglering bör uppställa samma principiella krav som vid hemlig teleavlyssning eller hemlig rumsavlyssning (se bilaga 3–4 avsnitt 6.5). Redan av det sagda följer, enligt utredningens mening, att det finns skäl att reglera vissa typer av bildupptagning.

I Integritetsskyddskommitténs betänkande (SOU 2008:3) har vidare föreslagits att det ska införas en ny bestämmelse i 4 kap. BrB enligt vilken olovlig fotografering ska kriminaliseras. Bestämmelsen föreslås placerad som en ny 6 a § och förslagets lydelse är följande.

> Den som olovligen fotograferar någon som befinner sig på en plats dit allmänheten inte har insyn döms, om inte gärningen med hänsyn till omständigheterna var försvarlig, för olovlig fotografering till böter eller fängelse i högst två år.

Förslaget bereds för närvarande inom Regeringskansliet. Om och i så fall när en sådan lagstiftning införs kommer det – förutsatt att man överhuvudtaget vill att de brottsbekämpande myndigheterna ska kunna använda sig av sådan bildupptagning som träffas av bestämmelsen – att finnas behov av regler som ger polisen rätt att foto-

grafera en person som befinner sig på en plats dit allmänheten inte har insyn.

Mot denna bakgrund gör utredningen bedömningen att det framför allt är vid tre typer av bildupptagningar som integritetsintresset gör sig så starkt gällande att det finns ett behov av en lagreglering. Det gäller för det första bilder som tas i en bostad eller i annat hus eller rum som inte är tillgängligt för allmänheten samt bilder som tas av en sådan plats ifrån ett ställe utanför bostaden, rummet etc. Det gäller vidare bilder av korrespondens genom särskilt riktad bildupptagning. Beträffande annan fotografering med handhållen kamera finns det enligt utredningens mening inte behov av någon särskild lagreglering.

10.6.2 När ska befogenheten få användas?

Förslag: I en förundersökning ska bildupptagning få ske om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

I underrättelseverksamhet ska bildupptagning få ske om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver.

I båda fallen ska förutsättas att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Bildupptagning i förundersökning

Som ovan utvecklats måste bildupptagning, också om den avser t.ex. fotografering in i den enskildes hem, generellt sett anses vara en mindre integritetskänslig åtgärd än ljudupptagning. Mot denna bakgrund bör kraven för användningen av åtgärden i vart fall inte ligga högre än för ljudupptagning. Avseende ljudupptagning gjordes (se ovan avsnitt 10.5.2) bedömningen att åtgärden bör förutsätta att fråga är om utredning av brott för vilket är föreskrivet ett års fängelse eller mer.

Vid uppställande av krav på brottets svårhet kan emellertid inte varje skillnad mellan olika åtgärder komma till uttryck, eftersom lagstiftaren är hänvisad till de olika straffskalesteg som faktiskt

används i strafflagstiftningen. På och kring den nivå som här är aktuell kan t.ex. knytas till att det för brottet är föreskrivet fängelse (vilket i praktiken innebär att det är föreskrivet fängelse i sex månader), fängelse i ett år eller mer eller fängelse i två år eller mer. Några steg däremellan finns inte.

Också med utgångspunkt i bedömningen att bildupptagning är en åtgärd som från integritetssynpunkt är något mindre känslig är det därför svårt att se att det är rimligt att gå ned ytterligare vad gäller kravet på brottets svårhet. För att fotografering i, eller in i, t.ex. rum eller bostäder ska framstå som befogad synes också vad gäller bildupptagning som huvudregel förutsättas att fråga är om annat än rena bötesbrott och brott med ett maximistraff på sex månaders fängelse. Man kan uttrycka detta så att utredningen finner att den skillnad som i ett integritetsperspektiv kan anses finnas mellan åtgärderna inte är så stor att den motiverar att kravet avseende brottslighetens svårhet ska sättas lägre vid bild än vid ljud.

Det kan diskuteras om det finns brottslighet vid vilken bildupptagning av aktuellt slag är av särskild betydelse och vid vilken sådan bör kunna ske också om det för brottet inte är föreskrivet fängelse i mer än sex månader. Såvitt utredningen kan se skulle möjligen köp av sexuell tjänst enligt 6 kap. 11 § BrB kunna utgöra ett sådant exempel. Med hänsyn till att det föreligger ett förslag om att skärpa maximistraffet för detta brott till ett års fängelse (se SOU 2010:49) lämnar utredningen emellertid inget särskilt förslag i denna del.

Liksom beträffande ljudupptagning bör krävas att åtgärden kan antas vara av särskilt betydelse för utredningen. Det ska alltså kunna antas att man genom åtgärden kan uppnå något som är av större vikt för utredningen för att en bildupptagning av det mer integritetskänsliga slag som här är fråga om ska kunna anses befogad.

Bildupptagning i underrättelseverksamhet

Vad gäller ljudupptagning inom ramen för underrättelseverksamhet har tidigare föreslagits ett krav på att undersökningen ska avse brottslighet som innefattar brott för vilket är föreskrivet fängelse i ett år eller mer. Med hänsyn till att bildupptagning, som tidigare utvecklats, får bedömas vara en åtgärd som från integritetssynpunkt är något mindre känslig än ljudupptagning, kan det övervägas om inte bildupptagning i detta avseende bör ligga på en lägre nivå.

De tillgängliga alternativen är då att gå ned till ett krav på brottslighet innefattande brott för vilket är föreskrivet fängelse (vilket i praktiken innebär att brott med ett maximistraff på sex månader kommer att inkluderas) eller att hålla kvar nivån och kräva brott för vilket är föreskrivet fängelse i ett år eller mer. Enligt utredningens mening framstår det, av samma skäl som när det gäller förundersökning, som lämpligt att avseende bild välja det senare alternativet. Det innebär att kravet läggs på samma nivå som när det gäller ljudupptagning.

10.6.3 Vem ska fatta beslut?

Förslag: I förundersökning ska beslut om bildupptagning fattas av undersökningsledaren.

I underrättelseverksamhet ska beslut om bildupptagning fattas av chefen för den brottsbekämpande myndigheten. Denne ska ha rätt att delegera beslutanderätten till annan tjänsteman på chefsnivå.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller bildupptagning som är särskilt ingripande ska frågor om bildupptagning i förundersökning prövas av rätten på ansökan av åklagaren, med möjlighet för åklagaren eller – i särskilt brådskande fall – polisman att fatta ett interimistiskt beslut. Ett interimistiskt beslut ska skyndsamt prövas av rätten.

I underrättelseverksamhet ska frågor om bildupptagning som är särskilt ingripande prövas av Nämnden på ansökan av den brottsbekämpande myndigheten, med möjlighet för chefen för den brottsbekämpande myndigheten eller – i särskilt brådskande fall – polisman att fatta ett interimistiskt beslut. Ett interimistiskt beslut ska skyndsamt prövas av Nämnden.

Bildupptagning genom handhållen kamera är idag inte reglerad särskilt. Ett beslut om att ta en bild kan fattas av enskild polisman oberoende av om det är fråga om förundersökning eller underrättelseverksamhet. Ytterst finns det naturligtvis i allmänna bestämmelser och principer en begränsning av denna allmänna befogenhet (jfr t.ex. de allmänna principer som kommer till uttryck i 8 § polis-

lagen), men några fasta gränser eller särskilda bestämmelser om hur beslut ska fattas finns inte.

När det gäller bildupptagning av den typ som här diskuteras – fotografering inne i (eller in i) ett hem, fotografering av korrespondens etc. – bör emellertid i den kommande regleringen ställas krav på att beslut om bildupptagning som huvudregel ska prövas av undersökningsledaren (i förundersökning) eller av chefen för den brottsbekämpande myndigheten med möjlighet till delegation till personer på chefsnivå (i underrättelseverksamhet).

Eftersom ett behov av bildupptagning kan aktualiseras i situationer där det inte finns möjlighet att invänta ett beslut av undersökningsledaren eller den ordinarie beslutsfattaren inom den brottsbekämpande myndigheten måste det emellertid härutöver finnas en möjlighet för polisman att fatta beslut om det föreligger fara i dröjsmål (särskilt brådskande fall).

I likhet med vad som har föreslagits gällande ljudupptagning bör frågor om bildupptagning prövas av rätten (förundersökning) respektive Nämnden (underrättelseverksamhet) när åtgärden kan antas bli av särskilt ingripande slag. Liksom vad gäller ljudupptagning bör i dessa fall finnas möjlighet för undersökningsledaren (förundersökning) eller chefen för den brottsbekämpande myndigheten (underrättelseverksamhet) och – i särskilt brådskande fall – polisman att fatta interimistiska beslut. Regleringen bör i denna del motsvara den som gäller för ljudupptagning.

10.7 Lokalisering av person

10.7.1 Vad ska befogenheten avse?

Förslag: De brottsbekämpande myndigheterna ska få använda teknisk utrustning som placeras på eller i föremål för att bestämma var en person befinner sig.

Europadomstolen har i målet Uzun mot Tyskland (mål 35623/05, dom av den 2 september 2010) tagit ställning i frågan om användning av pejlingsutrustning i vissa fall kan innebära ett intrång i den enskildes rättigheter enligt artikel 8 i Europakonventionen. Som framgår av praxisgenomgången (se bilaga 3–4 avsnitt 5.3.4) konstaterade domstolen att GPS-övervakning skiljer sig från andra metoder för visuell och akustisk övervakning, eftersom de sistnämnda meto-

derna i regel lättare utgör intrång i en persons rättigheter enligt artikel 8 eftersom de ger mer information om personens beteende, åsikter och känslor. Den GPS-övervakning som Europadomstolen hade att ta ställning till i Uzun-målet utgjorde dock enligt domstolens bedömning ett intrång i rätten till privatliv.

I sin analys av Uzun-avgörandet framhåller Iain Cameron följande (se bilaga 3–4 avsnitt 5.3.4).

> Man kan hävda att domslutet i Uzun-målet inte med nödvändighet innebär att *all* användning av GPS- och liknande utrustning utgör ett intrång i privatlivet. När det gäller Uzun-målet identifierades den övervakade personen och syftet var att övervaka denna person. Andra situationer kan dock identifieras när intrånget i privatlivet inte är lika uppenbart. Exempelvis kan GPS-utrustning eller annan sändare kopplas till ett larm eller till ett objekt som är dolt någonstans, t.ex. en hemlig vapendepå, stöldgods eller en väska som innehåller en lösensumma i ett kidnappningsfall. Samtidigt skulle situationen kunna vara annorlunda om sändaren är kopplad till en mer avancerad utrustning som kan medföra identifiering, t.ex. om man skulle kunna ta bilder med utrustningen med hjälp av fjärrutlösning.
>
> Situationen i Uzun-målet skiljer sig också från ett tänkbart fall där polis eller tulltjänstemän placerar liknande utrustning i t.ex. en container för att spåra stöldgods, smuggelgods eller förfalskade varor. I detta fall skulle syftet normalt vara att spåra det aktuella godset.
>
> En tredje situation som jag skulle vilja påstå skiljer sig från Uzun-målet är om polisen bistår en fordonsägare genom att se till att denne får tillbaka sitt stulna fordon (eller vice versa). Många dyra bilar och lastbilar är utrustade med GPS, som kan användas som en stöldskyddsanordning med vilken ägare eller polis kan spåra ett stulet fordon.
>
> Men även om man kan hävda att användning av GPS-utrustning i sådana eller liknande situationer inte nödvändigtvis utgör ett intrång i privatlivet, så underlättar den naturligtvis visuell övervakning. Och i sådana fall där lagring sker av permanent eller systematisk information som avser visuell övervakning, föreligger det ett intrång. Dessutom måste man ta hänsyn till risken för missbruk. Om polisen fritt kan bestämma över användningen av GPS-utrustning i en typ av situation, finns det naturligtvis en risk för att tillämpningsområdet för denna typ av användning utvidgas i praktiken. Det förnuftiga verkar i detta fall vara att reglera all polisiär användning av GPS-utrustning på ett liknande sätt som för inhämtning av uppgift om elektronisk kommunikation.

I linje med vad som sägs inledningsvis i citatet menar utredningen att enbart det förhållandet att man med hjälp av pejlingsutrustning försöker följa ett visst föremål inte kan anses innebära ett sådant intrång i den enskildes rättigheter enligt artikel 8 i Europakonventionen att det på den grunden krävs en lagreglering. Att använda

pejlingsutrustning för att följa ett parti med narkotika genom att t.ex. fästa utrustningen på ett fordon eller en container kan sålunda inte bedömas kräva annat stöd än det stöd som redan finns (i t.ex. polislagen) gällande de brottsbekämpande myndigheternas uppgifter och allmänna befogenheter. Detta gäller under förutsättning att avsikten med åtgärden inte är att bestämma var en person befinner sig (chauffören kan vara relativt ointressant i sammanhanget) utan att t.ex. följa en narkotikaleverans till en slutdestination och där gripa de inblandade personerna.

Som tidigare utvecklats närmare framstår det emellertid som tydligt att åtgärden i de fall syftet är att följa en viss person måste sägas innefatta ett visst mått av kartläggning av den personens rörelsemönster som i många fall ligger mycket nära den som kan uppnås genom att följa en mobiltelefons lokalisering. Vidare framstår det som tydligt att integritetsaspekten gör sig gällande med större styrka när utrustningen fästs på något som personen kan förväntas bära på sig eller med sig (t.ex. på eller i kläder, skor, plånböcker, handväskor etc.) än när utrustningen fästs t.ex. på en bil eller annat fordon. I det senare fallet är ju möjligheterna att följa personen begränsade till den tid när denne använder det fordonet. Bedömningen att en lokalisering av person mer allmänt kan sägas innebära ett visst intrång i den enskildes integritet vinner stöd av argumentationen i praxisgenomgången, där det dras paralleller till vad som med svensk terminologi är att beteckna som hemlig teleövervakning.

Sammanfattningsvis menar utredningen dels att det finns skäl att reglera möjligheterna att använda teknisk utrustning för lokaliseringsändamål i den utsträckning som åtgärden syftar till att kunna följa en viss person, dels att det finns skäl att laborera med skärpta beslutsregler i de fall där det krävs att utrustningen fästs på något som personen kan förväntas bära på sig eller med sig än i de fall när det är fråga om en mera ”indirekt” lokalisering som bygger t.ex. på att utrustningen fästs på ett fordon som personen kan förväntas använda. När det primära syftet är att följa ett visst föremål eller använda en GPS-sändare på annat sätt än att följa en viss person finns det inte samma starka skäl för en lagreglering. Det är i stället utredningens uppfattning att sådana åtgärder – som i många fall inte heller kan anses utgöra något egentligt intrång i den enskildes rättigheter – normalt inte bör bli föremål för någon särskild lagreglering.

Det finns mot denna bakgrund skäl att föreslå en lagreglering av sådan användning av lokaliseringsutrustning som är att anse som

lokalisering av person, medan annan användning av lokaliseringsutrustning även i fortsättningen ska kunna användas enbart med stöd av de allmänna befogenheterna i polislagen.

10.7.2 När ska befogenheten få användas?

Förslag: I förundersökning ska lokalisering av person få ske om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

I underrättelseverksamhet ska lokalisering av person få ske om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver.

I båda fallen ska förutsättas att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Vad gäller lokalisering av person bör förutsättningarna för åtgärden inom förundersökning motsvara de som gäller för ljud- och bildupptagning. Det ska alltså vara fråga om situationer där åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller mer. På motsvarande sätt bör förutsättningarna för lokalisering av person inom underrättelseverksamheten knytas till den föreslagna regleringen av ljud- och bildupptagning, dvs. åtgärden ska förutsätta att det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver.

Liksom vad gäller upptagning av ljud och bild motiveras skillnaden mellan förundersökning och underrättelseverksamhet av att underrättelseverksamheten har en mer allmän inriktning och att det därför, på sätt som är fallet när det gäller en förundersökning, saknas den begränsning som ligger i kopplingen till ett visst särskilt brott (se även utredningens delbetänkande SOU 2009:1 s. 109).

10.7.3 Vem ska fatta beslut?

Förslag: I förundersökning ska beslut om lokalisering av person fattas av undersökningsledaren eller åklagaren.

I underrättelseverksamhet ska beslut om lokalisering av person fattas av chefen för den brottsbekämpande myndigheten, som ska ha möjlighet att i viss utsträckning delegera beslutanderätten. Sådan delegation ska få ske till annan person på chefsnivå.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller lokalisering av person i situationer där utrustningen placeras på eller i föremål som personen kan antas bära på sig eller ha med sig, eller om åtgärden annars kan antas bli av särskilt ingripande slag, ska frågor om lokalisering av person i förundersökning prövas av rätten på ansökan av åklagaren, med möjlighet för åklagaren eller – i särskilt brådskande fall – polisman att fatta ett interimistiskt beslut. Ett interimistiskt beslut ska skyndsamt prövas av rätten.

Inom ramen för underrättelseverksamhet ska frågor om lokalisering av person, i de fall där rätten fattar beslut inom ramen för en förundersökning, prövas av Nämnden på ansökan av den brottsbekämpande myndigheten. Interimistiska beslut ska i dessa fall kunna fattas av chefen för den brottsbekämpande myndigheten eller – i särskilt brådskande fall – polisman. Ett interimistiskt tillstånd ska skyndsamt prövas av Nämnden.

Lokalisering av person är liksom de tidigare behandlade åtgärderna idag inte reglerad särskilt och beslut om åtgärden kan följaktligen fattas av såväl åklagare som polis. Enligt utredningens mening bör huvudregeln vad gäller lokalisering av person motsvara den som gäller för ljud- och bildupptagning, dvs. att beslut fattas av undersökningsledare eller åklagare (inom förundersökning) och av chefen för den brottsbekämpande myndigheten med möjlighet till delegation (inom underrättelseverksamhet).

När det gäller lokalisering av person i situationer där utrustningen placeras på eller i föremål som personen kan antas bära på sig eller ha med sig, eller om åtgärden annars kan antas bli av särskilt ingripande slag, bör emellertid – på motsvarande sätt som när det gäller ljud- och bildupptagning – beslutet läggas på ett beslutsorgan som är fristående från de brottsbekämpande myndigheterna.

Inom ramen för en förundersökning innebär detta att frågan bör prövas av rätten på ansökan av åklagare och inom ramen för underrättelseverksamhet av Nämnden på ansökan av den brottsbekämpande myndigheten. Också vad gäller lokalisering av person bör det – på motsvarande sätt som vid ljud- och bildupptagning – finnas möjlighet till interimistiska beslut.

10.8 Installation m.m. av lokaliseringsutrustning

10.8.1 Behovet av en reglering

Bedömning: För att på ett effektivt sätt kunna använda lokaliseringsutrustning behöver brottsbekämpande myndigheter kunna få tillgång till skyddade utrymmen för att installera utrustningen. Det finns även ett motsvarande behov av att tillfälligt kunna flytta det föremål på eller i vilket lokaliseringsutrustningen ska placeras samt att kunna vidta vissa andra åtgärder för att utrustningen ska kunna fungera effektivt.

Lokalisering av personer och föremål är en åtgärd som i vissa avseenden skiljer sig från t.ex. ljudupptagning av samtal eller bildupptagningar av skyddade utrymmen. Åtgärden bygger på att viss lokaliseringsutrustning kan placeras i, på, eller i närheten av det objekt som ska lokaliseras. Detta är emellertid inte unikt för just lokaliseringsutrustning. Motsvarande gäller även för hemlig rumsavlyssning. Enligt 6 § lagen om hemlig rumsavlyssning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet bereda sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får dock endast avse den plats som ska avlyssnas.

Regeringen framhöll i propositionen med förslag till lag om hemlig rumsavlyssning (prop. 2005/06:178 s. 104 ff.) att polisen i likhet med vad som gäller enligt bestämmelserna om husrannsakan får ta sig in i det skyddade utrymmet med våld och att polisen – om det anses nödvändigt – får bryta sig in i t.ex. en bostad eller ett annat utrymme som tillståndet gäller för att installera utrustningen. Enligt regeringen innefattar bestämmelsen även en befogenhet för polisen att, när det anses nödvändigt, tillfälligtvis sätta larmanordningar ur funktion, exempelvis genom användning av störningsutrustningar.

Utredningen om utvärdering av vissa hemliga tvångsmedel pekar i betänkandet Utvärdering av buggning och preventiva tvångsmedel (SOU 2009:70 s. 153 f.) på att polisen, när det gäller hemlig rumsavlyssning i fordon, har framhållit att det i vissa situationer finns ett påtagligt behov av att tillfälligt kunna flytta fordonet för att utrustningen ska kunna installeras, eftersom det i många fall inte är möjligt att genomföra en installation där fordonet står uppställt med hänsyn till att detta skulle väcka för stor uppmärksamhet. I betänkandet drog utredningen slutsatsen att en tillfällig förflyttning av ett fordon i syfte att installera avlyssningsutrustning utgjorde ett avsevärt mindre ingrepp i den enskildes integritet än själva avlyssningen och att det därför var rimligt att den myndighet som ska verkställa ett beslut om hemlig rumsavlyssning får möjlighet att flytta det fordon i vilket avlyssningsutrustningen ska installeras. Utredningen framhöll även att säkerhetsskäl ibland kunde motivera att fordonet flyttades. I utvärderingen av hemlig rumsavlyssning och preventiva tvångsmedel framhöll utredningen också behovet av att i vissa situationer tillfälligt kunna sätta larmanordningar ur spel.

När det gäller installation och underhåll av lokaliseringsutrustning gör sig i många fall samma frågor gällande som när det gäller buggningsutrustning. Utredningen har erfarit att det finns behov av att kunna ta sig in i skyddade utrymmen och även störa ut larmanläggningar för att kunna installera lokaliseringsutrustning. Utredningen har vidare erfarit att det många gånger kan finnas behov av att vidta åtgärder för att lokaliseringsutrustningen ska kunna fungera under längre perioder utan underhåll. Sådana åtgärder handlar normalt om icke förstörande ingrepp i det aktuella föremålet.

10.8.2 Vad ska befogenheten avse?

Förslag: De brottsbekämpande myndigheterna ska för att installera, underhålla eller avlägsna teknisk utrustning för lokalisering i hemlighet kunna

1. bereda sig tillträde till en plats som annars skyddas mot intrång,
2. tillfälligt flytta det föremål på eller i vilket utrustningen ska placeras eller finns placerad, samt
3. vidta de andra åtgärder som behövs för att utrustningen ska fungera effektivt.

På motsvarande sätt som när det gäller installation av buggningsutrustning bör brottsbekämpande myndigheter kunna i hemlighet bereda sig tillträde till en plats som annars skyddas mot intrång för att ha möjlighet att installera, underhålla eller avlägsna teknisk utrustning för lokalisering. Det handlar huvudsakligen om det som skyddas genom bestämmelserna i 4 kap. 6 § BrB om hemfridsbrott och olaga intrång. I fråga om hemfridsbrott skyddas inte endast en bostad utan också en trädgård som hör till bostaden. Arbetsplatser, föreningslokaler och trappuppgångar nämns i förarbetena som exempel på lokaler som omfattas av skyddet i bestämmelsen om olaga intrång (se NJA II 1962 s. 133). Även offentliga lokaler som på dagtid står öppna för allmänheten torde omfattas av bestämmelsen under tider då lokalen är stängd. I likhet med vad som gäller för installation av buggningsutrustning bör befogenheten även innefatta att polisen, när det är nödvändigt, får sätta larmanordningar ur funktion, exempelvis genom användning av störningsutrustning.

Som ovan anförts konstaterade Utredningen om utvärdering av vissa hemliga tvångsmedel att det fanns ett påtagligt behov av att kunna flytta ett fordon för att kunna installera buggningsutrustning, eftersom det i många fall inte är möjligt att genomföra en installation där fordonet står uppställt. På motsvarande sätt har, när det gäller installation av lokaliseringsutrustning, kunnat konstateras ett behov av att tillfälligt kunna flytta ett fordon eller annat föremål.

Som framhållits tidigare har utredningen även kunnat konstatera ett behov av att kunna vidta åtgärder för att lokaliseringsutrustningen ska kunna fungera under längre perioder utan underhåll. Sådana åtgärder handlar normalt om icke förstörande ingrepp i det aktuella föremålet.

Behoven av dessa åtgärder är inte kopplade enbart till lokalisering av person utan gör sig med samma styrka gällande även när det gäller lokalisering av föremål. Regleringen bör därför utformas så att befogenheterna att vidta de aktuella installationsåtgärderna inte knyts till bestämmelserna om lokalisering av person utan ges generell tillämplighet vid installation av lokaliseringsutrustning.

10.8.3 Vem ska fatta beslut?

Förslag: I förundersökning ska beslut om tillträde till skyddade utrymmen m.m. för installation av lokaliseringsutrustning fattas av undersökningsledaren eller åklagaren.

I underrättelseverksamhet ska beslut om tillträde till skyddade utrymmen m.m. för installation av lokaliseringsutrustning fattas av chefen för den brottsbekämpande myndigheten, som ska ha möjlighet att i viss utsträckning delegera beslutanderätten. Sådan delegation ska få ske till annan person på chefsnivå.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller lokalisering av person i situationer där utrustningen placeras på eller i föremål som personen kan antas bära på sig eller ha med sig, eller om åtgärden annars kan antas bli av särskilt ingripande slag, ska den beslutsordning som gäller för beslutet om lokalisering även gälla för beslut om tillträde till skyddade utrymmen m.m. för installation av lokaliseringsutrustning.

Till skillnad från vad som gäller för användandet av lokaliseringsåtgärder, som redan nu används av polisen, är möjligheten att få tillträde till skyddade utrymmen en ny befogenhet. När det gäller frågan om vem som ska fatta beslut om åtgärden gör utredningen bedömningen att beslutsbefogenheten för installationsåtgärder bör följa befogenheten att besluta om lokalisering av person. Det bör gälla även för sådana lokaliseringsåtgärder som inte avser person och som därför inte omfattas av regleringen i den föreslagna lagens 2 kap. men väl enligt den här aktuella bestämmelsen.

Detta innebär att beslut om installationsåtgärder i förundersökning får fattas av undersökningsledaren eller åklagaren med beslutanderätt för polisman när det föreligger fara i dröjsmål. I underrättelseverksamhet får beslut om installationsåtgärder fattas av chefen för den brottsbekämpande myndigheten med viss delegationsmöjlighet. Även i underrättelseverksamhet ska polisman kunna fatta beslut om installationsåtgärder om det föreligger fara i dröjsmål.

Om den lokaliseringsåtgärd som föranleder installation av utrustningen är av sådant särskilt ingripande slag att den kvalificerade beslutordningen med tillstånd av rätten respektive Nämnden ska tillämpas, så ska samma beslutsordning tillämpas även för beslut om installa-

tionsåtgärder. Det innebär att beslutet om installationsåtgärder normalt sett ska fattas av samma instans som fattar beslutet om lokalisering. I vissa situationer kan dock besluten fattas av olika instanser. Det handlar om att det, när beslut om lokaliseringsåtgärder fattades, inte gick att förutse att det skulle krävas beslut om särskilda installationsåtgärder eller underhållsåtgärder. Om det i en sådan situation på grund av fara i dröjsmål inte finns möjlighet att inhämta beslut från t.ex. åklagaren eller rätten kan polisman fatta dessa beslut.

10.9 Vissa gemensamma bestämmelser

Förslag: Ett beslut om tillstånd till ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person eller särskilda befogenheter vid installation av lokaliseringsutrustning ska inte få bestämmas till längre tid än nödvändigt. Tiden ska inte få överstiga tre månader från dagen för beslutet.

Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Om det inte längre finns skäl för åtgärden ska beslutet omedelbart hävas.

Ett beslut om tillstånd till ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person eller särskilda befogenheter vid installation av lokaliseringsutrustning bör inte få bestämmas till längre tid än nödvändigt. Det kan givetvis inte krävas att det anges exakt när åtgärderna ska vidtas. Istället bör det vara tillräckligt att tillståndet begränsas till att gälla en viss tidsperiod som förslagsvis bör kunna vara maximalt tre månader. Tiden har valts med hänsyn till att många spaningsoperationer regelmässigt pågår under längre tid och att integritetsintrånget typiskt sett inte är så stort som vid hemliga tvångsmedel, där tillståndstiden är maximerad till en månad. Det framstår därför inte som ändamålsenligt att i lagtext föreskriva en kortare maximal tillståndstid än tre månader.

Det finns inget som hindrar att tiden för tillståndet sätts till en kortare tid än tre månader. Den tidsmässiga begränsningen av tillståndets längd hindrar inte heller att tillstånd ges på nytt. Tvärtom

får antas att operationer som sträcker sig över längre perioder än tre månader inte kommer att bli ovanliga.

En prövning ska alltid göras av i vilken utsträckning ett tillstånd ska förenas med sådana villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Vilka villkor det kan vara fråga om får avgöras från fall till fall.

11 Identifiering och störning av mobil elektronisk kommunikationsutrustning m.m.

11.1 Bakgrund

11.1.1 Uppdraget

Utredningen ska enligt direktiven överväga i vad mån den användning av tekniska metoder som i dag förekommer hos de brottsbekämpande myndigheterna bör regleras i lag. Utredningen ska särskilt överväga behovet av författningsreglering när det gäller polisens och tullens möjligheter att inhämta uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel i syfte att identifiera viss teknisk utrustning, t.ex. en mobiltelefon.

11.1.2 Användning av egen utrustning för att identifiera mobil elektronisk kommunikationsutrustning m.m.

Vid de brottsbekämpande myndigheterna förekommer en relativt omfattande användning av s.k. IMSI-catcher.

En IMSI-catcher är ett tekniskt hjälpmedel som närmast kan betraktas som en mobil basstation för mobiltelefoni. Den ger uppgift om IMSI- och IMEI-numren avseende de mobiltelefoner som finns i närheten av den. Ett IMSI-nummer (International Mobile Subscriber Identity) är kopplat till abonnentens telefonnummer medan IMEI-numret (International Mobile Equipment Identity) ger uppgift om identiteten på utrustningen (hårdvaran). Båda typerna av nummer betraktas som en teleadress och kan därför ligga till grund för beslut om hemlig teleavlyssning eller hemlig teleövervakning (jfr 27 kap. 18–20 §§ RB).

Typexempel på när en IMSI-catcher används är för att identifiera vilka mobiltelefoner som används av personer som är föremål för hemlig teleavlyssning men försöker undgå avlyssningen genom att skifta mellan ett antal telefoner och kontantkort. Bakgrunden till detta är framför allt den stora användningen av anonyma kontantkort i mobiltelefoner som används vid brottslig verksamhet och att tillstånd till hemlig teleavlyssning och hemlig teleövervakning inte kan ges utan att teleadressen anges i tillståndet (se 27 kap. 21 § andra stycket RB). Dessutom behöver teleoperatören få kunskap om den specifika teleadressen för att över huvud taget kunna verkställa tvångsmedelsbesluten. Säkerhetspolisen har i denna del hänvisat till vad myndigheten anförde om behovet av metoden i samband med att BRU utredde frågan (SOU 2005:38) och framhållit att behovet inte har minskat.

IMSI-catchern ger kännedom inte enbart om den mobiltelefon som är intressant för sökningen utan även om andra mobiltelefoner som används i närheten. Allt efter omständigheterna kräver då detta att den fysiska spaningen fortsätter och att det sker fler sökningar i området kring den mobiltelefon som ska ”ringas in”. Det sker genom en jämförelse mellan uppgifterna från de olika platserna. Det geografiska området i vilka de korta sökningarna sker (någon enstaka sekund) kan begränsas genom att utrustningens räckvidd justeras efter förhållandena på platsen. Utgångspunkten är då är att den fysiska spaningen visar var inom ett klart begränsat område den mobiltelefon finns som man vill ha uppgift om. I stadsmiljö kan det i praktiken röra sig om en radie på högst ett hundratal meter.

En IMSI-catcher kan användas för att lokalisera en mobiltelefon till ett mycket snävare område än vad som är möjligt genom information som kan erhållas från teleoperatörerna. Detta användningssätt är mycket effektivt också när det gäller att söka efter och lokalisera personer som försvunnit, kidnappats eller av andra skäl måste kunna lokaliseras.

På motsvarande sätt kan IMSI-catchern användas för att kontrollera om en person mot vilken det bedrivs spaning, eller mer korrekt en viss mobiltelefon, befinner sig på en viss plats.

Samtliga åtgärder sker genom att IMSI-catchern identifierar vilka mobiltelefoner eller andra mobila kommunikationsutrustningar, t.ex. modem för mobilt bredband, som finns inom ett visst geografiskt område. När metoden används har det hittills skett med stöd av principen om att etern är fri (se avsnitt 3.1.7).

IMSI-catchern fungerar tekniskt på så sätt att den under en mycket kort tid presenterar sig som en basstation för mobiltelefoner i närheten av den. Genom detta blir det klarlagt vilka IMSI- eller IMEI-nummer och därmed vilka teleadresser som är aktiva i området. Det är inte nödvändigt att mobiltelefonen är uppkopplad för samtal utan det räcker med att den är påslagen.

11.1.3 Störning av mobil elektronisk kommunikation m.m.

En störsändare är ett tekniskt hjälpmedel som genom att sända störande radiosignaler på vissa frekvenser kan hindra kommunikation till och från en mobiltelefon som befinner sig i närheten av störsändaren. Det kan också handla om att på motsvarande sätt hindra kommunikation som sker t.ex. via s.k. bluetooth, trådlösa nätverk eller radiosändare.

I propositionen Hemlig rumsavlyssning (prop. 2005/06:178 s. 104 f.) angav regeringen att polisen, när det är nödvändigt i samband med installation av tekniska hjälpmedel, ska få sätta larmanordningar ur funktion, exempelvis genom användning av störningsutrustning. Någon förändring i förordningen (2003:396) om elektronisk kommunikation som skulle möjliggöra detta har dock inte gjorts i samband med det lagstiftningsärendet. Senare har Utredningen om utvärdering av vissa hemliga tvångsmedel dragit slutsatsen att störningsutrustning bör få användas vid verkställighet av beslut om hemlig rumsavlyssning (se SOU 2009:70 s. 153) men samtidigt hänvisat till den här utredningen för ytterligare överväganden i samband med behandling av andra tekniska metoder.

Enligt 14 § förordningen om elektronisk kommunikation gäller dock ett förbud mot att inneha elektriska eller elektroniska anläggningar som, utan att vara radioanläggningar, är avsedda att sända radiovågor i annat syfte än för kommunikationsändamål i ledning eller för industriellt, vetenskapligt eller något annat liknande syfte (se 3 kap. 14 § första stycket LEK). Förbudet gäller dock inte sådana anläggningar som behövs i verksamhet som bedrivs av Försvarsmakten, Försvarets radioanstalt eller Försvarets materielverk. Dessutom får Post- och telestyrelsen efter ansökan av Kriminalvården besluta att förbudet inte ska gälla viss sådan anläggning som behövs i en anstalt eller ett häkte inom kriminalvården för att hindra otillåten mobiltelefonkommunikation, om anläggningen kan användas utan att skadlig störning uppstår utanför anstalten eller häktet.

Det är således inte tillåtet för de brottsbekämpande myndigheterna att inneha och därmed inte heller använda utrustning för störande av radiosignaler (frånsett i nödsituationer).

I mars 2005 hemställde Säkerhetspolisen i en skrivelse till regeringen om en förordningsändring så att myndigheten, för test- och försöksverksamhet, skulle undantas från förbudet att inneha vissa elektroniska anläggningar, inkluderande störningsutrustningar. Någon ändring av förordningen har dock inte skett.

11.1.4 Användning av IMSI-catcher i vissa andra länder

I *Danmark* är användning av IMSI-catcher (telefonskanning) tillåten endast som nödåtgärd vid t.ex. en extraordinär situation i syfte att avvärja en terrorhandling. År 2006 lämnade Strafferetsplejeudvalget ett förslag om att införa en särskild reglering om telefonskanning i retsplejeloven. Förslaget har dock inte lett till lagstiftning.

I *Finland* är användning av IMSI-catcher tillåten genom bestämmelsen i 36 § polislagen. Genom den får polisen rätt att använda tekniska anordningar för att inhämta information som identifierar teleanslutningar och teleterminalutrustningar.

Även i *Norge* är användning av IMSI-catcher uttryckligen tillåten enligt 216 b § första och andra styckena i straffeprocessloven. Enligt de bestämmelserna får rätten ge tillstånd till ”annen kontroll av kommunikationsjonsanlegg” när någon är misstänkt för ett brott som kan föranleda fem års fängelse eller mer eller när det är fråga om vissa specifikt angivna brott. En sådan typ av kontroll kan enligt lagtexten vara att med hjälp av teknisk utrustning identifiera telefoner.

Användning av IMSI-catcher är också tillåten i Estland, Grekland, Litauen, Luxemburg, Nederländerna, Storbritannien, Tjeckien, Tyskland och Ungern.

Belgien och Slovenien tillåter inte användning av IMSI-catcher. Slovakien och Spanien har uttryckt att användningen av IMSI-catcher inte är reglerad.

11.1.5 Användning av störsändare i vissa andra länder

I *Danmark* är användningen av störsändare tillåten genom regleringen i retsplejelovens 791 c §. För att förhindra terrordåd eller andra allvarliga brott har det införts en bestämmelse om störning eller avbrytande av radio- eller telekommunikation. Enligt bestämmelsen får polisen störa eller avbryta radio- eller telekommunikation om det finns tvingande skäl att göra så för att förhindra brott med fängelse i 6 år eller däröver i straffskalan eller brott mot strafflagens 12 och 13 kap. (terrorbrott m.m.). Det är också en förutsättning att brottet kan äventyra människors liv eller hälsa eller riskera betydande samhälleliga värden. Beslut fattas av domstol med interimistisk beslutanderätt för polisen.

I *Norge* pågår arbetet med att införa så kallade mobilregulerte soner för identitetsfangning eller jamming (identifiering eller störning) inom vilka polisen ska kunna använda störsändare. Arbetet med att anpassa kommunikationslagstiftningen pågår.

11.2 Överväganden och förslag

11.2.1 Vad ska befogenheten avse?

Identifiering

Förslag: De brottsbekämpande myndigheterna ska med tekniska hjälpmedel för sändning eller mottagning av radiovågor få identifiera vilken mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som befinner sig inom ett visst geografiskt område.

Utredningen kan konstatera att IMSI-catchern är ett numera mycket viktigt hjälpmedel för att polisen ska ha möjlighet att bedriva effektiv spaning mot vissa former av avancerad brottslighet. Det rör sig om framför allt om välplanerad, allvarlig brottslighet där gärningsmännen på olika sätt försöker försvåra polisens spaning, t.ex. genom att kontinuerligt skifta mellan ett flertal mobiltelefoner och telefonabonnemang. Med det regelverk som styr möjligheterna till hemlig teleavlyssning och hemlig teleövervakning innebär sådant agerande problem för de brottsbekämpande myndigheterna. Hemlig teleavlyssning och hemlig teleövervakning, som båda är viktiga verktyg

för de brottsbekämpande myndigheterna, måste enligt 27 kap. 18–20 §§ RB avse en viss teleadress, dvs. ett abonnemang, en enskild anknytning, adressen för elektronisk post, en kod eller någon annan identifieringsmetod, som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte.

I utredningens delbetänkande (SOU 2009:1 s. 94 f.) framhölls det förhållandet att personer som var involverade i vissa kriminella aktiviteter köper, byter och slänger mobiltelefoner eller anonyma kontantkort mycket frekvent som en av de stora anledningarna till att det fattas relativt många beslut om att inhämta uppgifter om elektronisk kommunikation enligt 6 kap. 22 § första stycket 3 LEK. Vidare angavs att myndigheterna behövde få fram vilka teleadresser som användes, bl.a. genom basstationstömning, för att kunna få tillstånd till hemlig teleavlyssning och hemlig teleövervakning. Företrädare för Säkerhetspolisen, Rikskriminalpolisen och länskriminalpolisen i Stockholm hade uttryckt till BRU (SOU 2005:38 s. 210 f.) att anonyma kontantkort utgör ett av de absolut största effektivitetshindren vid utredning av grova brott. De anonyma kontantkorten och kravet på att teleadresser ska vara identifierade för att tvångsmedlen ska kunna beslutas och verkställas skapar så stora problem i brottsutredningarna att det betecknades som ”en utredningsmässig, tidsmässig och resursmässig katastrof”. Det sades att det läggs ned ”fruktansvärt stora resurser” på att på olika sätt ändå identifiera de teleadresser som används av brottslingarna och att arbetet med någon enstaka teleadress kan engagera en mängd personer under flera veckors tid, vilket kostar mycket pengar samtidigt som brottsutredningsarbetet tappar markant i effektivitet. Det finns dessutom enligt myndigheterna en uppenbar risk för att arbetet med att identifiera teleadresserna blir resultatlöst, vilket innebär att bl.a. hemlig teleövervakning över huvud taget inte kan användas i arbetet med att utreda grova brott.

Som beskrivits i avsnitt 11.1.2 är IMSI-catchern ett tekniskt hjälpmedel för identifiering av mobila elektroniska kommunikationsutrustningar som närmast kan betraktas som en portabel basstation för mobiltelefoni. En IMSI-catcher kan presentera uppgifter om vilka IMSI- och IMEI-nummer de mobiltelefoner och annan motsvarande utrustning har, som finns i närheten av den. I detta avseende finns det likheter med den information som man kan få tillgång till vid s.k. basstationstömningar.

Enligt vad som beskrivits för utredningen skiljer sig dock användningen av IMSI-catchern väsentligt ifrån en hemlig teleövervakning. En skillnad är att IMSI-catchern används som ett operativt spaningshjälpmedel snarare än ett verktyg för inhämtning av bevisning. Detta påverkar också graden av integritetsintrång. IMSI-catchern används främst för att sortera ut relevanta kommunikationsutrustningar genom att göra flera sökningar på olika platser. Genom detta förfarande kan man sortera bort uppgifter om alla kommunikationsutrustningar som inte bedöms vara intressanta. Genom att kombinera användandet av en IMSI-catcher med traditionell fysisk spaning är det möjligt att på ett mycket effektivt och kostnadsbesparande sätt ta reda på vilka kommunikationsutrustningar och abonnemang en viss person använder sig av, eller var personen befinner sig. Detta sker utan att generera sådana stora mängder information om kommunikationsutrustningar som inte är relevanta för utredningen som blir resultatet av en basstationstömning. Sett i detta perspektiv innebär användningen av en IMSI-catcher ett mindre integritetsintrång än en basstationstömning. Vidare kan framhållas att en IMSI-catcher kan justeras i sändningsstyrka så att det geografiska område som täcks in av utrustningen inte blir mer vidsträckt än nödvändigt. Denna möjlighet finns inte vid en basstationstömning.

Det bör även framhållas att en IMSI-catcher använd med hög sändningsstyrka i centrala delarna av en stad skulle kunna hämta in uppgifter om ett relativt stort antal mobila kommunikationsutrustningar. Detta användningssätt framstår dock inte som ändamålsenligt ur de brottsbekämpande myndigheternas perspektiv. Att täcka in större områden med ett stort antal kommunikationsutrustningar kan dessutom anses tveksamt från proportionalitetssynpunkt. Vidare bör också framhållas att en IMSI-catcher, på grund av den justerbara sändningsstyrkan, kan skilja ut ett avsevärt mindre område inom vilket en viss kommunikationsutrustning finns än vad som är möjligt med hjälp av en basstationstömning. Detta är självfallet mycket värdefullt för de brottsbekämpande myndigheterna men en mer preciserad positionering skulle också kunna uppfattas som ett större integritetsintrång.

Sammantaget anser utredningen dock att det integritetsintrång som uppstår genom användandet av en IMSI-catcher normalt är avsevärt mindre än vid en basstationstömning eller en hemlig teleövervakning. Mot bakgrund av IMSI-catcherns betydelse som hjälpmedel för de brottsbekämpande myndigheterna bör en fortsatt möj-

lighet att använda sådan utrustning säkerställas. Användandet bör regleras i den särskilda inhämtningslag som utredningen föreslår.

Störning

Förslag: Brottsbekämpande myndigheter ska få inneha tekniska hjälpmedel för sändning eller mottagning av radiovågor och med sådan utrustning få störa kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som befinner sig inom ett visst geografiskt område.

De brottsbekämpande myndigheterna har ett behov av att kunna inneha och använda störsändare t.ex. för att störa mobiltrafik vid ingripanden mot kriminella, för att störa ut larmsystem och webbkamerautrustning i samband med intrång, exempelvis vid installation av buggningsutrustning, eller för att förhindra att bomber exploderar vid misstanke om ett förestående terrorbrott. Som nyss nämndes har behovet av att kunna använda metoden i brottsbekämpningen påtalats i flera olika sammanhang. Den reglering som i dag finns och som innebär att de brottsbekämpande myndigheterna inte får inneha och använda utrustningen bör förändras så att detta blir möjligt.

En användning av utrustning för att störa ut radiosignaler får närmast ses som en del av verkställigheten av andra åtgärder som hemlig rumsavlyssning eller lokalisering. Att störa ut larmsystem och webbkamerautrustning i samband med intrång i syfte att installera teknisk utrustning kan inte anses innebära något ytterligare intrång i den enskildes rättigheter enligt Europakonventionen utöver vad själva tillträdet för installationen innebär. Befogenheten att använda störsändare i dessa sammanhang följer av 6 § lagen (2007:978) om hemlig rumsavlyssning samt av den i kapitel 9 föreslagna bestämmelsen om tillträde till vissa utrymmen för att installera tekniska hjälpmedel för lokalisering.

Enligt utredningens uppfattning förhåller det sig dock annorlunda när störsändare används för att slå ut t.ex. mobiltelefoner eller datorer med trådlös Internetuppkoppling. I dessa fall kan åtgärden att hindra kommunikationen ses som ett intrång i rätten till korrespondens enligt Europakonventionens artikel 8. En sådan rätt får endast inskränkas med stöd av lag och om det i ett demokratiskt

samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Utredningen gör bedömningen att den ovannämnda användningen av störsändare generellt kan anses godtagbar enligt dessa kriterier. Sådan användning som riskerar att komma i konflikt med artikel 8 bör därför regleras i lag. Det handlar alltså om situationer där man begränsar personers rätt till kommunikation och inte om sådana situationer där en störsändare enbart används för att slå ut ett larm eller en övervakningskamera.

11.2.2 När ska befogenheten få användas?

Identifiering

Förslag: I en förundersökning ska identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation få ske endast om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

I underrättelseverksamhet ska identifiering av mobil elektronisk kommunikationsutrustning m.m. få ske endast om undersökningen innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver och det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Användningen av IMSI-catcher är som framgått en polisiär spaningsmetod som huvudsakligen syftar till att inhämta sådan information som många gånger är nödvändig för att senare kunna begära beslut om hemlig teleavlyssning eller hemlig teleövervakning. Åtgärderna används såväl i förundersökningar som i underrättelseverksamhet.

I utredningens delbetänkande (SOU 2009:1) föreslogs att de brottsbekämpande myndigheterna ska få tillgång till uppgifter om vilka mobiltelefoner som har befunnit sig i ett visst område både i förundersökning och i underrättelseverksamhet. Till skillnad från vad som gäller för närvarande föreslog utredningen att tillgången till lokaliseringsuppgifter även skulle omfatta uppgifter rörande mobil-

telefoner som inte varit uppkopplade för kommunikation utan enbart varit påslagna.

Med hänsyn till att de uppgifter som erhålls genom de tekniska hjälpmedlen i viss utsträckning kan sägas överensstämma med sådana uppgifter om lokalisering som man enligt förslaget i utredningens delbetänkande ska kunna erhålla från teleoperatörerna finns det vissa skäl att knyta an till de förutsättningar som gäller för sådan inhämtning. Mot detta talar dock, som ovan anförts, att inhämtning av uppgifterna med egna tekniska hjälpmedel normalt avser betydligt kortare tidsperioder och inte kan anses utgöra ett lika stort integritetsintrång som t.ex. en basstationstömning. Framhållas bör också att det framför allt handlar om ett spaningshjälpmedel, inte ett verktyg för bevisinhämtning.

Sammantaget anser därför utredningen att förutsättningarna för inhämtning av uppgifter om vilken mobil elektronisk kommunikationsutrustning som befinner sig inom ett visst geografiskt område genom tekniska hjälpmedel för sändning eller mottagning av radiovågor bör överensstämma med vad som enligt utredningens förslag ska gälla för ljud- och bildupptagning samt för lokalisering av person.

Det ska alltså vara fråga om situationer där åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller mer. På motsvarande sätt bör förutsättningarna inom underrättelseverksamhet knytas till den föreslagna regleringen av ljud- och bildupptagning samt lokalisering av person, dvs. att det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver.

Liksom vad gäller upptagning av ljud och bild samt lokalisering av person motiveras skillnaden mellan förundersökning och underrättelseverksamhet av att underrättelseverksamheten har en mer allmän inriktning och att det därför, på sätt som är fallet när det gäller en förundersökning, saknas den begränsning som ligger i kopplingen till ett visst särskilt brott.

Störning

Förslag: I förundersökning ska störning av kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation få ske endast om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

I underrättelseverksamhet ska sådan störning få ske endast om undersökningen innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver och det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

I befogenheten att bereda sig tillträde till viss plats för att installera buggningsutrustning finns en möjlighet att använda störningsutrustning. Utredningen föreslår i avsnitt 10.8.2 att en sådan befogenhet även ska finnas vid installation av lokaliseringsutrustning. Ett sådant användningsområde kan inte i det sammanhanget anses utgöra något ytterligare intrång i den enskildes rättigheter. Detta medför att 14 § förordningen om elektronisk kommunikation bör ändras så att polisen även får inneha störningsutrustningen.

I än högre grad än när det gäller identifiering utgör störning ett operativt hjälpmedel för polisen snarare än ett verktyg för bevisinhämtning. Det kan dock enligt utredningens mening förväntas att användningen av störsändare i andra syften än att störa ut larm vid installation av övervakningsutrustning kommer att tillämpas i mycket ringa omfattning och framförallt vid mycket allvarlig brottslighet eller i vad som får betraktas som rena nödsituationer.

När det gäller frågan vilka förutsättningar som bör gälla för att de brottsbekämpande myndigheterna, utöver vad som följer av t.ex. lagen om hemlig rumsavlyssning, ska få använda störsändare gör utredningen bedömningen att dessa bör motsvara vad som föreslås gälla för identifiering av mobil elektronisk utrustning. Detta innebär att störning av mobil elektronisk kommunikationsutrustning eller annan radioutrustning i förundersökning ska få ske endast om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver. På motsvarande sätt ska det i underrättelseverksamhet krävas att undersökningen innefattar brottslig verksamhet för vilket är föreskrivet fängelse i ett år eller däröver och det finns särskild anledning att

anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

11.2.3 Vem ska fatta beslut?

Identifiering

Förslag: I en förundersökning ska beslut om identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation fattas av undersökningsledare eller åklagare.

I underrättelseverksamhet ska beslut om sådan identifiering fattas av chefen för polismyndigheten, som ska ha möjlighet att delegera beslutanderätten.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller frågan om sådan identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som kan antas bli av särskilt ingripande slag, ska frågor om sådan identifiering prövas av rätten på ansökan av åklagaren. Det ska finnas möjlighet för åklagaren eller – i särskilt brådskande fall – polisman att fatta interimistiska beslut. Ett interimistiskt beslut ska skyndsamt prövas av rätten.

I underrättelseverksamhet ska frågor om identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, i de fall där rätten fattar beslut inom ramen för en förundersökning, prövas av Nämnden på ansökan av polismyndigheten. Interimistiska beslut ska i dessa fall kunna fattas av chefen för polismyndigheten med rätt till delegation eller – i särskilt brådskande fall – av polisman. Ett interimistiskt tillstånd ska skyndsamt prövas av Nämnden.

Som tidigare framhållits sker identifiering av mobil elektronisk kommunikationsutrustning i nuläget med stöd av principen om att eterburen radiokommunikation är fri att ta del av och är idag inte reglerad särskilt. Beslut att använda utrustning för identifiering av mobil elektronisk kommunikationsutrustning fattas i samråd mellan polismyndigheterna och Rikskriminalpolisen eller Säkerhetspolisen. Utrustningens avancerade natur och det förhållandet att det finns förhållandevis få exemplar av den tekniska utrustningen gör att

besluten om hur användningen ska prioriteras får relativt stor betydelse.

Eftersom behovet att med hjälp av egen teknisk utrustning kunna identifiera mobil elektronisk kommunikationsutrustning ofta uppkommer med kort varsel och behöver verkställas skyndsamt, i normalfallet även kompletteras med traditionell fysisk spaning och inte framstår som särskilt integritetskränkande, bör beslutsfattandet inte ske på för hög nivå. Även om de uppgifter som kan erhållas med identifieringsutrustningen på många sätt kan jämföras med sådana uppgifter som kan inhämtas med hjälp av hemlig teleövervakning finns det också skillnader både i avseende på i vilka situationer respektive metod används och hur resultatet kan utnyttjas. Identifieringsutrustningen används som framhållits ovan framförallt som ett operativt spaningshjälpmedel för att kunna påbörja eller fortsätta en pågående hemlig teleavlyssning eller hemlig teleövervakning eller för att lokalisera personer genom att kunna bestämma var deras mobiltelefoner befinner sig. Eftersom det alltså är ett operativt spaningsverktyg snarare än ett utredningsverktyg vars uppgifter är avsedda att i någon vidare utsträckning ligga till grund för lagföringen finns det, om beslutsnivån i normalfallet läggs för högt, t.ex. hos rätten i en förundersökning, en uppenbar risk att nyttan med identifieringsutrustningen omintetgörs.

Sammantaget gör detta att utredningen gör bedömningen att beslutanderätten bör ligga så nära den operativa verksamheten som möjligt. Beslut om identifiering av mobil elektronisk kommunikationsutrustning i förundersökning bör därför fattas av undersökningsledare eller åklagare och i underrättelseverksamhet av chefen för den brottsbekämpande myndigheten med möjlighet för denne att delegera beslutsfattandet till annan tjänsteman vid myndigheten om han eller hon har den kompetens, utbildning och erfarenhet som behövs.

När fråga är om identifiering av mobil elektronisk kommunikationsutrustning i situationer där åtgärden kan antas bli av särskilt ingripande slag bör dock – på motsvarande sätt som när det gäller ljud- och bildupptagning samt lokalisering av person – beslutet läggas på ett beslutsorgan som är fristående från de brottsbekämpande myndigheterna. Inom ramen för en förundersökning innebär detta att frågan bör prövas av domstol på ansökan av åklagare och inom ramen för underrättelseverksamhet av Nämnden på ansökan av polismyndigheten. I dessa fall ska dock på motsvarande sätt som vid andra särskilda inhämtningsåtgärder finnas möjligheter till interim-

istiska beslut av åklagare (förundersökning), chefen för den brottsbekämpande myndigheten (underrättelseverksamhet) eller – i särskilt brådskande fall – av polisman. Rätten respektive Nämnden ska skyndsamt pröva det interimistiska beslutet.

Störning

Förslag: I en förundersökning ska beslut om störning av kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation fattas av undersökningsledare eller åklagare.

I underrättelseverksamhet ska beslut om sådan störning fattas av chefen för polismyndigheten, som ska ha möjlighet att delegera beslutanderätten.

I såväl förundersökning som underrättelseverksamhet ska vid fara i dröjsmål beslut kunna fattas av polisman.

När det gäller sådan störning av kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som kan antas bli av särskilt ingripande slag, ska frågor om sådan identifiering prövas av rätten på ansökan av åklagaren. Det ska finnas möjlighet för åklagaren eller – i särskilt brådskande fall – polisman att fatta interimistiska beslut. Ett interimistiskt beslut ska skyndsamt prövas av rätten.

I underrättelseverksamhet ska frågor om störning, i de fall där rätten fattar beslut inom ramen för en förundersökning, prövas av Nämnden på ansökan av polismyndigheten. Interimistiska beslut ska i dessa fall kunna fattas av chefen för den polismyndigheten med rätt till viss delegation eller – i särskilt brådskande fall – av polisman. Ett interimistiskt tillstånd ska skyndsamt prövas av Nämnden.

Till skillnad från identifiering av mobil elektronisk kommunikationsutrustning använder de brottsbekämpande myndigheterna inte störsändare för närvarande. Det finns dock påtagliga likheter vad gäller förutsättningarna för användandet.

Eftersom behovet att kunna störa mobil elektronisk kommunikationsutrustning ofta uppkommer med kort varsel och därför kan behöva verkställas skyndsamt bör beslutsfattandet inte läggas på för hög nivå. Dock måste vägas in att en störsändning med stark

effekt kan påverka ett större antal människor och att effekterna för dessa människor kan vara svåra att förutse för beslutsfattaren. Det är därför av särskild vikt att övervägandena och avvägningarna som behöver göras inför ett beslut om användning av störsändare görs noggrant. Utredningen gör ändå bedömningen att beslutanderätten bör ligga nära den operativa verksamheten. Beslut om störning av mobil elektronisk kommunikationsutrustning i förundersökning bör, på motsvarande sätt som vad som föreslås för identifiering, fattas av undersökningsledare eller åklagare och i underrättelseverksamhet av chefen för den brottsbekämpande myndigheten med möjlighet för denne att delegera beslutsfattandet till annan tjänsteman på chefsnivå eller motsvarande.

När fråga är om störning av mobil elektronisk kommunikationsutrustning i situationer där åtgärden kan antas bli av särskilt ingripande slag bör dock – på motsvarande sätt som när det gäller identifiering – beslutet läggas på ett beslutsorgan som är fristående från de brottsbekämpande myndigheterna. Inom ramen för en förundersökning innebär detta att frågan bör prövas av domstol på ansökan av åklagare och inom ramen för underrättelseverksamhet av Nämnden på ansökan av polismyndigheten. Det bör dock i dessa fall finnas möjlighet för åklagare vid förundersökning, chefen för den brottsbekämpande myndigheten i underrättelseverksamhet eller – i särskilt brådskande fall – polisman att vid fara i dröjsmål fatta interimistiskt beslut om åtgärden. Ett sådant interimistiskt beslut ska sedan skyndsamt prövas av domstolen respektive Nämnden.

11.3 Vissa gemensamma bestämmelser

Förslag: Ett beslut om tillstånd till identifiering eller störning av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation ska inte få bestämmas till längre tid än nödvändigt. Tiden ska inte få överstiga tre månader från dagen för beslutet.

Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Om det inte längre finns skäl för åtgärden ska beslutet om denna omedelbart hävas.

På motsvarande sätt som gäller beslut om tillstånd till ljudupptagning av samtal m.m. enligt avsnitt 10.9 bör inte ett beslut om tillstånd till identifiering av mobilelektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation få bestämmas till längre tid än nödvändigt. Detsamma bör även gälla för störning av sådan utrustning.

När det gäller sådan identifiering som används i samband spaning kan det på samma sätt som när det gäller ljudupptagning av samtal m.m. inte krävas att det alltid ska anges exakt när åtgärderna ska vidtas. Istället bör det då vara tillräckligt att tillståndet begränsas till att gälla en viss tidsperiod som också för identifierings- och störningsåtgärder bör kunna bestämmas till som längst tre månader. Det finns inget som hindrar att tiden för tillståndet sätts till en kortare tid än tre månader.

Många gånger torde dock tillståndsbesluten, särskilt när det gäller störning, kunna begränsas till en avsevärt kortare tidsperiod och snarare avse timmar än månader.

Den tidsmässiga begränsningen av tillståndets längd hindrar dock inte att tillstånd ges på nytt för en ny tidsperiod. Detta skulle t.ex. kunna komma i fråga i de fall besluten avser identifiering av mobiltelefoner i samband med en hemlig teleavlyssning som pågår.

En prövning ska alltid göras av i vilken utsträckning ett tillstånd ska förenas med sådana villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Vilka villkor det kan vara fråga om får avgöras från fall till fall i rättstillämpningen.

12 Rättssäkerhetsgarantier och vissa övriga frågor

12.1 En ny beslutsinstans för underrättelseverksamhet

12.1.1 Behovet av en ny beslutsinstans

Förslag: Beslut i underrättelseverksamhet om tillstånd till särskilt ingripande åtgärder som avser ljud- eller bildupptagning, lokalisering av person, identifiering av mobil elektronisk kommunikation m.m. eller störning av sådan kommunikation samt tillstånd till annars brottsliga gärningar eller särskilda provokativa åtgärder ska fattas av ett särskilt beslutsorgan – Nämnden.

Nämnden ska arbeta fristående från de brottsbekämpande myndigheterna och utgöra en oberoende beslutsinstans.

Utredningen föreslår att beslut om tillstånd till åtgärder enligt den nya lagen om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet i normalfallet ska få fattas inom de brottsbekämpande myndigheterna. När det gäller beslut om åtgärder som bedöms vara särskilt ingripande föreslår utredningen att det i förundersökning är rätten som ska pröva tillståndsfrågan. När det gäller underrättelseverksamheten finns det inte någon motsvarande oberoende beslutsinstans. Att låta dessa beslut fattas inom de brottsbekämpande myndigheterna framstår inte som tillräckligt ur ett rättssäkerhetsperspektiv. Hur beslutsordningen ska utformas i underrättelseverksamheten kräver därför särskilda överväganden.

I underrättelseverksamheten är syftet att genom en bred informations- och kunskapsinsamling ge underlag för bearbetning och analys (kartläggning). Utgångspunkten är, ofta utifrån en mer övergripande ansats, att studera och kartlägga en befarad brottslig verk-

samhet för att förebygga eller förhindra att brottsligheten genomförs.

Mer kvalificerade inhämtningsåtgärder av sådan typ som föreslås i inhämtningslagen utgör många gånger intrång i den enskildes integritet. Å andra sidan medför målsättningen för inhämtning i underrättelseverksamhet, i ljuset av det framåtblickande perspektivet, att partsintresset inte framstår som lika framträdande som under en förundersökning.

I utredningens delbetänkande behandlas frågan om lämplig beslutsinstans för beslut i underrättelseverksamhet om att hämta in uppgifter om elektronisk kommunikation (se SOU 2009:1 s. 128 ff.). Utredningen konstaterar där att det finns tungt vägande skäl som talar mot att allmän domstol ges en roll i underrättelseverksamheten och att dessa skäl gör sig gällande med minst samma styrka vad gäller åklagare.

Samma skäl som utredningen anförde i delbetänkandet mot att låta åklagare eller domstol pröva tillståndsfrågor i underrättelseverksamheten gör sig gällande även när det gäller frågor enligt inhämtningslagen. Det finns sålunda all anledning att vara tveksam till att ge åklagare en central roll i att pröva olika åtgärder i underrättelseverksamheten, eftersom det kan ge anledning att ifrågasätta deras ställning och beslut, om det senare blir fråga om en förundersökning och åtal där han eller hon eller någon annan åklagare intar partsställning. Det finns på samma sätt skäl att framhålla problematiken i att låta domstol generellt rättsligt pröva olika åtgärder som vidtas i underrättelseverksamheten och därmed i många fall ge klartecken till olika operativa spaningsåtgärder. Detta kan leda till att domstolens roll som oberoende prövningsinstans i brottsmålsförfarandet ifrågasätts, i varje fall när åtgärderna senare leder fram till förundersökning och åtal. Det är inte heller naturligt för allmän domstol att ha en sådan roll i det svenska rättssystemet.

Ett annat alternativ skulle kunna vara att låta Säkerhets- och integritetsskyddsnämnden fatta besluten. Säkerhets- och integritetsskyddsnämnden är tillsynsmyndighet för bl.a. användningen av hemliga tvångsmedel och föreslås i avsnitt 12.5 få utökade tillsynsuppgifter avseende åtgärder enligt inhämtningslagen. Detta skulle kunna vara acceptabelt om besluts- och tillsynsfunktionerna utövas på sådant sätt att det blir fråga om skilda enheter inom myndigheten som självständigt gentemot varandra svarar för funktionerna. Lösningen framstår dock inte som helt lyckad ur ett rättsäkerhetsperspektiv, eftersom det beslutsorgan som ger tillståndet inte bör

kunna sammankopplas med det organ som i efterhand utövar tillsyn över den verksamhet i vilket beslutet har tillämpats. Vid kontakter med Säkerhets- och integritetsskyddsnämnden har också nämnden ställt sig tveksam till ett sådant förslag.

Den lösning som därmed återstår är inrättandet av ett särskilt organ, t.ex. en nämnd, för prövningen. Med ett sådant beslutsorgan skulle besluten kunna fattas helt fristående från både de verkställande brottsbekämpande myndigheterna och tillsynsmyndigheten. En sådan lösning framstår enligt utredningen som principiellt riktig och ändamålsenlig.

Nämnden föreslås som framgått av tidigare avsnitt fatta beslut i underrättelseverksamhet avseende särskilt ingripande fall av ljud- eller bildupptagning, lokalisering av person, identifiering av mobil elektronisk kommunikation m.m. eller störning av sådan kommunikation samt rörande annars brottsliga gärningar och särskilda provokativa åtgärder.

12.1.2 Nämndens organisation och arbetsformer

Förslag: Nämndens ledamöter ska utses av regeringen för en bestämd tid, högst fyra år. Nämndens ordförande och vice ordförande ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Det ska också finnas minst två och högst fyra särskilda ledamöter med specialistkompetens.

Nämnden ska vara beslutför med ordförande och två särskilda ledamöter. Fler än tre ledamöter ska inte få delta i ett avgörande.

Ordföranden ska självständigt få vidta förberedande åtgärder och avskriva mål. Även en tjänsteman med juridisk kompetens som är knuten till Nämnden ska, efter ordförandens förordnande, få vidta förberedande åtgärder.

Med hänsyn till bedömningen ovan i avsnitt 12.1.1 bör det framhållas att syftet med att inrätta Nämnden är att den ska arbeta fristående från de brottsbekämpande myndigheterna och utgöra en oberoende beslutsinstans.

Att utredningen i betänkandet genomgående använder beteckningen Nämnden innebär inte att myndigheten också bör organiseras som en nämndmyndighet enligt myndighetsförordningen (2007:515). Att inrätta myndigheten som en nämndmyndighet

skulle visserligen ha den fördelen att Nämndens kansliresurser med stöd av 18 § myndighetsförordningen skulle kunna tillhandahållas av en värdmyndighet. Den värdmyndighet som i så fall främst skulle komma på fråga torde, trots de invändningar som tidigare anförts, vara Säkerhets- och integritetsskyddsnämnden. Utredningen avstår dock från att föra fram ett särskilt förslag i denna del utan frågan om myndighetens formella styrelseform får i stället avgöras utifrån vad som befinns lämpligast i samband med inrättandet.

Det är i dagsläget svårt att göra tillförlitliga prognoser om vilken omfattning Nämndens verksamhet kommer att få, se även avsnitt 14. Det kan dock antas att verksamheten i vart fall inte inledningsvis kommer att få en särskilt stor omfattning.

För att i viss mån begränsa tillämpningen av interimistiska beslut bör det dock ställas vissa krav på att Nämnden sammanträder med viss regelbundenhet. En sammanträdesfrekvens på i alla fall två gånger i månaden kan framstå som rimlig.

När det gäller Nämndens sammansättning kan en jämförelse göras med allmän domstols sammansättning vid prövning av en ansökan om användning av hemliga tvångsmedel. Tingsrätten är därvid domför med en lagfaren domare enligt huvudregeln i 1 kap. 3 § RB. Vid överklagande av sådant beslut är hovrätten domför med tre lagfarna domare (2 kap. 4 § RB).

Vid ställningstagande i frågan om beslutförhet bör beaktas att ärendena vid Nämnden är av sådan karaktär att den information som delges i samband med prövningen måste hållas inom en begränsad krets samtidigt som det också krävs att Nämnden tillförs expertkunskaper och att medborgarintresset tillvaratas. Mot den bakgrunden är det lämpligt att Nämnden är domför med en ordförande och två särskilda ledamöter. På motsvarande sätt som när det gäller t.ex. Försvarsunderrättelsedomstolen bör fler än tre ledamöter inte få delta vid avgörandet av ett ärende (se prop. 2008/09:201 s. 72).

En naturlig utgångspunkt är att ordföranden liksom vice ordföranden är lagfarna. Eftersom de också ska kunna leda Nämndens sammanträden bör därutöver ställas krav på att de har tidigare erfarenhet av tjänstgöring som ordinarie domare.

De särskilda ledamöterna bör utses på grundval av kriteriet att de ska besitta särskild kunskap om förhållanden av betydelse för Nämndens verksamhet. Bland dessa ledamöter bör finnas såväl erfarenhet och kunskap om underrättelseverksamhet och förutsättningarna för sådan verksamhet som särskild förmåga att belysa integritetsskyddsintresset och tillvarata medborgarnas perspektiv.

Ordföranden bör själv kunna fatta beslut i samband med förberedande åtgärder och besluta om avskrivning. Efter ordförandens förordnande bör beslut i samband med förberedande åtgärder även kunna fattas av tjänstemän som är knutna till Nämnden, t.ex. en sekreterare med juridisk kompetens.

12.2 Överprövning m.m.

Förslag: Beslut av rätten om åtgärder enligt inhämtningslagen ska kunna överklagas på samma sätt som rättens beslut om åtgärder enligt 25–28 kap. RB. Har särskilda inhämtningsåtgärder beslutats av undersökningsledaren eller åklagaren ska den som är föremål för åtgärden kunna begära rättens prövning av beslutet.

Beslut av brottsbekämpande myndigheter om särskilda inhämtningsåtgärder i underrättelseverksamhet ska kunna bli föremål för prövning i Nämnden, om den som berörts av åtgärden begär det. Nämndens beslut ska inte kunna överklagas.

En tingsrätts slutliga beslut får överklagas (49 kap. 3 § RB). Bestämmelsen i 49 kap. 5 § 6 RB innebär att om en tingsrätt har prövat frågor om åtgärder enligt 25–28 kap. RB får beslutet överklagas särskilt, dvs. utan samband med överklagande av dom eller slutligt beslut (se även 54 kap. 4 § RB). Enligt den nu föreslagna lagen ska rätten fatta beslut om vissa särskilt ingripande inhämtningsåtgärder. Även om sådana inhämtningsåtgärder inte kan anses utgöra hemliga tvångsmedel kan de i många fall utgöra påtagliga intrång i den personliga integriteten. Mot denna bakgrund bör det införas en bestämmelse med innebörd att vad som enligt rättegångsbalken gäller för överklagande av domstols beslut om åtgärder enligt 25–28 kap. RB också ska gälla för domstols beslut om särskilda inhämtningsåtgärder.

När det gäller beslut om särskilda inhämtningsåtgärder inom ramen för en förundersökning och som får fattas inom de brottsbekämpande myndigheterna blir frågan om det finns tillräckliga skäl att införa en överprövningsmöjlighet även rörande sådana beslut.

En polismans beslut om tvångsmedel under en förundersökning kan inte överprövas av domstol. Det innebär att det inte finns någon möjlighet att överklaga en polismans beslut om bl.a. medtagande till förhör, hämtning till förhör, husrannsakan, kroppsvisitation

och kroppsbesiktning. En åklagares beslut om de nämnda tvångsmedlen kan inte heller överklagas och den som drabbas kan inte få rättens prövning av åtgärden (jfr dock beslag, reseförbud och anmälningsskyldighet).

Mot att införa en rätt att överpröva polismans, undersökningsledarens och åklagarens beslut om särskilda inhämtningsåtgärder talar att en sådan möjlighet närmast torde bli av teoretiskt intresse med hänsyn till att den som är föremål för åtgärden normalt saknar kännedom om att åtgärden verkställs. Trots det kan det i undantagssituationer förekomma att personen blir medveten om detta. Det är därför enligt utredningens mening inte lämpligt att helt frånta en person möjligheterna att få en överprövning av beslutet. Utredningen gör bedömningen att en lämplig ordning är att införa ett system motsvarande vad som gäller för beslag, reseförbud och anmälningsskyldighet. För beslag gäller att den som drabbas av ett beslag som verkställts utan rättens förordnande får, enligt 27 kap. 6 § RB, begära rättens prövning av beslaget. Motsvarande gäller enligt 25 kap. 5 § RB för beslut om reseförbud och anmälningsskyldighet.

De omständigheter som nu anförts gör sig gällande på motsvarande sätt när det gäller de särskilda inhämtningsåtgärder som vidtas av de brottsbekämpande myndigheterna inom underrättelseverksamheten. Det bör därför också tillskapas en möjlighet att begära prövning av beslutet hos Nämnden, om den som berörs av beslutet skulle bli medveten om detta och särskilt begär det. Nämndens beslut bör däremot inte kunna överklagas.

12.3 Offentliga ombud

Bedömning: Det bör inte införas ett krav på att offentligt ombud ska delta vid rättens eller Nämndens prövning av åtgärder enligt inhämtningslagen.

När det gäller hemliga tvångsmedel eller liknande hemliga åtgärder får den som utsatts för åtgärden av naturliga skäl normalt inte reda på beslutet i sådan tid att det blir praktiskt möjligt eller meningsfullt att överklaga beslutet. Mot den bakgrunden finns systemet med offentliga ombud som ska bevaka enskildas integritetsintressen i ärenden om hemlig teleavlyssning, hemlig kameraövervakning och

hemlig rumsavlyssning. Bestämmelserna omfattar inte ärenden enligt rättegångsbalken om hemlig teleövervakning. När bestämmelserna om offentliga ombud infördes ansågs behovet av sådana ombud vara mindre vid hemlig teleövervakning än vid hemlig teleavlyssning och reglerna kom inte att omfatta sådan övervakning (se prop. 2002/03:74 s. 22 f.). Däremot ska offentliga ombud medverka vid prövningen av om hemlig teleövervakning, liksom övriga tvångsmedel, ska tillåtas enligt 6 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

De flesta åtgärder som utredningen föreslår ska regleras i inhämtningslagen är sådana som redan nu kan beslutas av de brottsbekämpande myndigheterna utan någon ordinär tillsyn. De aktuella åtgärderna är dessutom enligt utredningens bedömning inte lika ingripande eller integritetskränkande som de hemliga tvångsmedlen. Det finns mot denna bakgrund inte skäl att föreslå en utvidgning av tillämpningsområdet för offentliga ombud att närvara vid rättens eller Nämndens prövning av åtgärder enligt den föreslagna lagen.

12.4 Underrättelse till enskild

Förslag: Den som i förundersökning har varit utsatt för en åtgärd enligt 2 kap. 5 § inhämtningslagen (särskilt ingripande ljud- eller bildupptagning eller lokaliseringsåtgärd) ska i efterhand underrättas om åtgärden.

När det gäller sådan underrättelse, tidpunkt för underrättelsen och undantag från underrättelseskyldigheten ska vad som föreskrivs i 27 kap. 31 § andra och tredje styckena, 32 och 33 §§ RB tillämpas.

Bedömning: Det bör inte införas någon underrättelseskyldighet vid åtgärder enligt inhämtningslagen som vidtas i de brottsbekämpande myndigheternas underrättelseverksamhet. Inte heller bör det, avseende åtgärder enligt inhämtningslagen som vidtas i en förundersökning, införas någon underrättelseskyldighet vid särskilda provokativa åtgärder, tillträde till vissa utrymmen i samband med infiltration, identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation eller störning av kommunikation med sådan utrustning.

12.4.1 Allmänt om underrättelseskyldighet

Sedan den 1 januari 2008 gäller en underrättelseskyldighet för de brottsbekämpande myndigheterna i förhållande till enskild som varit utsatt för hemliga tvångsmedel. Underrättelse ska lämnas så snart det kan ske utan men för utredningen, dock senast en månad efter det att förundersökningen avslutades. Underrättelsen ska innehålla uppgifter om vilket tvångsmedel som har använts och när det har skett. Dessutom ska personen underrättas om vilken brottsmisstanke som legat till grund för åtgärden. Alternativt ska det finnas uppgift om att personen inte är eller har varit misstänkt för brott. Om det gäller sekretess för en uppgift i en underrättelse ska den skjutas upp till dess att sekretessen inte längre gör sig gällande. Om sekretess hindrat underrättelse under ett års tid, får underrättelsen underlåtas. Underrättelse behöver inte heller lämnas om förundersökningen angår vissa brott inom Säkerhetspolisens ansvarsområde, dvs. allmänfarliga brott, brott mot rikets säkerhet och terroristbrott (27 kap. 32 och 33 §§ RB). Bestämmelser om underrättelse till enskild finns även i 15 § lagen om hemlig rumsavlyssning och i 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

12.4.2 Underrättelseskyldighet vid förundersökning

Bör det införas en underrättelseskyldighet vid förundersökning?

Syftet med att lämna underrättelse om att hemliga tvångsmedel har använts är att den enskilde ska få möjlighet att bedöma vilket integritetsintrång som åtgärden har inneburit och att reagera mot vad han eller hon kan anse ha varit en rättsstridig åtgärd.

I många av de åtgärder som föreslås regleras i den nya lagen är integritetsintrånget inte så stort att det enligt utredningens bedömning motiverar införandet av en underrättelseskyldighet. Men när det gäller sådana åtgärder som bedöms utgöra särskilt ingripande ljud- eller bildupptagningar eller lokalisering av person enligt den föreslagna inhämtningslagen torde integritetsintrånget normalt vara så betydande att det av den anledningen bör införas en underrättelseskyldighet.

Närmare om underrättelseskyldigheten vid förundersökning

Underrättelseskyldighet vid användning av hemliga tvångsmedel gäller endast i förhållande till den som är eller har varit misstänkt för brott eller, i de fall avlyssningen eller övervakningen avsett en teleadress som innehas av någon annan än den misstänkte, även innehavaren (27 kap. 31 § RB). Det är alltså en i förhållande till det totala antalet personer vilkas kommunikation kan komma att bli föremål för åtgärden begränsad krets som kan komma att underrättas. Den som ringer till en avlyssnad teleadress eller utan att vara innehavare använder en sådan teleadress blir inte underrättad. Med hänsyn till svårigheten att identifiera sådana personer är detta en naturlig avgränsning (se prop. 2006/07:133 s. 37). Regeringen uttalade även att en underrättelseskyldighet beträffande sådana ovidkommande personer skulle skapa betydande praktiska problem och dessutom typiskt sett medföra att integritetskränkningen för den enskilde skulle kunna öka (se prop. 2006/07:133 s. 39 f.).

När det gäller underrättelseskyldighet enligt inhämtningslagen anser utredningen inte att det finns anledning att göra någon annan principiell bedömning av underrättelseskyldighetens omfattning än den som gjorts i samband med att underrättelseskyldighet vid användning av hemliga tvångsmedel infördes. På motsvarande sätt som vid sådan underrättelseskyldighet måste en underrättelseskyldighet vid åtgärder enligt inhämtningslagen följaktligen begränsas till de personer som varit föremål för något aktivt ställningstagande inom ramen för inhämtningen. En lämplig ordning är därför att den som varit utsatt för en särskilt ingripande ljud- eller bildupptagning eller lokaliseringsåtgärd, ska underrättas om åtgärden.

En ljud- eller bildupptagning kan, om den sker på en plats med mycket folk, komma att beröra ett stort antal personer. Integritetsintrånget för dessa måste dock normalt sett bedömas vara så ringa att det inte motiverar någon underrättelse. Beträffande sådana för brottsutredningen ovidkommande personer skulle en underrättelseskyldighet typiskt sett innebära att integritetsintrånget ökar. Åtskilliga av dessa kommer inte heller att kunna identifieras, i varje fall inte utan att stora utredningsresurser läggs ned på identifieringen.

Vid särskilt ingripande ljud- eller bildupptagning bör den som innehar den plats, där åtgärden har genomförts, underrättas om åtgärden. Om åtgärden har genomförts på en plats till vilken allmän-

heten har tillträde, ska det dock inte behöva lämnas någon underrättelse till innehavaren av platsen.

Undantag från underrättelseskyldigheten

En ovillkorlig underrättelseskyldighet skulle innebära en stor risk för att brottsbekämpande verksamhet skadas. Det är därför nödvändigt att bestämmelser om underrättelseskyldighet förses med undantag. Undantagen bör utformas på motsvarande sätt som avseende hemliga tvångsmedel. Det innebär att underrättelse ska kunna skjutas upp på grund av att sekretess gäller för uppgifterna. Det innebär vidare att underrättelse inte heller behöver lämnas om förundersökningen angår vissa brott inom Säkerhetspolisens ansvarsområde, dvs. allmänfarliga brott, brott mot rikets säkerhet och terroristbrott (27 kap. 32 och 33 §§ RB).

Med hänsyn till att sekretess kan bestå under lång tid är det rimligt att, liksom är fallet beträffande underrättelseskyldighet avseende användning av hemliga tvångsmedel, föreskriva en tidsfrist efter vilken underrättelse inte behöver lämnas om sekretessen fortfarande består. Vad gäller tidsfristens längd bör den motsvara vad som gäller för hemliga tvångsmedel, dvs. ett år. Har ingen underrättelse kunnat lämnas under den tiden ska underrättelse få underlåtas.

En underrättelse behöver inte heller lämnas till den som redan enligt 23 kap. 18 § RB eller på annat sätt fått del av eller tillgång till uppgifterna. En underrättelse ska heller inte behöva lämnas, om den med hänsyn till omständigheterna uppenbart är utan betydelse.

Vem ska fullgöra underrättelseskyldigheten?

Enligt 14 b § förundersökningskungörelsen ska underrättelseskyldigheten enligt 27 kap. 31 § RB fullgöras av den åklagare som är eller har varit förundersökningsledare. När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket RB, dvs. när det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, ska den åklagare som har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.

Utredningens förslag till inhämtningslag innebär att enskild polisman, förundersökningsledare vid polisen och tullen, liksom åklagare, i fortsättningen kommer att kunna besluta om vissa åtgärder enligt den föreslagna lagen. I andra fall kommer besluten att fattas av rätten. I de fall underrättelseskyldighet införs är det fråga om beslut som har fattats av rätten. Det finns därför skäl att ansluta till utformningen av underrätteskyldighet vid användning av hemliga tvångsmedel.

Enligt 27 kap. 31 § andra stycket RB ska en underrättelse lämnas så snart det kan ske utan men för utredningen. Den bedömningen behöver alltså göras kontinuerligt. Det faller sig naturligt att den åklagare som är eller har varit förundersökningsledare också ska ha ansvaret för att en underrättelse lämnas när förutsättningarna för detta är uppfyllda. En underrättelse ska alltid lämnas senast en månad efter det att förundersökningen avslutades, om inte underrättelsen av sekretesskäl ska skjutas upp eller helt underlåtas.

12.4.3 Underrättelseskyldighet i underrättelseverksamhet

Bör det införas en underrättelseskyldighet i underrättelseverksamheten?

När det gäller frågan om det bör införas en underrättelseskyldighet för åtgärder vidtagna i underrättelseverksamheten bör följande beaktas.

Som tidigare framhållits är underrättelseverksamheten inte inriktad mot en viss person och partsintressena är inte så framträdande i ett sådant tidigt utredningsskede. I stället är det först senare när en förundersökning eventuellt har inletts rörande ett konkret brott och där information kan användas mer riktat mot den enskilde som partsintressena blir påtagliga. Utredningen menar att integritetsintrånget inte är av det slaget att det behöver tillskapas en ordning med underrättelse i efterhand till den enskilde om inhämtning. Mot bakgrund av underrättelseverksamhetens framåtblickande perspektiv och övergripande natur, där information hämtas in, bearbetas och analyseras för att förhindra och förebygga brottslig verksamhet, är en sådan underrättelseskyldighet också problematisk, eftersom den riskerar att motverka själva huvudsyftet med underrättelseverksamheten. Av samma skäl skulle det också vara nödvändigt att omgärda en underrättelseskyldighet med så många

undantag att den närmast skulle framstå som illusorisk (jfr övervägandena i utredningens delbetänkande SOU 2009:1 s. 150). Någon underrättelseskyldighet bör således inte införas i underrättelseverksamheten.

12.5 Tillsyn

Förslag: Säkerhets- och integritetsskyddsnämnden ska utöva löpande tillsyn över användningen av inhämtningsåtgärder enligt inhämtningslagen, dvs.

1. ljud-, bild- eller lokaliseringsåtgärder (2 kap.),
2. identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, eller störning av kommunikation med sådan utrustning (3 kap.),
3. tillträde till vissa utrymmen (4 kap.),
4. särskilda provokativa åtgärder (5 kap.),
5. annars brottsliga gärningar (6 kap.),
6. biträde av enskilda (7 kap.), samt
7. särskilda åtgärder i Säkerhetspolisens verksamhet (9 kap).

Säkerhets- och integritetsskyddsnämnden ska även vara skyldig att på begäran av en enskild person kontrollera om han eller hon har utsatts för sådana åtgärder i de brottsbekämpande myndigheternas verksamhet och om åtgärden och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning.

Säkerhets- och integritetsskyddsnämndens verksamhet regleras i lagen om tillsyn över viss brottsbekämpande verksamhet. Nämnden ska bestå av högst tio ledamöter som utses av regeringen för en tid av högst fyra år. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.

Säkerhets- och integritetsskyddsnämnden ska bl.a. utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed sammanhängande verksamhet samt Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (som den 1 mars 2012 ersätts av en ny polisdatalag, se avsnitt 3.1.6). Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i

enlighet med lag eller annan författning. Fr.o.m. den 1 mars 2012 kommer tillsynen även att omfatta polisens behandling av personuppgifter enligt lagen om polisens allmänna spaningsregister.

Tillsynen omfattar således användning av hemliga tvångsmedel, såsom hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Att tillsynen även avser med tvångsmedelsanvändningen ”sammanhängande verksamhet” innebär att både själva avlyssningen eller övervakningen och den vidare hanteringen av upptagningarna, såsom hur överskottsinformation används eller förstörs, liksom fullgörandet av reglerna om underrättelseskyldighet, omfattas av tillsynen. Även den brottsbekämpande verksamhet som föregår och ligger till grund för ansökan om tvångsmedlet omfattas. Tillsynen är avgränsad till ”brottsbekämpande myndigheters” användning av metoderna. Det innebär att domstolarnas handläggning av och beslut i ärenden om tillstånd till användning av hemliga tvångsmedel inte omfattas av nämndens tillsyn.

Säkerhets- och integritetsskyddsnämnden utför sin tillsyn genom inspektioner och andra undersökningar. I uppdraget ingår att uttala sig om konstaterade förhållanden och om behovet av förändringar i verksamheten. Säkerhets- och integritetsskyddsnämnden ska vidare verka för att brister i lag eller annan författning avhjälps.

Säkerhets- och integritetsskyddsnämnden är skyldig att på begäran av enskild kontrollera om han eller hon har utsatts för tvångsmedelsanvändning och därmed sammanhängande verksamhet eller har varit föremål för sådan personuppgiftsbehandling som omfattas av nämndens tillsyn. Den enskilde ska underrättas om att kontrollen har utförts.

Säkerhets- och integritetsskyddsnämnden har rätt att utan hinder av gällande sekretess av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Även domstolar samt de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna de uppgifter som Säkerhets- och integritetsskyddsnämnden begär.

Av 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden följer att nämnden, om den uppmärksammar förhållanden som kan utgöra brott, ska anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Om Säkerhets- och integritetsskyddsnämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten ska nämnden anmäla det till Justitiekanslern. Det finns även en anmälningsskyldighet till Datainspektionen.

Säkerhets- och integritetsskyddsnämndens tillsyn fyller en viktig funktion för att upprätthålla en hög rättssäkerhet kring bl.a. användningen av hemliga tvångsmedel. Även om de åtgärder som utredningen förslår ska regleras i inhämtningslagen inte kan anses lika ingripande som hemliga tvångsmedel står det klart att en effektiv tillsyn över användningen av inhämtningsåtgärderna är viktig.

Det framstår enligt utredningens bedömning som angeläget att tillsynen över de brottsbekämpande myndigheternas inhämtningsåtgärder enligt lagen blir effektiv och oberoende.

Det kan visserligen diskuteras om behovet av tillsyn är lika stort i förundersökningssituationer som i underrättelseverksamheten, med tanke på den rättsliga kontroll som ligger i en öppen rättegång med partsinsyn m.m. Många av de åtgärder som regleras i inhämtningslagen är dock snarare spaningsåtgärder än bevisinhämtningsåtgärder. Det innebär också att det kan antas att de inte på samma sätt som hemliga tvångsmedel kommer att redovisas i förundersökningsprotokoll eller komma under rättens prövning. Det finns därför skäl att låta Säkerhets- och integritetsskyddsnämnden utöva tillsyn över de brottsbekämpande myndigheternas användning av åtgärder enligt inhämtningslagen både i underrättelseverksamhet och i förundersökning. Tillsynen ska dock inte avse beslut att lägga ned eller inte inleda förundersökning enligt lagens 8 kap.

Säkerhets- och integritetsskyddsnämnden ska även vara skyldig att på begäran av enskild kontrollera om han eller hon har utsatts för sådana åtgärder i de brottsbekämpande myndigheternas underrättelseverksamhet och om åtgärden och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning.

12.6 Regeringens redovisning till riksdagen

Bedömning: Det bör inte införas någon skyldighet att till riksdagen redovisa användningen av särskilda inhämtningsåtgärder motsvarande vad som gäller för användningen av hemliga tvångsmedel.

När det gäller frågan om någon av de särskilda inhämtningsåtgärder som utredningen föreslår ska omfattas av lagregleringen, bör ingå i regeringens redovisning till riksdagen av hemliga tvångsmedel gör utredningen bedömningen att det inte föreligger lika starka skäl för

en sådan redovisning som det gör för de hemliga tvångsmedlen. Detta beror på att det huvudsakligen handlar om åtgärder som redan nu används av de brottsbekämpande myndigheterna och som får anses utgöra mindre ingrepp i den enskildes integritet än hemliga tvångsmedel. Det beror också på att det avseende flera av åtgärderna handlar mer om spaningsåtgärder än åtgärder för att säkra bevisning för en kommande rättegång. Till detta kommer den kraftiga utvidgning av Säkerhets- och integritetsskyddsnämndens tillsyn som föreslås i avsnitt 12.5 Utredningen finner därför inte att nyttan av att redovisa användningen av särskilda inhämtningsåtgärder till riksdagen i en årlig skrivelse är så stor att en sådan ordning bör införas. I sammanhanget bör dock framhållas att den tillsyn över åtgärder enligt inhämtningslagen som Säkerhets- och integritetsskyddsnämnden ska bedriva bör redovisas på motsvarande sätt som nämndens övriga tillsynsåtgärder.

12.7 Frågor om sekretess och tystnadsplikt

12.7.1 Sekretess

Bedömning: De nuvarande sekretessreglerna till skydd för såväl intresset av att förebygga eller beivra brott som enskildas personliga och ekonomiska förhållanden ger ett tillräckligt och adekvat skydd för sådana inhämtningsåtgärder enligt den föreslagna lagen som kan behöva hemlighållas, och någon ändring behöver således inte göras.

I offentlighets- och sekretesslagen finns bestämmelser som syftar till att begränsa spridningen av information som innehas av de brottsbekämpande myndigheterna. Hos myndigheterna gäller sekretess bl.a. med hänsyn till intresset av att förebygga eller beivra brott och till skydd för enskilds personliga och ekonomiska förhållanden.

Enligt 18 kap. 1 § första stycket OSL gäller sekretess för bl.a. uppgift som hänför sig till förundersökning i brottmål eller angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott. Sekretessen gäller om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Bestämmelsen gäller uppgifter som hänför sig till viss verksamhet.

Det innebär att sekretessen för uppgifterna upprätthålls oavsett hos vilken myndighet de finns.

Av 18 kap. 2 § första stycket OSL framgår att sekretess även gäller för uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen, dvs. polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. RB. Av bestämmelsen framgår vidare att sekretess gäller för uppgift som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism. Sekretess gäller om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Sekretess gäller under samma förutsättningar uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Enligt 35 kap. 1 § första stycket OSL gäller som huvudregel sekretess för uppgift om enskilds personliga och ekonomiska förhållanden bl.a. i utredning enligt bestämmelserna om förundersökning i brottmål, i angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott samt i bl.a. åklagares, polisens och Tullverkets verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott. Sekretessen gäller om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

Sekretessen enligt 35 kap. 1 § OSL hindrar inte att uppgifter lämnas till enskild i vissa särskilt angivna fall, t.ex. enligt vad som föreskrivs i säkerhetsskyddslagen, lagen (1998:621) om misstankeregister och polisdatalagen. I 35 kap. 6 och 7 §§ OSL finns bestämmelser om att sekretessen enligt 35 kap. 1 § första stycket den lagen i vissa fall inte gäller. Så är fallet för flertalet uppgifter som lämnas till domstol med anledning av åtal.

Uppgifter som hänför sig till förundersökning och underrättelseverksamhet respektive enskilds personliga och ekonomiska förhållanden är föremål för sekretess genom ovan nämnda bestämmelser i offentlighets- och sekretesslagen. Sekretesskyddet enligt dessa bestämmelser ger enligt utredningen ett tillräckligt och adekvat skydd för de uppgifter som kan behöva hemlighållas och det behövs där-

för inte några kompletterande sekretessbestämmelser för de särskilda inhämtningsåtgärder som får vidtas enligt den av utredningen föreslagna regleringen.

12.7.2 Rätten att meddela och offentliggöra uppgifter

Förslag: För uppgifter som rör särskilda inhämtningsåtgärder ska – i likhet med vad som gäller för uppgifter från hemliga tvångsmedel – tystnadsplikten ha företräde framför meddelarfriheten.

En annan fråga som måste övervägas är om tystnadsplikten bör ha företräde framför meddelarfriheten för uppgifter som hänför sig till användning av särskilda inhämtningsåtgärder.

Det råder meddelarfrihet för de allra flesta uppgifter som omfattas av sekretess till skydd för den brottsbekämpande verksamheten, även uppgifter om användning av tvångsmedel. Ett undantag från meddelarfriheten rör användningen av hemliga tvångsmedel. Enligt 18 kap. 19 § OSL gäller att uppgifter som omfattas av sekretess enligt 18 kap. 1–3 §§ OSL och som avser användning av bl.a. hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och hemlig rumsavlyssning är undantagna från meddelarfriheten.

Inhämtningsåtgärder enligt den föreslagna regleringen kan i vissa avseenden jämställas med användningen av hemliga tvångsmedel. Ett sådant är den skada som ett utnyttjande av meddelarfriheten skulle innebära för utredningen eller undersökningen. Liksom när det gäller de hemliga tvångsmedlen skulle syftet med inhämtningsåtgärderna kunna omintetgöras om uppgifterna kommer ut. Det finns således ett påtagligt brottsbekämpningsintresse av att uppgifterna skyddas. I vissa fall skulle det kunna innebära fara för liv och hälsa om uppgifter om t.ex. särskilda provokativa åtgärder eller tillträde till vissa utrymmen i samband med infiltration avslöjades. Mot detta skyddsintresse står den tungt vägande meddelarfriheten. Det kan visserligen argumenteras för att åtgärderna borde differentieras så att endast de allvarligaste åtgärderna undantogs rätten att meddela och offentliggöra uppgifter. Vid den avvägning som bör göras menar utredningen dock att brottsbekämpningens intresse av att skydda metoderna i sig, de som arbetar med metoderna och de

som utsätts för metoderna klart väger över. Det bör därför införas ett generellt undantag från rätten att meddela och offentliggöra uppgifter för åtgärder enligt inhämtningslagen.

12.8 Bestämmelsernas tillämplighet för de brottsbekämpande myndigheterna

Förslag: Befogenheter enligt den föreslagna inhämtningslagen ska tillkomma Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten och Åklagarmyndigheten i dessa myndigheters brottsbekämpande verksamhet.

Tullverket ska ha befogenhet att, i myndighetens brottsbekämpande verksamhet, utföra ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person, identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m., installation av lokaliseringsutrustning, särskilda provokativa åtgärder samt ta biträde av enskilda.

Kustbevakningen ska ha befogenhet att, i myndighetens brottsbekämpande verksamhet, utföra bildupptagning av hem eller korrespondens, lokalisering av person, installation av lokaliseringsutrustning samt ta biträde av enskilda.

Skatteverket ska ha befogenhet att, i myndighetens brottsbekämpande verksamhet, utföra bildupptagning av hem eller korrespondens.

Vid tillämpning av inhämtningslagen ska, vid utövande av respektive myndighets befogenheter enligt ovan, vad som är föreskrivet om polismyndighet gälla även för den myndigheten. Vidare ska på motsvarande sätt vad som är föreskrivet om polisman även gälla tjänsteman vid Tullverket, Kustbevakningen respektive Skatteverket.

Åtgärder som avses i inhämtningslagen bör enligt utredningens bedömning generellt kunna vidtas av polisen och Åklagarmyndigheten i respektive myndighets brottsbekämpande verksamhet. Polisen bedriver brottsbekämpande verksamhet vid Rikspolisstyrelsen (inklusive Säkerhetspolisen) och polismyndigheterna samt vid Ekobrottsmyndigheten. Det föreligger dock behov av att kunna vidta vissa av

åtgärderna även vid andra myndigheter med brottsbekämpande verksamhet.

Utredningen gör bedömningen att Tullverket med hänsyn till den allvarliga och ofta organiserade brottslighet som verkets uppdrag omfattar bör kunna utföra ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person, identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m., installation av lokaliseringsutrustning, särskilda provokativa åtgärder samt ta biträde av enskilda. Åtgärderna bör enbart få vidtas i Tullverkets brottsbekämpande verksamhet.

På motsvarande sätt bör, enligt utredningens bedömning, Kustbevakningen med hänsyn till den brottslighet som myndigheten har uppdrag att utreda och beivra ges befogenhet att, i myndighetens brottsbekämpande verksamhet, utföra bildupptagning av hem eller korrespondens, varvid det bör noteras att fartyg kan i vissa fall bedömas som hem samt lokalisering av person, installation av lokaliseringsutrustning och få möjlighet att ta biträde av enskilda.

Slutligen bör Skatteverket ges befogenhet att, i myndighetens brottsbekämpande verksamhet, utföra bildupptagning av hem eller korrespondens.

Vid tillämpning av inhämtningslagen ska, vid utövande av respektive myndighets befogenheter enligt ovan, vad som är föreskrivet om polismyndighet gälla även för den myndigheten. Vidare ska på motsvarande sätt vad som är föreskrivet om polisman även gälla tjänsteman vid Tullverket, Kustbevakningen respektive Skatteverket.

13 Ikraftträdande och övergångsbestämmelser

Förslag: Den nya regleringen ska träda i kraft den 1 juli 2012.

För åtgärder enligt inhämtningslagen som har beslutats innan lagen träder i kraft och där verkställighet av åtgärden har påbörjats före ikraftträdandet, ska verkställighet av åtgärden få fortgå utan tillämpning av den lagen, dock längst till och med den 30 september 2012 (tre månader).

Bedömning: Övriga förslag behöver inga särskilda övergångsbestämmelser.

Utredningens förslag till inhämtningslag innebär en lagreglering av ett antal åtgärder som de brottsbekämpande myndigheterna sedan lång tid vidtar med stöd av allmänna lagregler eller principer. Den föreslagna lagen innebär att förutsättningarna för att använda metoderna klargörs och därmed uppnås en ökad tydlighet och förutsebarhet. Det finns enligt utredningen övertygande skäl som talar för att en tydlig och mer förutsebar reglering av befintliga inhämtningsmetoder i sig innebär en effektivare användning av metoderna, eftersom många oklarheter som tidigare funnits undanröjs. Den föreslagna lagen innehåller också betydande förbättringar av rättssäkerheten kring användandet av åtgärderna.

Det är mot denna bakgrund värdefullt att se till att inhämtningslagen träder i kraft så snart som möjligt.

Det bör särskilt framhållas att de metoder som redan nu används av de brottsbekämpande myndigheterna med stöd av allmänna lagregler eller principer och som föreslås omfattas av den nya lagen kommer att kunna användas enligt vad som gällt tidigare i avvaktan på att den nya lagen ska träda i kraft.

För sådana åtgärder, dvs. inhämtningsåtgärder som beslutats och påbörjats före lagens ikraftträdande och fortfarande pågår när regleringen träder i kraft, behövs enligt utredningen en övergångsreglering för att inte riskera effektivitetsförluster i den brottsbekämpande verksamheten.

Åtgärder som beslutats och påbörjats före ikraftträdandet bör därför få fortsätta att verkställas utan tillstånd enligt den nya lagen. Sådan verkställighet bör dock längst få ske under en tid om tre månader. Den tiden överensstämmer med den maximala tillståndslängden för flertalet åtgärder enligt den nya lagen.

När det gäller övriga förslag bedömer utredningen att det inte finns skäl för några särskilda övergångsbestämmelser.

14 Kostnads- och konsekvensanalys

14.1 Inledning

Kommittéer och särskilda utredare ska enligt kommittéförordningen (1998:1474) göra en konsekvensanalys i där angivna hänseenden beträffande de förslag som lämnas. I det följande redovisas därför konsekvenserna av utredningens förslag.

14.2 Ekonomiska konsekvenser för staten

Bedömning: Förslagen innebär kostnader för inrättande av Nämnden, ökade kostnader för Säkerhets- och integritetsskyddsnämnden samt i begränsad utsträckning ökade kostnader även för Åklagarmyndigheten och Sveriges Domstolar. Kostnadsökningarna bör finansieras inom de befintliga ramarna för rättsväsendet.

Med den nuvarande användningen av metoderna som utgångspunkt, har den öppna polisen bedömt att utredningens förslag till reglering av tekniska spaningsmetoder (ljud, bild och lokalisering) kan röra sig om uppskattningsvis 900 ärenden per år, varav merparten av ärendena torde avse lokalisering av person. Av dessa ärenden kommer en klart övervägande del att utföras inom ramen för förundersökningar och endast en mindre andel inom underrättelseverksamhet. När det gäller sådana åtgärder som bedöms vara särskilt ingripande och därför kräver prövning av rätten eller Nämnden kan dessa, när det gäller tekniska spaningsmetoder, uppskattas till 15–20 ärenden per år, varav omkring 5 ärenden i underrättelseverksamheten.

När det gäller övriga tekniska spaningsmetoder, som användning av IMSI-catcher och störsändare, är antalet ärenden svårt att uppskatta. Likaså är det svårt att uppskatta hur många särskilda provokativa åtgärder som kan komma att genomföras.

När det slutligen gäller tillträde till vissa utrymmen i samband med infiltrationsoperationer kan antalet vid en grov uppskattning uppgå till 30, varav 10 i underrättelseverksamhet. Lika många ärenden bedöms det kunna bli fråga om när det gäller annars brottsliga gärningar.

För *Rikspolisstyrelsen*, *polismyndigheterna* och *Säkerhetspolisen* innebär utredningens förslag i stor utsträckning en reglering av åtgärder som redan nu kan vidtas av dessa myndigheter. Ny är dock möjligheten att använda störsändare. Även om utredningens förslag i den delen för med sig ökade kostnader i form av utgifter för anskaffning av teknisk utrustning för störning får kostnaderna antas vara förhållandevis blygsamma. Regleringen av särskilda provokativa åtgärder och vissa frågor som berör infiltrationsoperationer bedöms inte medföra några ökade kostnader för polisen. Sammantaget innebär detta att eventuella kostnadsökningar för polisen inte kan förväntas bli så stora att de kräver några resurstillskott.

För *Åklagarmyndigheten* innebär förslagen dels att åklagare kopplas in och fattar fler beslut än vad som nu gäller, dels att åklagare i vissa ärenden ska begära tillstånd till åtgärden vid domstol. Till detta kommer att åklagaren kommer att ansvara för den förslagna underrättelseskyldigheten när det gäller särskilt ingripande ljud- och bildupptagning samt lokalisering av person i förundersökning. Dessa åtgärder kommer dock inte att bli särskilt många och innebär inte något påtagligt merarbete.

Utgångspunkt för de ekonomiska konsekvenserna är den omfattning av åtgärder som beskrivits ovan, samt uppgifter från Åklagarmyndigheten om vissa handläggningskostnader. Utredningen bedömer att åklagare på grund av de nya bestämmelserna i inhämtningslagen kan förväntas fatta ungefär 1 000 beslut per år. En rimlig utgångspunkt kan vara att varje beslut innebär en timmes arbete. Till en timkostnad av 650 kr per timme skulle den sammanlagda kostnaden uppgå till 650 000 kr. Till detta bör läggas kostnaden för de ärenden där åklagaren för talan i domstol. Vid en skälighetsuppskattning kan det röra sig om fem timmar per ärende i 50 ärenden per år och därmed en kostnad om cirka 160 000 kr. Sammantaget skulle de ökade kostnaderna för Åklagarmyndigheten uppgå till ca 810 000 kr. Denna kostnad bedöms rymmas inom Åklagarmyndighetens befintliga anslag.

För *Sveriges Domstolars* del kan det handla om uppskattningsvis omkring 100 nya tillståndsärenden varje år. Med en uppskattad snittkostnad om 1 000 kr per ärende handlar det om en kostnadsökning

på omkring 100 000 kr. Denna kostnad bör rymmas inom Sveriges Domstolars befintliga anslag.

Den förstärkning av *Säkerhets- och integritetsskyddsnämndens* tillsyn som utredningen föreslår kan enligt utredningens bedömning innebära ett behov av en förstärkning med två kvalificerade handläggare. Med beaktande av lönekostnader, kostnader för lokaler, resor m.m. skulle förslagen innebära en årlig kostnadsökning om 3 000 000 kr. Kostnaden ryms inte inom nämndens nuvarande anslag, utan nämndens anslag måste höjas. Ramhöjningen bör dock kunna finansieras genom omfördelningar inom rättsväsendets anslag.

När det gäller *Nämnden* är kostnaden svårbedömd, eftersom den blir beroende av faktorer som vilken styrelseform som väljs, om Nämnden ska ha ett eget kansli eller om den kan inordnas under en värdmyndighet samt i vilken omfattning ordföranden och vice ordföranden förväntas tjänstgöra. Det står dock klart att inrättandet av Nämnden kommer att innebära vissa ökade kostnader jämfört med dagsläget. Med hänsyn till den förväntade mängden ärenden bedöms emellertid dessa kostnader inte bli högre än att de kan finansieras genom omfördelningar inom rättsväsendets anslag.

Även när det gäller *Ekobrottsmyndigheten*, *Kustbevakningen*, *Tullverket* och *Skatteverket* avser lagregleringen främst sådana åtgärder som myndigheterna redan nu får vidta. Eventuella tillkommande kostnader för dessa myndigheter bedöms vara så låga att de ryms inom ramen för respektive myndighets befintliga anslag.

14.3 Konsekvenser för brottsligheten

Bedömning: Utredningens förslag kan förväntas innebära ökad effektivitet i de brottsutredande myndigheternas verksamhet. Genom förslagen kommer det att finnas bättre förutsättningar att effektivt utreda grov brottslighet. Därigenom kan polis och åklagare förväntas beivra fler brott, vilket kan förväntas leda till en på sikt minskad brottslighet.

Även om flertalet åtgärder som omfattas av inhämtningslagen är sådana som redan i dag används av de brottsbekämpande myndigheterna, finns det enligt utredningen övertygande skäl som talar för att en tydlig och mer förutsebar reglering av befintliga inhämtnings-

metoder i sig innebär en effektivare användning av metoderna, eftersom många oklarheter som tidigare funnits undanröjs.

Ett effektivare brottsbekämpande arbete innebär bättre förutsättningar att effektivt utreda grov organiserad brottslighet. Effektivare brottsutredningar bör leda till ett ökat antal dömda personer samt som en konsekvens därav även, på sikt, minskad brottslighet.

14.4 Övriga konsekvenser

Bedömning: Utredningens förslag förväntas inte i övrigt få några konsekvenser av det slag som anges i kommittéförordningen.

Det finns inte någon anledning att anta att utredningens förslag kommer att påverka kostnaderna eller intäkterna för kommuner, företag eller enskilda.

Förslagen kan inte heller förväntas få direkt betydelse för jämställdheten mellan kvinnor och män, barn, det kommunala självstyret, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags eller för möjligheten att nå de integrationspolitiska målen.

15 Författningskommentar

15.1 Förslaget till lag (0000:00) om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet

1 kap. Lagens tillämpningsområde och syfte

1 §

Denna lag innehåller bestämmelser om befogenhet att i brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten och Åklagarmyndigheten använda vissa särskilda åtgärder i syfte att hämta in information för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet (underrättelseverksamhet), eller
2. utreda eller beivra brott (förundersökning).

I lagen finns även bestämmelser om befogenheternas tillämplighet för Tullverket, Kustbevakningen och Skatteverket i dessa myndigheters brottsbekämpande verksamhet.

Paragrafen anger lagens tillämpningsområde. Lagen ger de brottsbekämpande myndigheterna befogenheter att använda vissa särskilda åtgärder för inhämtning av information. Åtgärderna det rör sig om är

- ljudupptagning av samtal (2 kap. 2 §),
- bildupptagning av hem eller korrespondens (2 kap. 3 §),
- lokalisering av person (2 kap. 4 §),
- identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m. (3 kap. 2 och 3 §§),
- tillträde till vissa utrymmen i infiltrationsverksamhet (4 kap. 1 §), och vid installation av lokaliseringsutrustning (4 kap. 7 §),
- särskilda provokativa åtgärder (5 kap. 1 §),
- annars brottsliga gärningar (6 kap. 1 §),

Åtgärderna är inte hemliga tvångsmedel utan befogenheter att använda vissa särskilda åtgärder, jfr kommentaren till 3 § nedan.

Lagen utesluter inte att andra åtgärder i den brottsbekämpande verksamheten fortfarande kan användas med stöd av annan lag, t.ex. polislagen. Den föreslagna lagen påverkar med andra ord inte tillåtligheten av andra åtgärder än de som uttryckligen regleras.

I bestämmelsen anges att syftena med att genomföra åtgärderna ska vara att hämta in information för att antingen förebygga, förhindra eller upptäcka brottslig verksamhet (punkten 1), eller utreda eller beivra brott (punkten 2). Det som åsyftas i punkten 1 är det som vanligtvis kallas underrättelseverksamhet, dvs. arbete med insamling, bearbetning och analys av information i ett skede när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts (se närmare avsnitt 4.2.2). Med uttrycket att utreda eller beivra brott i punkten 2 avses förundersökning eller annan utredning enligt bestämmelserna i 23 kap. RB. I senare paragrafer används begreppen underrättelseverksamhet respektive förundersökning för dessa båda verksamheter. I annan lagstiftning kan de begreppen ha annan innebörd.

2 §

> Syftet med denna lag är att reglera vissa särskilda åtgärder som kan utgöra ingrepp i grundläggande fri- och rättigheter enligt 2 kap. regeringsformen eller Europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

I paragrafen anges det övergripande syftet med lagen. Det är att säkerställa skyddet för den enskildes integritet genom att reglera vissa åtgärder i den brottsbekämpande verksamheten som kan utgöra ingrepp i grundläggande fri- och rättigheter enligt 2 kap. RF eller enligt Europakonventionen. Det är framför allt fråga om dels skyddet för den kroppsliga och personliga integriteten enligt 2 kap. 6 § RF, dels rätten till en rättvis rättegång och skyddet för privat- och familjeliv enligt artiklarna 6 och 8 i Europakonventionen.

3 §

Denna lag innehåller bestämmelser om
1. ljud- eller bildupptagning samt lokalisering av person (2 kap.)
2. identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m. (3 kap.)
3. tillträde till vissa utrymmen (4 kap.)
4. särskilda provokativa åtgärder (5 kap.)
5. annars brottsliga gärningar (6 kap.)
6. biträde av enskilda (7 kap.)
7. nedläggning av förundersökning (8 kap.)

Lagen innehåller även vissa särskilda bestämmelser för Säkerhetspolisen (9 kap.).

Denna lag omfattar inte åtgärder som enligt annan lag utgör hemliga tvångsmedel.

I paragrafens första stycke finns en förteckning som anger vad lagens kapitel innehåller.

Av andra stycket framgår att det i lagens 9 kap. finns vissa särskilda bestämmelser för Säkerhetspolisen.

Av tredje stycket följer att lagen inte ger stöd för åtgärder som enligt annan lag utgör hemliga tvångsmedel. Med hemliga tvångsmedel avses postkontroll, hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning samt hemlig rumsavlyssning. Är omständigheterna vid t.ex. en ljudupptagning sådana som beskrivs i 1 § lagen om hemlig rumsavlyssning, ska bestämmelserna i den lagen tillämpas. På samma sätt gäller att om en bildupptagning genomförs på sätt som anges i rättegångsbalkens bestämmelser om hemlig kameraövervakning (27 kap. 20 a §) ska de bestämmelserna tillämpas.

4 §

Tillstånd till åtgärder enligt denna lag får meddelas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden avser eller för något annat motstående intresse.

I paragrafen finns proportionalitetsprincipen uttryckt (se även t.ex. 8 § polislagen). Principen brukar i korthet beskrivas på det sättet att en åtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med den. Principen måste beaktas vid prövningen av om åtgärden ska tillåtas. Den får också betydelse för hur lång tillståndstiden ska vara och vilka vill-

kor tillståndet eventuellt ska förenas med. Principen måste också beaktas under hela verkställighetsförfarandet och ska alltså, även sedan tillstånd har meddelats, beaktas självmant av den brottsbekämpande myndigheten. Det skulle kunna inträffa situationer när integritetsintrånget under verkställigheten blir så stort att åtgärden inte längre kan anses tillåten.

När det gäller särskilda provokativa åtgärder innebär de begränsningar som följer av proportionalitetsprincipen att det i regel inte är möjligt att fatta beslut om provokativa åtgärder som riskerar att leda till skada på människors liv eller hälsa, eller annars innebär oåterkallelig skada på enskild egendom.

2 kap. Ljud- eller bildupptagning samt lokalisering av person

Vad befogenheten avser

1 §

I den utsträckning som följer av 2–5 §§ får teknisk utrustning användas för att ta upp ljud eller bild eller bestämma lokalisering av person.

Paragrafen innehåller en allmän bestämmelse om de befogenheter som ges till de brottsbekämpande myndigheterna i det nu aktuella kapitlet. Befogenheterna avser att i vissa fall med teknisk utrustning få ta upp ljud (2 §) eller bild (3 §) eller bestämma lokalisering (4 §) samt särskilt ingripande ljud-, bild- eller lokaliseringsåtgärder (5 §). I bestämmelsen används det teknikneutrala begreppet teknisk utrustning.

Ljudupptagning av samtal

2 §

Med ljudupptagning av samtal avses i denna lag användande av tekniskt hjälpmedel för upptagning av ljud, dolt eller genom vilseledande, för att ta upp

1. samtal där företrädare för myndigheten själv deltar, eller
2. sådant som avhandlas vid sammanträde eller sammankomst vartill allmänheten inte har tillträde, om företrädare för myndigheten själv deltar i sammanträdet eller sammankomsten.

Bestämmelsen definierar vad som i denna lag avses med ljudupptagning av samtal, dvs. att dolt eller genom vilseledande ta upp vissa samtal eller sådant som avhandlas vid vissa sammanträden och sammankomster med hjälp av tekniskt hjälpmedel. Bestämmelsen omfattar inte åtgärder som enligt annan lag utgör hemliga tvångsmedel (se 1 kap. 3 §). Som angetts i kommentaren till 1 kap. 3 § om lagens tillämpningsområde så innebär det att om åtgärden i sig utgör hemlig teleavlyssning enligt 27 kap. RB eller hemlig rumsavlyssning enligt lagen om hemlig rumsavlyssning blir den nu aktuella lagen inte tillämplig.

Syftet med de befogenheter som lagen innehåller framgår av 1 kap. 1 §. Det är att förebygga, förhindra eller upptäcka brottslig verksamhet, eller att utreda eller beivra brott. Det innebär att om ljudet tas upp enbart i annat syfte, t.ex. för polismannens skydd och säkerhet, kommer en sådan upptagning även fortsättningsvis att kunna ske med stöd av polislagen. Det sistnämnda kan vara fallet när polismannen exempelvis vill skydda sig mot falska påståenden vid senare tillfälle om vad som sagts vid ett möte med en informatör eller när polismannen använder en kroppsmikrofon som en säkerhetsåtgärd vid ett tillslag.

Upptagningen ska ske med hjälp av tekniskt hjälpmedel för återgivning av ljud. Med det uttrycket avses alla slag av fungerande avlyssnings- och inspelningsapparater. Lagrummet blir därmed inte tillämpligt när någon lyssnar med blotta örat, med ett dricksglas mot en vägg eller liknande.

Att ljudet ska tas upp genom det tekniska hjälpmedlet innebär inte att det behöver vara fråga om inspelning av ljud på medium. Även avlyssning som sker utan sådan inspelning faller under bestämmelsen, om ljudet förmedlas via det tekniska hjälpmedlet. Det tekniska hjälpmedlet behöver inte bäras av någon enskild, alltså vara av typen kroppsmikrofon, utan kan även vara placerat på annat sätt, t.ex. dolt i en möbel. Det avgörande är att en företrädare för myndigheten deltar i samtalet eller närvarar vid sammanträdet eller sammankomsten. I annat fall måste förutsättningarna för hemlig rumsavlyssning vara uppfyllda.

Upptagningen av ljud ska ske dolt eller genom vilseledande. Att åtgärden sker dolt innebär att minst en person som deltar i samtalet eller vid sammanträdet eller sammankomsten är ovetande om att upptagning av ljud sker. Dock måste bestämmelserna om ljudupptagning ändå följas, om upptagningen är avslöjad så att den person som skulle vara ovetande om den faktiskt vet om upptagningen

men agerar som om han vore ovetande. Med begreppet vilseledande avses att ljudupptagningen sker öppet för de inblandade medan det brottsbekämpande syftet med åtgärden är dolt. Det sistnämnda kan exempelvis förekomma när en polisman som infiltratör öppet spelar in ljud vid ett möte men de personer som deltar tror att det sker i ett annat syfte än det brottsbekämpande.

I punkterna 1 och 2 preciseras vilka typer av ljud som paragrafen omfattar. Det rör sig om samtal där företrädare för myndigheten själv deltar, eller sådant som avhandlas vid ett sammanträde eller en sammankomst vartill allmänheten inte har tillträde, om någon företrädare för myndigheten själv deltar i sammanträdet eller sammankomsten. Paragrafen omfattar det talade ordet och kan exempelvis avse ljud som förmedlas via en telefon, t.ex. en konferenstelefon vid ett möte. Ljud som åstadkoms i enrum faller utanför regleringen och kan därför åtkommas endast genom hemlig rumsavlyssning. Detsamma gäller som framgått när ingen företrädare för myndigheten deltar i samtalet, sammanträdet eller sammankomsten.

Den person som dolt eller genom vilseledande får samtalet upptaget behöver inte vara misstänkt för brott. Vid prövningen av om åtgärden ska tillåtas måste alltid proportionalitetsprincipen beaktas (se 1 kap. 4 §) och dessutom ska villkor för verkställigheten ges, om det bedöms behövas (se 2 kap. 12 §).

Bestämmelsen innehåller ingen begränsning i lokalt hänseende. Det har därför ingen betydelse i sig var samtalet, sammanträdet eller sammankomsten äger rum. Platsen kan vara en bostad eller ett annat skyddat utrymme som kontor, fabriker och andra arbetsplatser, men också platser som gator, torg, butiker, restauranger, bilar och bussar.

Punkten 1 avser samtal där företrädare för myndigheten själv deltar. Under begreppet företrädare för myndigheten faller polismän och andra tjänstemän vid myndigheten. Bestämmelsen är även tillämplig när polisen vid genomförande av en åtgärd tar biträde av en enskild med stöd av 7 kap. Mot bakgrund av att privatpersoner har rätt att utan rättsligt stöd utföra egna ljudupptagningar av samtal kommer det att finnas ett behov av att skilja mellan situationer där den enskilde biträder polisen med stöd av regleringen i denna lag och situationer där denne själv vidtar åtgärden på egen hand. Avgörande för den bedömningen blir om upptagningen – mot bakgrund av omständigheterna i det enskilda fallet – kan anses ske i polisens eller den enskildes intresse, se även kommentaren till 7 kap. 1 §. Enbart det förhållandet att polisen tillhandahåller tek-

nisk utrustning för en ljudupptagning som genomförs av t.ex. en informatör eller en målsägande innebär dock inte att regleringen blir tillämplig. Ofta torde därför en ljudupptagning som genomförs av en målsägande, i en utpressningssituation eller vid en grov kvinnofridskränkning, inte falla in under bestämmelserna, oavsett om de tekniska hjälpmedlen har tillhandahållits av polisen eller inte.

Enligt punkten 2 kan ljudupptagningen avse sådant som avhandlas vid ett sammanträde eller en sammankomst vartill allmänheten inte har tillträde. Det är därmed fråga om enskild sammankomst (jfr 2 kap. 1 § ordningslagen [1993:1617]) som är tillgänglig endast för en på ett eller annat sätt bestämd eller sluten krets av personer. Företrädaren för myndigheten ska vara en del av den krets av personer som har förtroende att närvara vid sammanträdet eller sammankomsten och ta del av vad som förekommer men behöver inte själv delta i något samtal där.

Bestämmelsen har behandlats i avsnitt 10.5.

Bildupptagning av hem eller korrespondens

3 §

Med bildupptagning av hem eller korrespondens avses i denna lag användande av teknisk utrustning för upptagning av bild, dolt eller genom vilseledande, för att ta upp

1. bild i bostad, annat hus eller rum som inte är tillgängligt för allmänheten,
2. sådan bild som avses i 1 genom särskilt inriktad bildupptagning som sker från annan plats, eller
3. bild av korrespondens genom särskilt inriktad bildupptagning.

Bestämmelsen definierar befogenheten att dolt eller genom vilseledande ta upp vissa bilder med hjälp av teknisk utrustning. Bestämmelsen omfattar inte åtgärder som enligt annan lag utgör hemliga tvångsmedel (se 1 kap. 3 §). Det innebär att om åtgärden i sig skulle utgöra hemlig kameraövervakning enligt 27 kap. 20 a § RB, dvs. den genomförs i hemlighet med fjärrstyrda TV-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar för optisk personövervakning i förundersökning, blir den nu aktuella lagen inte tillämplig. Den tekniska utrustningen som avses i lagen får med andra ord inte vara sådana fjärrstyrda utrustningar som används vid hemlig kameraövervakning. I stället ska det vara fråga

om annan, s.k. handhållen, utrustning. Med det avses inte att utrustningen hela tiden behöver hållas i handen vid upptagningen. Däremot behöver personen som genomför upptagningen finnas i närheten. Gränsdragningen mellan sådan utrustning och utrustning som avses i 27 kap. 20 a § RB får lösas i rättstillämpningen.

Bestämmelsen omfattar såväl en videofilmning som upptagning av enstaka stillbild.

Syftet med de befogenheter som ges i denna lag framgår av 1 kap. 1 §. Det är att förebygga, förhindra eller upptäcka brottslig verksamhet, eller utreda eller beivra brott. Det innebär att om bilden tas upp enbart i annat syfte, t.ex. för polismannens skydd och säkerhet under ett tillslag, kommer en sådan upptagning även fortsättningsvis att kunna ske med stöd av polislagen.

Med uttrycket teknisk utrustning för upptagning av bild avses sådan utrustning som spelar in eller på annat sätt bevarar den upptagna bilden. Således omfattas inte olika slag av kikare som enbart används för att förstärka det mänskliga sinnet. Inte heller omfattas den situationen att en kamera enbart används som kikare utan att bilder tas upp.

Liksom vad som gäller för ljudupptagningar enligt 2 § tillkommer befogenhet att ta upp bilder enligt 3 § de brottsbekämpande myndigheterna. Under begreppet företrädare för myndigheten faller polismän och andra tjänstemän vid myndigheten. Bestämmelsen är även tillämplig när polisen vid genomförande av en åtgärd tar biträde av en enskild med stöd av 7 kap. Mot bakgrund av att privatpersoner har rätt att utan rättsligt stöd göra egna bildupptagningar kommer det att finnas ett behov av att skilja mellan situationer där den enskilde biträder polisen med stöd av regleringen i denna lag och situationer där denne själv vidtar åtgärden på egen hand. Avgörande för den bedömningen blir om upptagningen kan anses ske i polisens eller den enskildes intresse, se även kommentaren till 2 § och 7 kap. 1 §. Enbart det förhållandet att polisen tillhandahåller en kamera för en bildupptagning som genomförs av t.ex. en informatör eller en målsägande innebär inte att regleringen blir tillämplig. En bedömning måste alltid göras mot bakgrund av omständigheterna i det enskilda fallet där den huvudsakliga frågan blir att bedöma på vems initiativ som åtgärden vidtas.

Upptagningen av bild ska ske dolt eller genom vilseledande. En helt öppen bildupptagning av företrädare för myndigheten regleras således inte. Att åtgärden sker dolt innebär att upptagningen genomförs utan att den som blir föremål för den, dvs. någon som

bilden avser att avbilda eller som på någon grund har rådighet över det utrymme eller ställe som avbildas, är medveten om åtgärden. Dock måste bestämmelserna om bildupptagning ändå följas, om upptagningen är avslöjad så att den person som skulle vara ovetande om den faktiskt vet om upptagningen men agerar som om han vore ovetande. Bildupptagning som sker dolt men inom ramen för ett annat tvångsmedel, t.ex. bildupptagning under verkställandet av en husrannsakan som sker utan att den enskilde som blir utsatt för åtgärden vet om den, faller inte under denna lag.

Med begreppet vilseledande avses att bildupptagningen sker öppet för de inblandade medan det brottsbekämpande syftet med åtgärden är dolt. Det sistnämnda kan exempelvis förekomma när en infiltratör öppet fotograferar vid ett möte men de personer som deltar tror att det sker i ett annat syfte än det brottsbekämpande.

I punkterna 1–3 preciseras vilka bilder som paragrafen omfattar. Det rör bild i bostad, annat hus eller rum som inte är tillgängligt för allmänheten och sådan bild tagen från annan plats, om det sker genom särskilt inriktad bildupptagning. Det rör också bild av korrespondens genom särskilt inriktad bildupptagning. Annan bildupptagning, som inte är särskilt reglerad i annan lagstiftning, som lagen om allmän kameraövervakning, får för polisens del genomföras med stöd av polislagen.

Punkten 1 avser bild i bostad, annat hus eller rum som inte är tillgängligt för allmänheten. Upptagningen av bild sker i de fallen inne i det skyddade utrymmet och avser något som finns därinne. Den situationen att bilden tas upp inifrån utrymmet men är särskilt inriktad mot något som finns utanför faller därmed utanför tillämpningsområdet (se dock kommentaren till punkten 2 nedan).

Punkten 1 omfattar bl.a. bostad. Med bostad avses inte enbart permanentbostad utan även tillfällig bostad under den tid den faktiskt används som bostad, t.ex. fritidshus, hotellrum, hytt på båt, tält, husvagn, husbil eller sovdelen i en lastbilshytt.

Vid sidan om bostad omfattar punkten 1 annat hus eller rum som inte är tillgängligt för allmänheten. Med det avses t.ex. uthus, ekonomibyggnader, fritidsbostad (under den tid den inte används som bostad), kontorslokaler, skolor, butiker, trappuppgångar, restauranger, teatrar och biografer. Kravet enligt bestämmelsen är att utrymmet inte ska vara tillgängligt för allmänheten. En restaurang eller en teater kan under viss tid vara tillgänglig för allmänheten men under annan tid vara stängd för allmänheten. Det har därmed betydelse för tillämpningen av paragrafen när bildupptagningen sker i

sådana lokaler. I lokalen kan det dessutom finnas utrymmen med olika karaktär i det avseendet, t.ex. matsalsdelen på en restaurang i förhållande till restaurangköket. En bil hör normalt inte till de platser som omfattas av regleringen. Bestämmelsen omfattar inte heller gårdsplaner och trädgårdar kring bostadshus.

Punkten 2 avser bild enligt punkten 1 där bildupptagningen inte sker inne i sådant utrymme utan i stället från annan plats. Bildupptagningen ska dock vara särskilt inriktad. Innebörden av det är att avsikten med bildupptagningen ska vara att avbilda något inne i utrymmet, t.ex. en upptagning som sker genom att polisen befinner sig ute på en allmän väg och tar fotografi i avsikt att avbilda något innanför ett fönster i en bostad. En bildupptagning som enbart avser att avbilda en fasad på ett hyreshus i stadsmiljö faller därmed inte under bestämmelsens tillämpningsområde.

Enligt punkten 3 omfattas särskilt inriktad bildupptagning av korrespondens av paragrafen. Med korrespondens avses postförsändelser men även exempelvis telefax och elektronisk post. Bestämmelsen blir tillämplig om upptagningen sker före respektive efter befordran, t.ex. ett foto taget av en bildskärm där ett e-postmeddelande visas som ska befordras eller har befordrats eller av ett brev som någon håller på att skriva eller som har förmedlats med posten. Bildupptagningen ska vara särskilt inriktad, dvs. bildupptagningen ska ske i avsikt att avbilda korrespondensen.

Frågorna behandlas i avsnitt 10.6.

Lokalisering av person

4 §

> Med lokalisering av person avses i denna lag användande av teknisk utrustning som placeras på eller i föremål för att bestämma var en person befinner sig.

Bestämmelsen definierar befogenheten att bestämma var en person befinner sig genom att använda teknisk utrustning som placeras på eller i föremål. Personen behöver inte vara identifierad för att åtgärden ska få genomföras. Personen kan också vara helt okänd, eftersom det många gånger inte är möjligt för polisen att ha samtidig visuell spaning mot det föremål som bär den tekniska utrustningen och därmed är det heller inte möjligt att veta vem som faktiskt t.ex. befinner sig i bilen.

Den person som ska lokaliseras genom åtgärden behöver inte vara misstänkt för brott. Vid prövningen av om åtgärden ska tillåtas måste dock alltid proportionalitetsprincipen beaktas (se 1 kap. 4 §) och dessutom ska villkor för verkställigheten ges, om det anses behövas (se 2 kap. 12 §).

Syftet med åtgärden ska vara att bestämma var en person befinner sig, dvs. det är fråga om lokalisering av personen. Är syftet i stället att bestämma ett föremåls lokalisering t.ex. narkotika eller vapen i en container eller lastbil, utan att den som för fartyget eller kör lastbilen i och för sig är av intresse i sammanhanget, sker åtgärden med stöd av enbart polislagen.

I 4 kap. 7 § finns bestämmelser om rätt för polisen att i samband med att den tekniska utrustningen ska installeras, underhållas eller avlägsnas bereda sig tillgång till annars skyddade utrymmen.

Frågorna behandlas i avsnitt 10.7.

Särskilt ingripande åtgärder

5 §

> Om åtgärd som avses i 2–4 §§ kan antas bli av särskilt ingripande slag ska frågan om tillstånd till åtgärden prövas i den ordning som föreskrivs i 8 § respektive 11 §. Vid lokalisering av person gäller detsamma om den tekniska utrustningen placeras på eller i föremål som personen kan antas bära på sig eller ha med sig.

Enligt bestämmelsen ska en åtgärd som kan antas bli av särskilt ingripande slag beslutas i särskild ordning. Vid bedömningen av om en åtgärd är av särskilt ingripande slag måste samtliga omständigheter kring åtgärden beaktas, bl.a. vilken åtgärd det är fråga om, åtgärdens tidsmässiga utsträckning, åtgärdens intensitet samt om åtgärden rör en plats eller person som från någon synpunkt kan betraktas som särskilt skyddsvärd i ett integritetsperspektiv. Intensiv övervakning som pågår under längre tid bör sålunda ofta vara att anses som en åtgärd av särskilt ingripande slag. Om övervakningen är mindre intensiv, t.ex. om det är fråga om lokaliseringsutrustning som placeras i en bil, bör emellertid övervakningen kunna pågå under relativt lång tid utan att den nödvändigtvis blir att se som en åtgärd av särskilt ingripande slag. En omständighet som normalt talar för att en åtgärd är av sådant slag är att den avser de personkategorier som omfattas av 36 kap. 5 § andra–sjätte styckena RB, t.ex. advo-

kater, läkare, präster och journalister. Ytterligare situationer som bör omfattas av bestämmelsen är sådana som avser bild- eller ljudupptagning av intima eller annars känsliga situationer. Vidare kan det vara att bedöma som särskilt ingripande om flera åtgärder kombineras så att integritetsintrånget sammantaget får anses stort. Vid bedömningen kan det förhållandet att lokalisering av person med hjälp av utrustning som sätts på den person som ska lokaliseras alltid ska anses vara särskilt ingripande, användas som en form av måttstock eller jämförelsestandard avseende gränsen för när en åtgärd bör bedömas som särskilt ingripande.

Enligt andra meningen ska åtgärden att lokalisera en person alltid anses vara särskilt ingripande när den tekniska utrustningen placeras på eller i föremål som personen kan antas bära på sig eller ha med sig. Det motsvarar sådana föremål som typiskt sett omfattas av en undersökning enligt bestämmelserna om kroppsvisitation enligt 28 kap. 11 § RB, exempelvis kläder, väskor, kassar, paket och barnvagnar. Däremot omfattas inte fordon som bilar och motorcyklar och inte heller båtar.

Förundersökning

6 §

I förundersökning får åtgärd enligt 2–5 §§ vidtas om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

Paragrafen anger de grundläggande förutsättningarna för att åtgärder enligt detta kapitel ska kunna komma i fråga i en förundersökning.

Enligt bestämmelsen ska åtgärden kunna antas vara av särskild betydelse för utredningen. Det innebär en begränsning så till vida att det inte kan vara fråga om en alltför vid bedömning av värdet av omständigheterna för att driva förundersökningen framåt. Bedömningen av omständigheternas värde får inte bygga på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter.

Av bestämmelsen framgår att åtgärden får användas vid utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver. Därmed kommer åtgärderna att kunna genomföras vid sådana brott som är häktningsgrundande enligt 24 kap. 1 § första stycket RB och som därmed skulle kunna leda till ett frihetsberövande.

Bestämmelserna har motiverats i avsnitt 10.5.2, 10.6.2 och 10.7.2.

7 §

I förundersökning prövas frågor om tillstånd till åtgärder enligt 2–4 §§ av undersökningsledaren eller åklagaren. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Av paragrafens första mening följer att det är undersökningsledaren eller åklagaren som beslutar i fråga om sådana åtgärder enligt 2 kap. som inte är särskilt ingripande enligt 5 §. Undersökningsledare kan vara polis eller åklagare, beroende på om det är polismyndighet eller åklagare som leder utredningen (se 23 kap. 3 § RB).

I bestämmelsens andra mening framgår att en polisman får besluta om åtgärden, om det är fara i dröjsmål. Det sistnämnda uttrycket har samma innebörd som i rättegångsbalkens bestämmelser om förvar, beslag och husrannsakan (26 kap. 3 §, 27 kap. 4 § och 28 kap. 5 §). Beslut av undersökningsledare ska inte hinna avvaktas utan risk för att syftet med åtgärden blir förfelat. Det kan också uttryckas så att ändamålet med åtgärden riskerar att gå förlorat om undersökningsledarens tillstånd skulle avvaktas. Så kan exempelvis vara fallet när polisens spanare iakttar hur någon går in i ett hus och omedelbart behöver dokumentera något för utredningen intressant genom att fotografera in genom fönstret.

Frågorna har behandlats i avsnitt 10.5.3, 10.6.3 och 10.7.3.

8 §

I förundersökning prövas frågor om tillstånd till åtgärder enligt 5 § av rätten på ansökan av åklagaren.

Kan det befaras att inhämtande av rättens tillstånd till åtgärden skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd, i avvaktan på rättens beslut, ges av åklagaren, eller, om åklagarens beslut inte kan avvaktas, av polisman

Har åklagaren eller polisman gett ett sådant interimistiskt tillstånd ska åklagaren genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. En sådan prövning ska ske även om åtgärden till fullo har verkställts. Finner rätten att det inte finns skäl för åtgärden ska den upphäva beslutet.

Av paragrafens första stycke framgår att det är rätten som beslutar i fråga om sådana särskilt ingripande åtgärder som avses i 5 § och att det sker på ansökan av åklagaren.

I andra stycket ges åklagaren respektive – i särskilt brådskande fall – polisman rätt att besluta om interimistiskt tillstånd. Det interimistiska tillståndet får ha samma omfattning som det domstolsbeslut som inte kan inväntas. Det kan ges i situationer där ändamålet med åtgärden riskerar att gå förlorat. Så kan exempelvis vara fallet i brådskande lägen där en målsägande blir utsatt för utpressning eller om de brottsbekämpande myndigheterna får kännedom om ett nära förestående möte som är av intresse att dokumentera. Polisman får ge ett sådant tillstånd om åklagarens beslut inte kan avvaktas. Det kan t.ex. bli aktuellt om polismannen vid ett ingripande hör att hot uttalas mellan personer och vill dokumentera detta med ljudupptagningsfunktionen i en mobiltelefon.

I paragrafens tredje stycke föreskrivs att om åklagaren eller polisman har fattat ett interimistiskt beslut, ska åklagaren genast göra en skriftlig anmälan om åtgärden hos rätten. Med ”genast” avses som utgångspunkt att ett beslut respektive en anmälan ska göras i ett sammanhang. Har polisman fattat beslutet, ska det så fort som möjligt rapporteras till åklagaren, som därefter genast ska göra anmälan. I anmälan ska åklagaren ange skälen för åtgärden. Rätten ska skyndsamt ta upp ärendet till prövning. Det kan ske utan att rätten håller ett sammanträde. Till skillnad från vad som gäller för frågor om häktning ska rätten pröva anmälan även om åtgärden har upphört, t.ex. på grund av att den till fullo har verkställts.

Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva åklagarens tillstånd. Skulle rätten upphäva tillståndet för att det inte finns skäl för åtgärden inträder inte något automatiskt förbud att använda informationen som har inhämtats, även om det torde kunna förväntas att informationen av närmast etiska skäl i normalfallet inte längre kommer att användas efter ett avslagsbeslut. Frågan om i vilken utsträckning sådan information ändå kan användas av de brottsbekämpande myndigheterna får i stället ses mot bakgrund av principen om fri bevisprövning. Några regler som förbjuder användningen av bevis som tillkommit på ett sätt som inte står i överensstämmelse med lagstiftningen finns inte (se t.ex. NJA 1986 s. 489 och 2007 s. 1037), även om det enligt Europakonventionen finns ett visst begränsat utrymme att avvisa olagligt åtkommen bevisning som medför att rätten till en rättvis rättegång skulle ha gått förlorad. En annan sak är att bevisning som tillkommit genom

användning av olagliga eller uppenbart otillbörliga metoder på grund av omständigheterna under vilka bevisen införskaffades kan ha ett lågt eller inget bevisvärde eller utgöra grund för strafflindring (se NJA 2007 s. 1037). Från detta får skiljas frågan om polis eller åklagare som vid anskaffandet av bevis bryter mot reglerna i rättegångsbalken eller annan lagstiftning kan bli föremål för disciplinära eller straffrättsliga åtgärder.

Frågorna har behandlats i avsnitt 10.5.3, 10.6.3 och 10.7.3.

Underrättelseverksamhet

9 §

> I en undersökning för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, får åtgärd enligt 2–5 §§ vidtas om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Paragrafen anger de grundläggande förutsättningarna för att åtgärder enligt detta kapitel ska kunna komma i fråga i underrättelseverksamhet.

Åtgärderna får enligt bestämmelsen ske i en undersökning i syfte att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Begreppet undersökning innefattar olika former av ärenden i underrättelseverksamheten. Det kan vara fråga om en särskild undersökning i kriminalunderrättelseverksamhet. En sådan innebär, enligt 3 § polisdatalagen, insamling, bearbetning och analys av uppgifter i syfte att ge underlag för beslut om förundersökning eller om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Även andra termer används av myndigheterna för att beskriva att det ska vara fråga om någon form av avgränsat ärende som uppgifterna hämtas in i. Exempel på begrepp är underrättelseprojekt och aktionsgruppsinsats.

Förutsättningen för att en åtgärd ska kunna komma i fråga är att det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Att det ska finnas ”särskild” anledning att anta att uppgifterna på det sättet kan vara till nytta i undersökningen markerar att det inte kan vara fråga om en alltför vid bedömning av värdet av uppgifterna för undersökningen. Bedömningar av uppgifternas värde får inte bygga

på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter. På grundval av faktiska omständigheter ska bedömningen som görs av uppgifternas värde i undersökningen mynna ut i att de kan bidra till att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Med begreppet ”kan bidra” avses att uttrycka att uppgifterna på något sätt ska kunna antas bli av värde i undersökningen och föra denna framåt.

Genom rekvisitet ”brottslig verksamhet” framgår att det i underrättelseverksamhet inte krävs misstanke om ett specifikt brott. Däremot måste den befarade brottsliga verksamheten innefatta brott för vilket är föreskrivet fängelse i ett år eller däröver. Därmed motsvarar kravet på brottslighetens svårhetsgrad i underrättelseverksamhet vad som gäller under förundersökning (se 2 kap. 6 §).

Frågorna har behandlats i avsnitt 10.5.2, 10.6.2 och 10.7.2.

10 §

> I verksamhet enligt 9 § prövas frågor om tillstånd till åtgärder enligt 2–4 §§ av chefen för polismyndigheten. Myndighetschefen får delegera beslutanderätten. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Enligt paragrafen är det i underrättelseverksamhet chefen för polismyndigheten som beslutar om sådana åtgärder enligt 2 kap. som inte är särskilt ingripande enligt 5 §. Beslutanderätten ligger därmed för Rikspolisstyrelsens del på rikspolischefen och för de lokala polismyndigheterna på länspolismästarna. Med myndighetschef avses även säkerhetspolischefen. För tullens del ligger beslutanderätten på generaltulldirektören (jfr lagens tillämplighet för Tullverket i 13 kap. 1 §).

Myndighetschefen får delegera beslutanderätten. I paragrafen anges inte vem som kan komma i fråga eller några kvalifikationskrav rörande den person som blir aktuell för att erhålla en sådan delegation. Det ska dock inte vara fråga om personer som deltar i den underrättelseverksamhet där åtgärden ska genomföras. I stället är det fråga om personer på chefsnivå, t.ex. myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen, biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet.

Ekobrottsmyndigheten är en åklagarmyndighet. I Ekobrottsmyndighetens underrättelseverksamhet blir det rikspolischefen som

fattar beslut med möjlighet att delegera beslutanderätten till den som leder polisverksamheten vid Ekobrottsmyndigheten.

I bestämmelsens andra mening framgår att en polisman får besluta om åtgärden, om det är fara i dröjsmål. Det sistnämnda uttrycket har samma innebörd som i rättegångsbalkens bestämmelser om förvar, beslag och husrannsakan (jfr 26 kap. 3 §, 27 kap. 4 § och 28 kap. 5 §). Beslut av chefen för polismyndigheten ska inte hinna avvaktas utan risk för att syftet med åtgärden blir förfelat. Det kan också uttryckas så att ändamålet med åtgärden riskerar att gå förlorat om chefens tillstånd skulle avvaktas, jfr författningskommentaren till 7 §.

Bestämmelserna har motiverats i avsnitt 10.5.3, 10.6.3 och 10.7.3.

11 §

I verksamhet enligt 9 § prövas frågor om tillstånd till åtgärder enligt 5 § av Nämnden.

Kan det befaras att inhämtande av Nämndens tillstånd till åtgärden skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd, i avvaktan på Nämndens beslut, ges av chefen för polismyndigheten. Myndighetschefen får delegera beslutanderätten. Om inte heller myndighetschefens beslut kan avvaktas får tillstånd, i avvaktan på Nämndens beslut, ges av polisman.

Har chefen för polismyndigheten eller polisman gett ett interimistiskt tillstånd ska polismyndigheten genast göra en skriftlig anmälan om åtgärden till Nämnden. I anmälan ska skälen för åtgärden anges. Nämnden ska skyndsamt pröva ärendet. En sådan prövning ska ske även om åtgärden till fullo har verkställts. Finner Nämnden att det inte finns skäl för åtgärden ska den upphäva beslutet.

Av paragrafens första stycke framgår att det i underrättelseverksamhet är Nämnden som beslutar i fråga om sådana särskilt ingripande åtgärder som avses i 5 § och att det sker på ansökan av polismyndigheten.

I andra stycket ges chefen för polismyndigheten respektive – i särskilt brådskande fall – polisman rätt att besluta om interimistiskt tillstånd. Det interimistiska tillståndet får ha samma omfattning som det beslut av Nämnden som inte kan inväntas. Det kan ges i situationer där ändamålet med åtgärden riskerar att gå förlorat. Även den interimistiska beslutanderätten kan delegeras. Detta kan göras till samma krets av personer som kan motta delegerad beslutanderätt enligt 10 §.

I andra styckets sista mening ges polisman en rätt att fatta interimistiskt beslut om inte heller beslut av chefen för polismyndigheten, eller den till vilken den interimistiska beslutanderätten delegerats, kan inväntas. Det får förutsättas att denna möjlighet kommer att användas sparsamt. Det bör endast i undantagsfall saknas tid att ens inhämta beslut enligt andra styckets första mening.

I paragrafens tredje stycke föreskrivs att om chefen för polismyndigheten eller polisman har fattat ett interimistiskt beslut, ska polismyndigheten genast göra en skriftlig anmälan om åtgärden hos Nämnden. Med ”genast” avses som utgångspunkt att ett beslut respektive en anmälan ska göras i ett sammanhang. Har polisman fattat beslutet, ska det så fort som möjligt rapporteras till sin förman. Till skillnad från vad som gäller enligt andra stycket är chefen för polismyndighet inte utpekad i tredje stycket. Anmälningsrätten får därmed delegeras också till andra än personer på chefsnivå (jfr 6 och 6 a §§ polisförordningen [1998:1558]). I anmälan ska anges skälen för åtgärden. Nämnden ska skyndsamt ta upp ärendet till prövning. Det kan ske utan att Nämnden håller ett sammanträde.

Om Nämnden finner att det inte finns skäl för åtgärden, ska den upphäva det interimistiska tillståndet. Skulle Nämnden upphäva tillståndet för att det inte finns skäl för åtgärden inträder, i likhet med vad som enligt 8 § gäller i en förundersökningssituation, inte något automatiskt förbud att använda informationen som har inhämtats (se närmare kommentaren till 8 § ovan).

Frågorna har behandlats i avsnitt 10.5.3, 10.6.3 och 10.7.3.

Gemensamma bestämmelser

12 §

> Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga tre månader från dagen för beslutet. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Av paragrafen framgår att tillstånd till åtgärder enligt detta kapitel, såväl i förundersökning som i underrättelseverksamhet, inte får bestämmas att gälla längre än nödvändigt och att tiden i alla händelser inte får överstiga tre månader från dagen för beslutet. Finns det, när tiden har gått ut, fortfarande förutsättningar för åtgärden, kan tillståndstiden förlängas vid en ny prövning.

Tillståndets omfattning kan vara begränsat till ett visst tillfälle men behöver inte vara det. Tillstånd kan i stället ges generellt t.ex. för viss ljudupptagning, bildupptagning eller lokalisering. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Sådana villkor kan exempelvis gå ut på att minska risken för att samtal med personer som är ovidkommande för utredningen tas upp eller att sådana personer tas upp på bild. Det kan röra begränsningar av på vilka platser eller vid vilka tidpunkter ljud- eller bildupptagning får ske. Det kan också vara fråga villkor som avser privilegierad eller annars känslig information. Exempelvis kan begränsningar ske vad gäller vissa platser, motsvarande vad som gäller vid hemlig rumsavlyssning enligt 4 § lagen om hemlig rumsavlyssning för t.ex. medieredaktioner, advokatkontor, läkarmottagningar och platser för bikt och själavård. De begränsande villkoren kan också avse samtal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § RB andra–sjätte styckena RB, inte skulle kunna höras som vittne om det som sagts eller på annat sätt framkommit, t.ex. advokater, läkare, präster och journalister. När det gäller lokalisering av person kan villkoren exempelvis gå ut på att minska risken för att personer som är ovidkommande för utredningen lokaliseras. Begränsningarna kan avse vilka föremål som den tekniska utrustningen får placeras på eller i, på vilka platser lokalisering får ske och under vilka tider åtgärden får genomföras.

Frågorna har behandlats i avsnitt 10.9.

13 §

> Om det inte längre finns skäl för åtgärden ska beslutet omedelbart hävas. Har beslutet fattats av rätten får det hävas även av åklagaren. Har beslutet fattas av Nämnden får det hävas även av polismyndigheten.

Om det under den tid som tillståndet gäller kommer fram att de lagliga förutsättningarna för tillståndet har fallit bort, ska, enligt bestämmelsen, beslutet omedelbart hävas. I förundersökning kan det exempelvis vara fallet när det upptäcks att brottsligheten inte är så allvarlig att den kan motivera ett beslut om ljudupptagning. I underrättelseverksamhet kan det ha kommit fram uppgifter om att den brottsliga verksamhet som avsågs förhindras har genomförts. Finns det i sistnämnda fall fortfarande skäl för att genomföra ljudupptagning, får beslut om det fattas enligt de bestämmelser som

gäller för förundersökning. Det får dock anses vara det normala att åtgärder som har beslutats i underrättelseverksamhet fortgår till dess beslut har hunnit inhämtats i förundersökning.

Det följer av allmänna principer att verkställigheten ska avbrytas redan före det att beslutet formellt hävs, om det kan konstateras att ett hävande kan bli aktuellt.

Skulle åklagaren enligt bestämmelsen ha hävt rättens beslut, bör åklagaren underrätta domstolen om det. På motsvarande sätt bör polismyndigheten underrätta Nämnden.

Frågan har behandlats i avsnitt 10.9.

3 kap. Identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m.

Vad befogenheten avser

1 §

I den utsträckning som följer av 2–4 §§ får tekniska hjälpmedel användas för att identifiera mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, eller för att störa kommunikation med sådan utrustning.

Bestämmelsen behandlar för det första användandet av tekniska hjälpmedel för sändning eller mottagning av radiovågor för att identifiera vilken mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som befinner sig inom ett visst geografiskt område. Med nuvarande tekniska standarder är det användningen av en s.k. IMSI-catcher som åsyftas.

En IMSI-catcher är ett tekniskt hjälpmedel som närmast kan betraktas som en portabel basstation för mobiltelefoni. IMSI-catchern ger uppgift om IMSI- och IMEI-nummer tillhörande de mobila elektroniska kommunikationsutrustningar som finns i närheten av den. Mobila elektroniska kommunikationsutrustningar som avses är huvudsakligen mobiltelefoner och datormodem som använder sig av mobiltelenätet för kommunikation. Den tekniska utvecklingen gör att det inte är otänkbar att det i en framtid kan omfatta även andra former av kommunikationsverktyg som fungerar på motsvarande sätt.

Ett IMSI-nummer (International Mobile Subscriber Identity) är kopplat till abonnentens telefonnummer medan IMEI-numret

(Internationl Mobile Equipment Identity) ger uppgift om identiteten på kommunikationsutrustningen.

IMSI-catchern ger information även om andra mobila elektroniska kommunikationsutrustningar som används i närheten. Allt efter omständigheterna kräver då detta att något fler än en enda ”sökning” sker i området kring den telefon som ska ”ringas in”. Det sker genom en jämförelse mellan uppgifterna från de olika platserna. Det geografiska området i vilka de korta sökningarna sker (någon enstaka sekund) begränsas genom att utrustningens räckvidd justeras efter förhållandena på platsen.

Vidare behandlar bestämmelsen användandet av tekniska hjälpmedel för sändning eller mottagning av radiovågor för att störa mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation. Det som här avses är sådana störsändare som anges i 14 § förordningen (2003:396) om elektronisk kommunikation.

Identifiering

2 §

> Med identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation avses i denna lag användande av tekniska hjälpmedel för sändning eller mottagning av radiovågor för att identifiera vilken mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation som befinner sig inom ett visst geografiskt område.

Bestämmelsen definierar vad som i lagen avses med identifiering av mobil elektronisk kommunikation eller annan utrustning för radiokommunikation. Den tar som framgått i dagsläget främst sikte på användningen av en IMSI-catcher. Typexempel på när en IMSI-catcher används är för att identifiera vilka mobiltelefoner som används av personer som är föremål för hemlig teleavlyssning men försöker undgå avlyssningen genom att skifta mellan ett antal telefoner och kontantkort. Ett annat exempel på användning av IMSI-catcher är för att lokalisera en viss mobiltelefon och, om personen bär mobiltelefonen med sig, därmed en viss eftersökt person. IMSI-catchern kan även användas för att vid spaningsarbete kontrollera om en viss mobiltelefon befinner sig på en viss plats. Samtliga åtgärder sker genom att IMSI-catchern identifierar vilka mobil-

telefoner eller andra mobila kommunikationsutrustningar, t.ex. modem för mobilt bredband, som finns inom ett visst geografiskt område.

Frågorna har behandlats i avsnitt 11.2.1.

Störning

3 §

Med störning av kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation avses i denna lag användande av tekniska hjälpmedel för sändning eller mottagning av radiovågor för att störa kommunikation med mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation inom ett visst geografiskt område.

Bestämmelsen definierar vad som i lagen avses med störning av kommunikation med mobil elektronisk kommunikation eller annan utrustning för radiokommunikation. En störsändare kan användas som ett verktyg för att hindra kommunikation med mobiltelefoner inom ett begränsat område, t.ex. i samband med gisslansituationer. Störsändare kan också inriktas på andra frekvenser och därmed hindra mottagning av t.ex. radio eller tv-utsändningar.

Effekten och frekvensen på en störsändare kan justeras för att inte störa ut ett större geografiskt område än nödvändigt och för att slå ut enbart vissa former av kommunikation.

Frågorna har behandlats i avsnitt 11.2.1.

Särskilt ingripande åtgärder

4 §

Om åtgärd som avses i 2 eller 3 § kan antas bli av särskilt ingripande slag ska åtgärden beslutas i den ordning som föreskrivs i 7 § respektive 10 §.

Paragrafen innehåller bestämmelser om att vid de fall en identifierings- eller störningsåtgärd är att anse som särskilt ingripande ska en särskild beslutsordning gälla. Hänvisningen till 7 § respektive 10 § innebär att det i sådana fall är rätten som prövar frågan i förundersökning och Nämnden i underrättelseverksamhet.

Åtgärder som får anses vara av särskilt ingripande slag är identifierings- eller störningsåtgärder där integritetsintrånget blir mer påtagligt. Det kan t.ex. bero på hur lång tid åtgärden är avsedd att användas. Det kan även röra sig om situationer där hög effekt på utrustningen används, vilket får till följd att ett stort antal utrustningar för mobil elektronisk kommunikation eller annan radioutrustning riskerar att påverkas av åtgärden, antingen genom att de identifieras, eller störs ut.

En störningsåtgärd får normalt anses betydligt mer ingripande än en identifieringsåtgärd, eftersom den rent faktiskt syftar till att hindra ett större eller mindre antal personer från att kommunicera via en mobiltelefon, en dator eller liknande. En störningsåtgärd som riskerar att drabba fler än ett fåtal personer under mer än en ytterst kort tid är normalt att anse som särskilt ingripande i paragrafens mening.

Å andra sidan får alltså identifieringsåtgärder normalt anses som mindre ingripande och bör mer sällan föranleda en tillämpning av paragrafen. Sådana situationer där identifieringsåtgärden ändå kan vara att anse som särskilt ingripande kan vara att en viss person, eller egentligen en viss persons elektroniska kommunikationsutrustningar, regelmässigt kommer att utsättas för identifieringsåtgärder under en längre tid. En jämförelse kan här göras med åtgärder för lokalisering av person. Identifieringsåtgärder skulle också kunna ses som särskilt ingripande om de tog sikte på att identifiera elektronisk kommunikationsutrustning som används av personkategorier som omfattas av 36 kap. 5 § andra–sjätte styckena RB, t.ex. advokater, läkare, präster och journalister. Ytterligare identifieringssituationer som kan omfattas av bestämmelsen är sådana som avser identifiering i anslutning till att någon befinner sig i intima eller annars känsliga situationer, jfr kommentaren till 2 kap. 5 §.

Frågorna har behandlats i avsnitt 11.2.3.

Förundersökning

5 §

I förundersökning får åtgärd enligt 2–4 §§ vidtas om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver.

Paragrafen anger de grundläggande förutsättningarna för att identifiering eller störning av mobil elektronisk kommunikationsutrustning eller annan radioutrustning ska få ske inom ramen för en förundersökning. Förutsättningarna överensstämmer med vad som enligt 2 kap. gäller för upptagning av ljud, bild och lokalisering av person.

Frågorna har behandlats i avsnitt 11.2.2.

6 §

I förundersökning prövas frågor om tillstånd till åtgärder enligt 2 eller 3 § av undersökningsledaren eller åklagaren. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Av paragrafens första mening följer att det är undersökningsledaren eller åklagaren som beslutar i fråga om sådana åtgärder enligt 3 kap. som inte särskilt ingripande enligt 4 §. Undersökningsledare kan vara polis eller åklagare, beroende på om det är polismyndighet eller åklagare som leder utredningen (se 23 kap. 3 § RB).

I bestämmelsens andra mening framgår att en polisman får besluta om åtgärden, om det är fara i dröjsmål. Det sistnämnda uttrycket har samma innebörd som i 2 kap. 7 §. Exempel på fara i dröjsmål kan vara om det pågår en beslutad identifieringsåtgärd mot en viss person och det i samband med det uppkommer misstankar mot en viss ytterligare person som måste följas upp genom ytterligare omedelbara identifieringsåtgärder. Det kan också föreligga fara i dröjsmål om polisen i nödliknande situationer behöver använda störsändare för att t.ex. förhindra samtal och meddelanden från att komma fram till en mobiltelefon med okänt nummer som finns i närheten av en misstänkt fjärrstyrd sprängladdning.

Frågorna har behandlats i avsnitt 11.2.3.

7 §

I förundersökning prövas frågor om tillstånd till åtgärder enligt 4 § av rätten på ansökan av åklagaren.

Kan det befaras att inhämtande av rättens tillstånd till åtgärden skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd, i avvaktan på rättens beslut, ges av åklagaren, eller, om åklagarens beslut inte kan avvaktas, av polisman.

Har åklagaren eller polisman gett ett sådant interimistiskt tillstånd ska åklagaren genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva

ärendet. En sådan prövning ska ske även om åtgärden till fullo har verkställts. Finner rätten att det inte finns skäl för åtgärden ska den upphäva beslutet.

Bestämmelsen motsvarar vad som enligt 2 kap. 8 § gäller för särskilt ingripande ljudupptagningar m.m.

Av paragrafens första stycke framgår att det är rätten som beslutar i fråga om sådana särskilt ingripande åtgärder som avses i 4 § och att det sker på ansökan av åklagaren.

I andra stycket ges åklagaren respektive – i särskilt brådskande fall – polisman rätt att besluta om interimistiskt tillstånd. Det interimistiska tillståndet får ha samma omfattning som det domstolsbeslut som inte kan inväntas. Det kan ges i situationer där ändamålet med åtgärden riskerar att gå förlorat på motsvarande sätt som gäller för ljudupptagningar m.m. enligt 2 kap. 8 §. Rätten för polisman att fatta interimistiskt beslut får förutsättas komma att användas mycket sparsamt. Det bör endast i speciella undantagsfall saknas tid att ens inhämta beslut från åklagaren.

I paragrafens tredje stycke föreskrivs att om åklagaren eller polisman har fattat ett interimistiskt beslut, ska åklagaren genast göra en skriftlig anmälan om åtgärden hos rätten. Bestämmelsen har samma innebörd som i 2 kap. 8 §.

I många fall när polis eller åklagare har fattat interimistiskt beslut får det antas att beslutet har hunnit verkställas till fullo innan rättens prövning kan ske. I likhet med vad som gäller enligt 2 kap. 8 § ska dock rätten ändå pröva om åtgärden varit tillåtlig eller inte. Om rätten finner att åtgärden inte varit tillåtlig får dock beslutet, särskilt när det gäller störsändare, inga andra konsekvenser än att det bör följas upp av de brottsbekämpande myndigheterna samt att det kan bli föremål för tillsyn.

Frågorna har behandlats i avsnitt 11.2.3.

Underrättelseverksamhet

8 §

I en undersökning för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, får åtgärd enligt 2–4 §§ vidtas om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Paragrafen anger de grundläggande förutsättningarna för att identifiering eller störning av mobil elektronisk kommunikationsutrustning eller annan radioutrustning ska få ske i underrättelseverksamheten. Förutsättningarna överensstämmer med vad som enligt 2 kap. gäller för upptagning av ljud, bild och lokalisering av person.

Frågorna har behandlats i avsnitt 11.2.2.

9 §

I verksamhet enligt 8 § prövas frågor om tillstånd till åtgärder enligt 2 eller 3 § av chefen för polismyndigheten. Myndighetschefen får delegera beslutanderätten. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Enligt paragrafens första mening är det i underrättelseverksamhet chefen för polismyndigheten som beslutar om sådana åtgärder enligt 3 kap. som inte är särskilt ingripande enligt 4 §.

Myndighetschefen får enligt andra meningen delegera beslutanderätten på motsvarande sätt som vad som enligt 2 kap. 10 § gäller för t.ex. ljudupptagningar.

I paragrafens tredje mening framgår att en polisman får besluta om åtgärden, om det är fara i dröjsmål. Det sistnämnda uttrycket har samma innebörd som i 2 kap. 7 och 10 §§.

Frågorna har behandlats i avsnitt 11.2.3.

10 §

I verksamhet enligt 8 § prövas frågor om tillstånd till åtgärder enligt 4 § av Nämnden på ansökan av polismyndigheten.

Kan det befaras att inhämtande av Nämndens tillstånd till åtgärden skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd, i avvaktan på Nämndens beslut, ges av chefen för polismyndigheten. Myndighetschefen får delegera beslutanderätten. Om inte heller myndighetschefens beslut kan avvaktas får tillstånd, i avvaktan på Nämndens beslut, ges av polisman.

Har chefen för polismyndigheten eller polisman gett ett interimistiskt tillstånd ska polismyndigheten genast göra en skriftlig anmälan om åtgärden till Nämnden. I anmälan ska skälen för åtgärden anges. Nämnden ska skyndsamt pröva ärendet. En sådan prövning ska ske även om åtgärden till fullo har verkställts. Finner Nämnden att det inte finns skäl för åtgärden ska den upphäva beslutet.

Bestämmelsen motsvarar vad som enligt 2 kap. 11 § gäller för särskilt ingripande ljudupptagningar m.m.

Av paragrafens första stycke framgår att det är Nämnden som beslutar i fråga om sådana särskilt ingripande åtgärder som avses i 4 § och att det sker på ansökan av polismyndigheten.

I andra stycket ges chefen för polismyndigheten respektive – i särskilt brådskande fall – polisman rätt att besluta om interimistiskt tillstånd. Det interimistiska tillståndet får ha samma omfattning som det beslut av Nämnden som inte kan inväntas. Det får ges i situationer där det uppkommit ett behov som inte tidigare har förutsetts och man på goda grunder kan befara att nyttan med åtgärden riskerar att gå förlorad om man inväntar Nämndens prövning. Det är i en sådan situation i första hand chefen för polismyndigheten som får fatta sådana interimistiska beslut. På motsvarande sätt som gäller för ljudupptagningar m.m. enligt 2 kap. 11 § kan den interimistiska beslutanderätten delegeras.

I andra styckets sista mening ges polisman en rätt att fatta interimistiskt beslut om inte heller beslut av chefen för polismyndigheten, eller den till vilken den interimistiska beslutanderätten delegerats, kan inväntas. Det får förutsättas att denna möjlighet kommer att användas mycket sparsamt. Det bör endast i speciella undantagsfall saknas tid att ens inhämta beslut enligt andra styckets första mening.

I paragrafens tredje stycke föreskrivs att om chefen för polismyndigheten eller en polisman har fattat ett interimistiskt beslut, ska polismyndigheten genast göra en skriftlig anmälan om åtgärden hos Nämnden. Bestämmelsen har samma innebörd som i 2 kap. 8 och 11§§.

I många fall när chefen för polismyndigheten eller polisman har fattat ett interimistiskt beslut får det antas att beslutet har hunnit verkställas till fullo innan Nämndens prövning kan ske. I likhet med vad som gäller enlig 2 kap. 11 § ska dock Nämnden ändå pröva om åtgärden varit tillåtlig eller inte. Om Nämnden finner att åtgärden inte varit tillåtlig får dock beslutet, särskilt när det gäller störsändare, inga andra konsekvenser än att det bör följas upp av de brottsbekämpande myndigheterna samt kan bli föremål för tillsyn.

Frågorna har behandlats i avsnitt 11.2.3.

Gemensamma bestämmelser

11 §

I ett beslut om identifiering eller störning enligt detta kapitel ska det anges vilken tid beslutet avser samt vilken teleadress, vilken person eller vilket avgränsat geografiskt område beslutet avser.

Paragrafen reglerar vilka uppgifter ett beslut om identifiering av mobil elektronisk kommunikationsutrustning eller störning av kommunikation med sådan utrustning ska innehålla. Ett sådant beslut ska alltid innehålla uppgift om vilken tid beslutet avser. Beslutet ska vidare innehålla uppgift om vilken teleadress, vilken person eller vilket avgränsat geografiskt område beslutet avser. Samtliga dessa uppgifter behöver dock inte anges. Vilken eller vilka av uppgifterna som beslutet kan innehålla är beroende av vad den aktuella identifierings- eller störningsåtgärden syftar till.

12 §

Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga tre månader från dagen för beslutet. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Paragrafen motsvarar vad som enligt 2 kap. 12 § gäller för ljudupptagningar m.m.

Tillståndets omfattning kan vara begränsat till ett visst tillfälle men behöver inte vara det. Tillstånd kan i stället ges generellt t.ex. för identifiering av mobil elektronisk kommunikationsutrustning som tillhör en viss person.

Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Det kan röra begränsningar av på vilka platser eller vid vilka tidpunkter identifiering eller störning får ske. Sådana villkor kan exempelvis syfta till att minska effekterna av åtgärder för störning av kommunikation för att minimera påverkan på kommunikation mellan personer som är ovidkommande för utredningen.

Frågorna har behandlats i avsnitt 11.3.

13 §

Om det inte längre finns skäl för åtgärden ska beslutet omedelbart hävas. Har beslutet fattats av rätten får det hävas även av åklagaren. Har beslutet fattas av Nämnden får det hävas även av polismyndigheten.

Paragrafen motsvarar vad som enligt 2 kap. 13 § gäller för ljudupptagningar m.m.

Frågorna har behandlats i avsnitt 11.3.

4 kap. Tillträde till utrymmen i vissa fall

Infiltrationsverksamhet

Vad befogenheten avser

1 §

I infiltrationsverksamhet får polisen, efter särskilt tillstånd, genom vilseledande åtgärder bereda sig tillträde till bostad, annat hus, rum eller ställe som inte är tillgängligt för allmänheten.

Av paragrafen framgår att det i vissa fall krävs särskilt tillstånd när polisen genom vilseledande åtgärder bereder sig tillträde till bostad, annat hus, rum eller ställe som inte är tillgängligt för allmänheten. Bestämmelsen är endast tillämplig när tillträdet sker i infiltrationsverksamhet. Med infiltrationsverksamhet avses dolda undersökningar där polisens interaktion med målpersonen bedrivs med hjälp av aktivt vilseledande och där det är fråga om vilseledande som har en viss varaktighet över tiden. Bestämmelsen är däremot inte tillämplig då åtgärden är att anse som en husrannsakan eller annan undersökning enligt rättegångsbalkens bestämmelser (jfr t.ex. 28 kap. 1, 3 och 10 §§ RB).

Vilseledande åtgärder enligt denna paragraf utgörs av sådana åtgärder där polisen aktivt ger sken av att vara någon annan än en polis, eller där personen ger sken av att åtgärden vidtas i något annat syfte än det verkligen avsedda. Typfallet är när en polis som arbetar under täckmantel blir inbjuden till en persons bostad eller arbetsplats.

I fråga om vilka platser som åtnjuter skydd motsvarar bestämmelsen delvis regleringen om upptagning av bild i 2 kap. 3 §. Det område som skyddas omfattar alltså bl.a. bostad. Med bostad avses

utrymmen som omfattas av bestämmelsen om hemfridsbrott i 4 kap. 6 § första stycket BrB. Dit hör inte enbart utrymmen som används som permanent bostad utan även sådana utrymmen som används som tillfällig bostad, t.ex. fritidsbostad, hotellrum, hytt på båt och tält.

Vid sidan om bostad omfattar skyddet annat hus, rum eller ställe som inte är tillgängligt för allmänheten. Med det avses utrymmen som omfattas av bestämmelsen om olaga intrång i 4 kap. 6 § andra stycket BrB. Dit hör t.ex. fritidsbostad (under den tid den inte används som bostad), arbetsplatser, fartyg, upplagsplatser, byggnadsplatser, föreningslokaler, skolor, butiker, trappuppgångar, restauranger, teatrar och biografer. Kravet enligt bestämmelsen är att utrymmet inte ska vara tillgängligt för allmänheten. En restaurang eller en teater kan under viss tid vara tillgänglig för allmänheten men under annan tid vara stängd för allmänheten. Det har därmed betydelse för tillämpningen av paragrafen när tillträdet sker i sådana lokaler. I lokalen kan det dessutom finnas utrymmen med olika karaktär i det avseendet, t.ex. matsalsdelen på en restaurang i förhållande till restaurangköket.

Till skillnad från vad som gäller för upptagning av bild omfattas även ”ställe” som inte är tillgängligt för allmänheten. Det innebär att även gård eller trädgård som hör till bostaden omfattas av bestämmelsen. Likaså omfattas uthus och andra ekonomibyggnader som finns inom gården eller trädgården samt gårdsplanen omkring byggnaderna, däremot inte mer avlägsna sådana byggnader.

Frågorna har behandlats i avsnitt 7.3.2.

2 §

> Bestämmelser om användningen av teknisk utrustning för ljud- eller bildupptagning finns i 2 kap.

Paragrafen erinrar om att bestämmelser om användning av teknisk utrustning för ljud- eller bildupptagning finns i 2 kap. Bestämmelserna i det kapitlet ska tillämpas när polisen efter tillstånd enligt 1 § i detta kapitel genom vilseledande bereder sig tillträde till utrymmen och ställen som inte är tillgängliga för allmänheten och samtidigt vill använda teknisk utrustning för sådan ljud- och bildupptagning.

Förundersökning

3 §

I förundersökning prövas frågor om tillstånd till tillträde enligt 1 § av undersökningsledaren eller åklagaren. Vid fara i dröjsmål får polisman, utan särskilt tillstånd, bereda sig sådant tillträde.

Av paragrafens första mening följer att det är undersökningsledaren eller åklagaren som beslutar om tillstånd till tillträde i förundersökning. Undersökningsledare kan vara polis eller åklagare, beroende på om det är polismyndighet eller åklagare som leder utredningen (se 23 kap. 3 § RB).

I bestämmelsen andra mening framgår att en polisman får bereda sig tillträde utan tillstånd av undersökningsledare, om det är fara i dröjsmål. I kommentaren till 2 kap. 7 § utvecklas innebörden av det sistnämnda uttrycket.

Frågorna har behandlats i avsnitt 7.3.2.

Underrättelseverksamhet

4 §

I en undersökning för att förebygga, förhindra eller upptäcka brottslig verksamhet prövas frågor om tillstånd till tillträde enligt 1 § av polismyndigheten. Vid fara i dröjsmål får polisman, utan särskilt tillstånd, bereda sig sådant tillträde.

Enligt paragrafen är det polismyndigheten som beslutar om tillstånd till tillträde i underrättelseverksamhet. Till skillnad från vid beslut om ljudupptagning m.m. i underrättelseverksamhet (se 2 kap. 10 §) är chefen för polismyndighet inte utpekad i paragrafen. Beslutanderätten får när det gäller tillträdesbeslut delegeras till andra än personer på chefsnivå (jfr 6 och 6 a §§ polisförordningen).

Bestämmelserna har motiverats i avsnitt 7.3.2.

Gemensamma bestämmelser

5 §

Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga tre månader från dagen för beslutet. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Av paragrafen framgår att tillstånd till tillträde, såväl i förundersökning som i underrättelseverksamhet, inte får bestämmas att gälla längre än nödvändigt och att tiden i alla händelser inte får överstiga tre månader från dagen för beslutet. Finns det, när tiden har gått ut, fortfarande förutsättningar för åtgärden, kan tillståndstiden förlängas vid en ny prövning.

Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Sådana villkor kan exempelvis röra begränsningar av vilka utrymmen och andra ställen som kan omfattas av åtgärden och under vilka tider åtgärden får genomföras.

6 §

Om det inte längre finns skäl för åtgärden ska beslutet omedelbart hävas.

Om det under den tid som tillståndet gäller kommer fram att det inte längre finns skäl för tillståndet till tillträde, ska, enligt bestämmelsen, beslutet omedelbart hävas. Kravet på omedelbart hävande innebär dock inte att verkställighetsåtgärder behöver avbrytas med sådan omedelbarhet att det skulle innebära en risk för att verksamheten röjs och därmed att polispersonal eller andra utsätts för fara.

Installation av lokaliseringsutrustning

Vad befogenheten avser

7 §

För att installera, underhålla eller avlägsna teknisk utrustning för lokalisering får polisen i hemlighet

1. bereda sig tillträde till en plats som annars skyddas mot intrång,

2. tillfälligt flytta det föremål på eller i vilket utrustningen ska placeras eller finns placerad, samt
3. vidta de andra åtgärder som behövs för att utrustningen ska fungera effektivt.

Polisen får använda teknisk utrustning för att lokalisera egendom eller person. Lokalisering av egendom, t.ex. vapen eller narkotika i containrar eller lastbilar, sker med stöd av polislagen, medan lokalisering av person regleras i 2 kap. För att möjliggöra verkställighet av befogenheterna kan det i båda situationerna krävas att polisen i hemlighet får vidta annars otillåtna åtgärder, såsom att bereda sig tillträde till en plats som annars skyddas mot intrång, att tillfälligt flytta det föremål på eller i vilket utrustningen ska placeras eller finns placerad, samt vidta de andra åtgärder som behövs för att utrustningen ska fungera effektivt. Den nu aktuella paragrafen ger en sådan befogenhet i syfte att installera, underhålla eller avlägsna den tekniska utrustningen. För att åtgärden ska få vidtas krävs särskilt tillstånd, se 8 och 9 §§.

Enligt punkten 1 får polisen bereda sig tillträde till en plats som annars skyddas mot intrång. Med det avses att polisen får öppna t.ex. en container, en väska eller en bil och placera utrustningen inne i utrymmet för att lättare kunna dölja den. Bestämmelsen ger också stöd för att polisen dolt eller genom ett vilseledande t.ex. går in i ett garage för att placera utrustningen på eller i en bil, för att byta batterier på utrustningen eller för att avlägsna utrustningen. I likhet med vad som gäller enligt bestämmelserna om husrannsakan och hemlig rumsavlyssning får polisen ta sig in i det skyddade utrymmet med våld. Polisen får alltså om det anses nödvändigt bryta sig in i t.ex. ett garage för att installera utrustningen. Detta innefattar även en befogenhet för polisen att när det är nödvändigt tillfälligtvis sätta larmanordningar ur funktion, t.ex. genom användning av störningsutrustning (jfr prop. 2005/06:178 s. 104 f.).

Enligt punkten 2 får polisen tillfälligt flytta det föremål på eller i vilket utrustningen ska placeras eller finns placerad. Det kan behöva ske när exempelvis en bil står parkerad på ett sätt som omöjliggör installation, underhåll eller avlägsnande. Det kan också behöva ske för att kunna placera utrustningen i en väska eller i ett paket med vapen eller narkotika.

Enligt punkten 3 får även andra åtgärder än som följer av punkterna 1 och 2 vidtas om det behövs för att utrustningen ska fungera

effektivt. Bestämmelsen ger stöd för att säkra strömförsörjningen till utrustningen genom att den ansluts till bilens elsystem.

Frågorna har behandlats i avsnitt 10.8.2.

Förundersökning

8 §

I förundersökning prövas frågor om tillstånd till åtgärder som avses i 7 § av undersökningsledaren eller åklagaren. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Om åtgärd enligt 7 § avser lokalisering av person av särskilt ingripande slag enligt 2 kap. 5 §, ska vad som sägs i 2 kap. 8 § gälla även för prövning av åtgärden enligt 7 §.

Av paragrafens första stycke framgår att det är undersökningsledaren eller åklagaren som prövar frågor enligt 4 kap. 7 §. Undersökningsledare kan vara polis eller åklagare, beroende på om det är polismyndighet eller åklagare som leder utredningen (se 23 kap. 3 § RB).

I bestämmelsen andra mening framgår att polisman får besluta om åtgärden, om det är fara i dröjsmål. I kommentaren till 2 kap. 7 § utvecklas innebörden av det sistnämnda uttrycket.

Av andra stycket framgår att om åtgärden avser sådan lokalisering av person som enligt 2 kap. 5 § är att anse som av särskilt ingripande slag, ska de bestämmelser om prövning i 2 kap. 8 § gälla även för frågan om tillträde m.m. enligt 4 kap. 7 §, dvs. frågan ska prövas av rätten.

Frågorna har behandlats i avsnitt 10.8.3.

Underrättelseverksamhet

9 §

I en undersökning för att förebygga, förhindra eller upptäcka brottslig verksamhet prövas frågor om tillstånd till åtgärder som avses i 7 § av chefen för polismyndigheten. Myndighetschefen får delegera beslutanderätten. En polisman får besluta om åtgärden, om det är fara i dröjsmål.

Om åtgärd enligt 7 § avser lokalisering av person av särskilt ingripande slag enligt 2 kap. 5 §, ska vad som sägs i 2 kap. 11 § gälla även för prövning av åtgärden enligt 7 §.

Enligt paragrafens första stycke är det chefen för polismyndigheten som prövar frågor som avses i 7 § i underrättelseverksamhet. Myndighetschefen får delegera beslutanderätten. I kommentaren till 2 kap. 10 § utvecklas närmare innebörden av delegationsrätten.

Av andra stycket framgår att om åtgärden avser sådan lokalisering av person som enligt 2 kap. 5 § är att anse som av särskilt ingripande slag, ska de bestämmelser om prövning i 2 kap. 11 § gälla även för frågan om tillträde m.m. enligt 4 kap. 7 §, dvs. frågan ska prövas av Nämnden.

Bestämmelserna har motiverats i avsnitt 10.8.3.

Gemensamma bestämmelser

10 §

> Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga tre månader från dagen för beslutet. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Av paragrafen framgår att tillstånd till åtgärder enligt 4 kap. 7 §, såväl i förundersökning som i underrättelseverksamhet, inte får bestämmas att gälla längre än nödvändigt och att tiden i alla händelser inte får överstiga tre månader från dagen för beslutet. Finns det, när tiden har gått ut, fortfarande förutsättningar för åtgärden, kan tillståndstiden förlängas vid en ny prövning.

Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Sådana villkor kan exempelvis röra begränsningar av vilka platser som får omfattas av åtgärden och hur intrånget eller åtgärden i övrigt får genomföras.

Frågorna har behandlats i avsnitt 10.9.

11 §

> Om det inte längre finns skäl för åtgärden ska beslutet omedelbart hävas. Har beslutet fattats av rätten får det hävas även av åklagaren. Har beslutet fattats av Nämnden får det hävas även av polismyndigheten.

Om det under den tid som tillståndet gäller kommer fram att det inte längre finns lagliga förutsättningar för åtgärden, ska, enligt be-

stämmelsen, beslutet omedelbart hävas. I förundersökning kan det vara fallet när det inte längre finns tillräckliga skäl att genomföra åtgärden, t.ex. för att brottsmisstankarna mot någon inte längre finns. I underrättelseverksamhet kan det exempelvis ha kommit fram uppgifter om att den brottsliga verksamhet som avsågs förhindras har genomförts. Finns det i sistnämnda fall fortfarande skäl för att genomföra åtgärden, får beslut om det fattas enligt de bestämmelser som gäller för förundersökning. Det får dock anses vara det normala att åtgärder som har beslutats i underrättelseverksamhet fortgår till dess beslut har hunnit inhämtas i förundersökning.

Det följer av allmänna principer att verkställigheten ska avbrytas redan före det att beslutet formellt hävs, om det kan konstateras att ett hävande kan bli aktuellt.

Skulle åklagaren enligt bestämmelsen ha hävt rättens beslut, bör åklagaren underrätta domstolen om det. På motsvarande sätt bör polismyndigheten underrätta Nämnden om beslutet fattats i underrättelseverksamheten.

Frågan har behandlats i avsnitt 10.9.

12 §

> Teknisk utrustning för lokalisering ska återtas eller göras obrukbar så snart som möjligt efter det att tiden för tillståndet har gått ut eller tillståndet hävts.

Paragrafen innebär att när tiden för tillstånd till åtgärder enligt 4 kap. 7 § har gått ut ska den tekniska utrustningen återtas eller göras obrukbar så snart som möjligt. Bestämmelsen reglerar därmed inte den situationen att beslut om lokalisering av person har fattas enligt 2 kap. utan att det samtidigt har fattats beslut om tillstånd enligt 4 kap. 7 § om befogenheter vid installation, underhåll och avlägsnande. Inte heller blir den nu aktuella paragrafen tillämplig vid lokaliseringsåtgärder som sker med stöd enbart i polislagen när det inte har fattats beslut om de nämnda befogenheterna.

Ett tillstånd till åtgärder enligt 4 kap. 7 § gäller enbart under den tid som anges i beslutet. Den tekniska utrustningen får alltså inte installeras med hjälp av sådana åtgärder innan tillståndet har getts. Däremot ger den nu aktuella bestämmelsen befogenhet att återta den tekniska utrustningen eller göra den obrukbar efter att tillståndstiden har gått ut, men det måste ske så snart som möjligt därefter.

5 kap. Särskilda provokativa åtgärder

1 §

> Vid förundersökning får polisen, för att få fram bevisning om redan begångna brott, vidta åtgärder som kan leda till att någon förmås att begå en brottslig gärning (särskilda provokativa åtgärder).
>
> Provokativa åtgärder enligt första stycket får vidtas endast om
>
> 1. det föreligger stark misstanke om allvarlig brottslighet, och
> 2. åtgärderna är av synnerlig vikt för utredningen.

Bestämmelsen syftar till att tydliggöra i vilken utsträckning myndigheterna får företa provokativa åtgärder som kan föranleda någon att begå en brottslig gärning och har behandlats ovan i avsnitt 5.3.3. Uttrycket ”kan leda till” är tänkt att inkludera såväl åtgärder som syftar till att föranleda någon att begå en brottslig gärning som åtgärder som riskerar att leda till ett sådant resultat.

Inledningsvis bör framhållas att bestämmelsen endast tar sikte på användningen av provokativa åtgärder inom ramen för en förundersökning. I sammanhanget kan, i linje med vad som anförts ovan i allmänmotiveringen, noteras att det inom ramen för den öppna polisens verksamhet i princip finns skäl att inleda förundersökning om förutsättningarna för att använda provokativa åtgärder föreligger. Frågan om användningen av provokativa åtgärder i Säkerhetspolisens underrättelseverksamhet behandlas i 9 kap.

Av första stycket framgår vidare att syftet med åtgärden ska vara att få fram bevisning om redan begången brottslighet. Provokativa åtgärder ska alltså inom ramen för en förundersökning inte användas för andra ändamål. Detta hindrar naturligtvis inte att åtgärden också kan bidra till att t.ex. rädda egendom som stulits eller att få bort vapen från gatan.

Avgränsningen till åtgärder som kan föranleda en person att begå en brottslig gärning innebär vidare att renodlade s.k. bevisprovokationer inte omfattas av bestämmelsen. Dylika åtgärder kommer också fortsättningsvis att kunna vidtas direkt med stöd av de allmänna principer om polisingripanden som kommer till uttryck i polislagen. Den nu föreslagna bestämmelsen får alltså inte förstås så att den skulle reglera alla typer av åtgärder med provokativa inslag. Som framgår av avsnitt 5.3.2 är syftet endast att reglera de typer av provokation som riskerar att föranleda någon att begå brott (jfr Riksåklagarens riktlinjer och RättsPM 2007:4).

Avgränsningen till åtgärder som kan föranleda någon att begå brott innefattar också en annan begränsning. Uttrycket är inte avsett att innefatta alla åtgärder som skulle kunna vara kausala och leda till att brott förövas, utan en åtgärd måste, för att omfattas av bestämmelsen, innefatta något slags försök att påverka den utsattes beteende. Fråga ska alltså vara om åtgärder som är i viss mån aktiva och innefattar t.ex. frestelser, initiativ, uppmuntran eller annan påverkan (t.ex. en förfrågan). Att tillhandahålla ett stöldobjekt på allmän plats kan normalt inte anses falla under denna kategori av åtgärder. Inte heller omfattas normalt åtgärder som innebär att man avstår från att ingripa eller att man tar över en neutral roll i en i förväg uppgjord plan (t.ex. låter en polisman ersätta en chaufför för att köra en lastbil till sin slutdestination).

Av första punkten i andra stycket framgår att provokativa åtgärder får vidtas endast under förutsättning att det föreligger stark misstanke om allvarlig brottslighet. Detta betyder att provokativa åtgärder får vidtas endast inom ramen för en förundersökning avseende allvarlig brottslighet.

Begreppet allvarlig brottslighet används bl.a. i 2 § lagen om kvalificerade skyddsidentiteter. I författningskommentaren till den bestämmelsen skrevs bl.a. följande (se prop. 2005/06:149 s. 82 f.).

> Begreppet ’allvarlig brottslighet’ är inte knutet till vissa särskilt utpekade straffbestämmelser eller strafflatituder. Huruvida den brottslighet som en viss polisiär verksamhet avser är av så allvarlig karaktär att den bör föranleda ett beslut om kvalificerad skyddsidentitet får bedömas efter omständigheterna. Härvid bör beaktas såväl straffvärdet hos de enskilda brott som verksamheten avser att bekämpa som den samlade brottslighetens omfattning och art. Det bör också tillmätas betydelse om brottsligheten kan sägas vara organiserad eller särskilt samhällsfarlig. Att brottsligheten bedrivs dolt är också av betydelse. Är verksamheten inriktad på brottslighet som enbart förskyller böter, bör beslut om kvalificerad skyddsidentitet givetvis inte komma i fråga.

Dessa uttalanden äger sin giltighet också i detta sammanhang. Om fråga är om brottslighet som inte innefattar brott med ett högt straffvärde bör alltså normalt krävas att den brottsliga verksamheten, på grund av att den bedrivs systematiskt eller organiserat, är särskilt samhällsfarlig.

För att provokativa åtgärder ska få företas ska det vidare föreligga stark misstanke om allvarlig brottslighet. I enlighet med vad som utvecklats i allmänmotiveringen bör det, när en provokativ åtgärd riktar sig mot en viss person, som huvudregel fordras att det

avseende denne föreligger stark misstanke om delaktighet i den allvarliga brottsligheten. Detta kan emellertid inte uppställas som ett ovillkorligt krav. I vissa fall kan det föreligga stark misstanke om allvarlig brottslighet mot en viss person (eller någon i en grupp av personer) samtidigt som det kan vara nödvändigt att rikta en provokativ åtgärd mot en annan person (t.ex. en mellanhand) för att nå fram till den misstänkte. Detta kan inom de ramar som sätts av behovs- och proportionalitetsprinciperna vara tillåtet. Normalt torde emellertid förutsättas att den utsatte är misstänkt för brottslighet av liknande slag eller att det föreligger misstanke om inblandning kopplad till brottslig verksamhet av ifrågavarande typ utan att förundersökning i och för sig behöver bedrivas mot personerna.

I fall där en provokativ åtgärd riktar sig mot en mer obestämd grupp av personer kan det, som ovan utvecklats, inte uppställas något krav på stark misstanke mot en viss person, men det bör istället krävas att det föreligger stark misstanke om att allvarlig brottslig verksamhet pågår eller att sådan brottslighet redan har förövats. Dessa krav kan sägas följa av att de provokativa åtgärderna alltid ska syfta till lagföring av redan begången brottslighet och att det därtill ska finnas goda skäl att tro att de kan leda till resultat.

Av andra stycket framgår att den provokativa åtgärden måste vara av synnerlig vikt för utredningen. Innebörden av begreppet synnerlig vikt berördes i propositionen Vissa tvångsmedelsfrågor (prop. 1988/89:124 s. 44 f.). Där sägs bl.a. följande.

> Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen ska ge avgörande bevisning som omedelbart kan leda till fällande dom. I de flesta fall har telefonavlyssning en indirekt verkan: den bidrar till att kartlägga kontaktvägar och förehavanden, ger uppslag till vidare spaning och bildar underlag för andra åtgärder. En annan, främst i fall enligt 1952 års lag förekommande verkan är att avlyssningen kan föra en på olika sätt uppkommen misstanke till nolläget, dvs. rentvå den misstänkte. Synnerlig vikt för utredningen inrymmer ett kvalitetskrav beträffande de upplysningar som avlyssningen kan ge. Dessa får sålunda inte inskränka sig till obetydliga detaljer, som man kan både ha och mista. Uttrycket innefattar emellertid därutöver ett krav på att utredningsläget gör avlyssningen nödvändig. Vad som kan vinnas genom åtgärden får i princip inte vara åtkomligt med andra, mindre ingripande metoder. En slentrianmässig bedömning får inte förekomma i fråga om vare sig utredningsläget eller de andra förutsättningarna som gäller för tvångsmedlet. En granskning av utredningsmöjligheterna i det enskilda fallet måste alltid verkställas. Granskningen måste mynna ut i bedömningen att utredningen i princip inte kan föras framåt med andra medel och att det finns skäl att räkna med att avlyssningen

ensam eller i förening med andra åtgärder verkligen kan få effekt. I och för sig behöver något absolut hinder inte föreligga mot att få fram information på andra vägar. Det krävs dock att hindret är sådant att det inte skäligen kan begäras att man ska avstå från teleavlyssning. Kan personlig övervakning (skuggning) eller andra åtgärder användas som alternativ, bör det ändå vara tillåtet med teleavlyssning, om alternativen skulle kräva en orimligt hög personalinsats eller vara förenade med avsevärd risk att den pågående utredningen avslöjas för tidigt. Utgångspunkten bör dock vara att i första hand pröva andra metoder.

Begreppet synnerlig vikt innebär alltså att situationen ska göra användningen av provokativa åtgärder nödvändig. Bevisningen ska i princip inte kunna skaffas med andra medel och det ska finnas skäl att räkna med att den provokativa åtgärden ensam eller i förening med andra åtgärder verkligen kan få effekt.

2 §

Frågor om tillstånd till särskilda provokativa åtgärder prövas av åklagaren. Ett tillstånd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks.

Av paragrafens första mening följer att det är åklagaren som beslutar i fråga om provokativa åtgärder. Detta motsvarar vad som redan nu gäller enligt Riksåklagarens riktlinjer för handläggning av provokativa åtgärder (RåR 2007:1). Beslut om och genomförande av provokativa åtgärder innefattar normalt ställningstagande till komplicerade juridiska frågor. Åklagaren bör därför senast vid ett beslut om provokativa åtgärder överta ledningen av förundersökningen enligt 23 kap. 3 § första stycket sista meningen RB.

I andra meningen föreskrivs att ett tillstånd till en provokativ åtgärd ska förenas med de villkor som behövs för att tillgodose intresset av att enskildas personliga integritet inte i onödan kränks. Sådana villkor kan exempelvis röra begränsningar av vilka brott och mot vem som en provokativ åtgärd får avse eller andra villkor kring utförandet av den provokativa åtgärden.

3 §

Om det inte längre finns skäl för de provokativa åtgärderna ska beslutet omedelbart hävas.

Om det under den tid som tillståndet gäller kommer fram att det inte längre finns lagliga förutsättningar för provokativa åtgärder, ska, enligt bestämmelsen, beslutet omedelbart hävas. Så kan vara fallet när det inte längre finns tillräckliga skäl att genomföra åtgärderna, t.ex. för att det, vid en riktad provokation, inte längre kvarstår brottsmisstankar mot den som åtgärderna riktas mot eller därför att den brottslighet som undersökningen avser har klarats upp.

Om ett beslut om en provokativ åtgärd hävs ska åtgärden avbrytas så snart det kan ske utan risk för verksamheten eller annars för inblandade personer. Det följer av allmänna principer att verkställigheten ska avbrytas redan före det att beslutet formellt hävs, om det kan konstateras att ett hävande kan bli aktuellt. Ett beslut om provokativa åtgärder ska hävas av domstolen eller åklagaren.

4 §

För brott som någon har förmåtts att begå genom särskilda provokativa åtgärder får inte dömas till påföljd.

Paragrafen innehåller en straffrihetsregel som tar sikte på sådana brott som föranletts av provokativa åtgärder och har behandlats ovan i avsnitt 5.3.8.

Bestämmelsen innebär att den tilltalade – trots att brott har förövats – inte ska fällas till ansvar, dvs. åtal ska inte väckas och ett eventuellt väckt åtal ogillas på samma sätt som om åtal väckts mot en person som var underårig när gärningen förövades (se 1 kap. 6 § BrB) eller om åtal väckts för en preskriberad gärning (se 35 kap. 1 § BrB). Fråga är alltså inte om en undantagsregel som rättfärdigar gärningen eller ursäktar gärningsmannen och därigenom gör att brott inte förövats. Den föreslagna regleringen innehåller istället en undantagsregel av innebörd att åtal inte ska väckas – och eventuellt väckt åtal ogillas – på den grunden att en materiell straffbarhetsbetingelse inte är uppfylld.

Det förhållandet att det i lagtexten talas om att personen ska ha ”förmåtts” att begå brottet innebär inte bara ett krav på orsakssamband mellan den provokativa åtgärden och brottet utan också

på att gärningen kan sägas ha blivit framprovocerad av åtgärderna. Bestämmelsen tar i första hand sikte på sådana åtgärder som straffrättsligt är att bedöma som anstiftan. Som ovan utvecklats innebär det att mer passiva och neutrala åtgärder – exempelvis att ställa ut ett stöldobjekt på allmän plats eller att enbart acceptera ett erbjudande om att köpa något som redan innehas av den som lämnar erbjudandet – inte omfattas av regleringen. Också mer passiva åtgärder bör dock kunna anses omfattade av bestämmelsen om de antingen på grund av att de innefattar moment av påtagliga frestelser eller på grund av att de upprepade gånger riktas mot en och samma person innebär att den enskilde utsätts för prövningar som klart går utöver det normala.

Den närmare avgränsningen av när någon kan anses ha förmåtts att begå ett brott måste emellertid överlämnas till rättstillämpningen. Det kan emellertid finnas skäl att närmare beröra betydelsen av att initiativet till händelsen kommer från den enskilde.

Enbart det förhållandet att initiativet till en viss gärning ursprungligen kommer från den enskilde bör inte utesluta att bestämmelsen kan bli tillämplig. Om någon t.ex. frågar en polisman om han eller hon har intresse av narkotika och polismannen genom att svara på detta initiativ förmår denne att skaffa fram narkotika, bör bestämmelsen sålunda hindra ansvar såvida det inte kan visas att personen innehaft narkotikan före polisens accepterande svar. I det sistnämnda fallet föreligger naturligtvis inget hinder mot att fälla till ansvar för det redan pågående innehavet.

I fall där polisen enbart svarar på ett erbjudande om att köpa något som redan innehas av den som lämnar erbjudandet kan emellertid den misstänkte i och för sig knappast anses ha förmåtts att begå gärningen på det sätt som bestämmelsen förutsätter. Det kan därför inte anses föreligga något hinder mot att väcka åtal för dylika gärningar (dvs. för den försäljning som kommer till stånd). Grunderna för bestämmelserna bör emellertid också i sådana fall anses ge utrymme för att åtala enbart för innehavet och beakta överlåtelsesyftet vid straffvärdebedömningen.

Det kan finnas skäl att framhålla att det förhållandet att förekomsten av provokation inte ska ses som en omständighet som gör gärningen tillåten – utan som en omständighet utanför brottsbegreppet som ska utgöra hinder mot åtal (liksom mot en fällande dom) – innebär att det inte har någon betydelse om gärningsmannen felaktigt tror sig ha blivit utsatt för provokativa åtgärder.

Straffrihetsregeln kan på sätt som ovan framgått innebära att åtal överhuvudtaget inte ska väckas och att eventuellt väckt åtal ska ogillas. Bestämmelsen kan emellertid också tillämpas i förhållande till sådana kvalificerade gärningsmoment som kan föranleda en gärning att rubriceras som ett allvarligare brott eller – mer allmänt – i relation till omständigheter som är straffvärdehöjande. Om ett stöldbrott hade begåtts oavsett förekomsten av en provokativ åtgärd, men gärningsmannen förmåtts att stjäla något särskilt värdefullt som gör att stölden kan bedömas som grov, ska straffriheten sålunda omfatta det framprovocerade, kvalificerande momentet och gärningsmannen fällas till ansvar för stöldbrott av normalgraden.

Straffriheten enligt denna bestämmelse omfattar inte enbart brott i gärningsmannaskap utan även sådana medverkansgärningar som indirekt bedöms föranledda av de provokativa åtgärderna. I det sammanhanget finns skäl att hänvisa till NJA 2007 s. 1037 (s. 1057):

> När det gäller D.K. hade han inte någon direktkontakt med Bo.K-v utan kom att delta på uppmaning av B.K. Även om han således endast indirekt förmåtts till sin medverkan genom polisens åtgärder måste emellertid också hans handlande anses föranlett av de provokativa åtgärder som polisen vidtagit.

För att straffrihet ska kunna aktualiseras förutsätts att den utsatte förmåtts till brottet genom en provokativ åtgärd. I grunden syftas på sådana åtgärder enligt 1 § som riskerar att föranleda den utsatte att begå brott. För straffrihet kan emellertid inte förutsättas att de provokativa åtgärder som har vidtagits fullt ut har stöd i regelverket. Det förhållandet att en provokativ åtgärd inte har beslutats på föreskrivet sätt eller har vidtagits mot brottslighet som inte kan bedömas som allvarlig bör sålunda inte hindra tillämpning av straffrihetsregeln.

Straffrihet kan emellertid inte komma ifråga om den enskilde förmåtts att begå ett brott vid vilket provokativa åtgärder överhuvudtaget inte får företas, t.ex. fullbordad misshandel eller mord eller dråp. Detta framgår av att det i lagtexten talas om att den utsatte ska ha förmåtts till gärningen ”genom provokativa åtgärder som avses i 1 §”. I dylika fall finns emellertid normalt möjlighet att beakta förekomsten av de provokativa åtgärderna vid straffmätningen enligt 29 kap. 5 § 8 BrB. Även om det är svårt att finna att en provokativ åtgärd i dylika fall helt undergräver rätten till en rättvis rättegång – fråga är inte om ett fall där myndigheterna har använt lagstiftningen för att pröva den utsatte – finns skäl att ta

hänsyn till att det brott som lagförs ytterst härrör från företrädare från staten.

6 kap. Annars brottsliga gärningar

Vad befogenheten avser

1 §

Vid förundersökning om allvarlig brottslighet eller undersökning för att förebygga, förhindra eller upptäcka sådan brottslighet får polisen, efter särskilt tillstånd, utföra en straffbelagd gärning, om det är nödvändigt för att kunna genomföra eller fullfölja en infiltrationsoperation.

Ett sådant tillstånd får endast avse

1. sådana gärningar som inte kan antas föranleda annan påföljd än böter eller,

2. gärningar som, om de bedöms enligt reglerna om medverkan till brott, skulle utgöra medverkan i mindre mån enligt 23 kap. 5 § brottsbalken.

Avser tillståndet en undersökning för att förebygga, förhindra eller upptäcka allvarlig brottslighet får ett tillstånd endast avse gärningar enligt andra stycket 1.

I paragrafen anges att polisen såväl inom ramen för förundersökning som underrättelseverksamhet kan ges tillstånd att utföra en straffbelagd gärning inom ramen för en infiltrationsåtgärd. Av bestämmelsens första stycke framgår att detta förutsätter att utförandet av gärningen, i linje med vad som gäller enligt den allmänna behovsprincipen, är nödvändigt för att kunna genomföra eller fullfölja infiltrationsoperationen.

I andra stycket anges – som ett slags ram för vad som kan omfattas av ett tillstånd – att det inte får vara fråga om andra gärningar än sådana som inte kan antas föranleda annan påföljd än böter. Om tillståndet avser förundersökning kan det emellertid också avse sådana gärningar som skulle kunna bedömas som medverkan i mindre mån enligt 23 kap. 5 § BrB.

Vad gäller dessa begränsningar måste det alltså på förhand göras en preliminär bedömning av gärningen. I det ena fallet avser bedömningen gärningens konkreta straffvärde. För att gärningen ska kunna tillåtas ska det kunna antas att gärningens straffvärde inte kommer att nå upp över bötesnivå. I sammanhanget bör beaktas att det förhållandet att det är fråga om en polisman som begår gär-

ningen i ett brottsbekämpande syfte naturligtvis i sig kan vara en omständighet som påverkar gärningens straffvärde i sänkande riktning. Sålunda kan straffvärdet för en otillåten befattning med vapen eller narkotika påverkas relativt mycket av vad som avses hända med vapnen eller narkotikan.

I det andra fallet avser bedömningen huruvida gärningen, om den bedöms enligt reglerna om medverkan till brott, skulle omfattas av bestämmelsen om medverkan i mindre mån i 23 kap. 5 § BrB. Som ovan framhållits är bedömningen av vad som utgör medverkan i mindre mån relativ och beroende av övriga medverkandes insatser. Medverkan i form av medhjälp torde, med undantag för situationer då gärningsmannen inte uppfyller det allmänna skuldrekvisitet (dvs. kravet på uppsåt eller oaktsamhet), i regel vara att bedöma som medverkan i mindre mån. Det sagda betyder att i fall där någon styr och kontrollerar utförandet av den brottsliga verksamheten bör den som enbart bistår denne kunna bedömas ha medverkat i mindre mån.

I viss utsträckning finns det utrymme att bedöma också vad som i strikt mening utgör brott i gärningsmannaskap – dvs. fall där den medverkande själv uppfyller rekvisiten i den enskilda straffbestämmelsen – som medverkan i mindre mån. Så kan exempelvis vara fallet om någon som hjälper en annan person att hantera ett parti narkotika och därvid tar befattning med narkotikan på ett sätt som avses i 1 § narkotikastrafflagen, men ändå har en begränsad roll i hanteringen av partiet.

I vissa fall av medverkan lagförs gärningen mer eller mindre regelmässigt som ensamt gärningsmannaskap. I dessa fall är bestämmelsen i 23 kap. 5 § BrB formellt inte tillämplig. Den nu föreslagna bestämmelsens formulering, dvs. att den avser sådana gärningar som, om de bedöms enligt reglerna om medverkan till brott, skulle utgöra medverkan i mindre mån enligt 23 kap. 5 § BrB, är avsedd att indikera att sådana fall inte på den grunden är uteslutna från tillämpningsområdet.

Frågorna behandlas i avsnitt 6.4.

2 §

Gärning som avses i 1 § får vidtas endast om infiltrationsoperationen är av synnerlig vikt för utredningen eller undersökningen och skälen för att i samband med infiltrationsoperationen utföra en straffbelagd gärning uppenbart uppväger det men som den kan innebära för allmänna eller enskilda intressen.

Som utvecklats ovan bör tillåtandet av en annars brottslig gärning förutsätta att detta kan motiveras med hänsyn till värdet av den verksamhet inom vilken åtgärden vidtas. I 2 § föreskrivs därför att tillåtandet av en annars brottslig gärning förutsätter dels att själva infiltrationsåtgärden är av synnerlig vikt för utredningen, dels att skälen för att utföra gärningen uppenbart uppväger det men som den kan innebära för allmänna eller enskilda intressen.

Det föreskrivs vidare att åtgärden ska vara av synnerlig vikt för utredningen. Innebörden av detta rekvisit har tidigare behandlats bl.a. i propositionen Vissa tvångsmedelsfrågor (prop. 1988/89: 124 s. 44 f.). De uttalanden som görs där avser telefonavlyssning, men är, *mutatis mutandis*, tillämpliga också i detta sammanhang.

> Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen skall ge avgörande bevisning som omedelbart kan leda till fällande dom. I de flesta fall har telefonavlyssning en indirekt verkan: den bidrar till att kartlägga kontaktvägar och förehavanden, ger uppslag till vidare spaning och bildar underlag för andra åtgärder. En annan, främst i fall enligt 1952 års lag förekommande verkan är att avlyssningen kan föra en på olika sätt uppkommen misstanke till nolläget, dvs. rentvå den misstänkte. Synnerlig vikt för utredning inrymmer ett kvalitetskrav beträffande de upplysningar som avlyssningen kan ge. Dessa får sålunda inte inskränka sig till obetydliga detaljer som man kan både ha och mista. Uttrycket innefattar emellertid därutöver ett krav på att utredningsläget gör avlyssningen nödvändig. Vad som kan vinnas med åtgärden får i princip inte vara åtkomligt med andra, mindre ingripande metoder. En slentrianmässig bedömning får inte förekomma i fråga om vare sig utredningsläget eller de andra förutsättningarna som gäller för tvångsmedlet. En granskning av utredningsmöjligheterna i det enskilda fallet måste alltid verkställas. Granskningen måste mynna ut i bedömningen att utredningen i princip inte kan föras framåt med andra medel och att det finns skäl att räkna med att avlyssningen ensam eller i förening med andra åtgärder verkligen kan få effekt. I och för sig behöver något absolut hinder inte föreligga mot att få fram information på andra vägar. Det krävs dock att hindret är sådant att det inte skäligen kan begäras att man ska avstå från teleavlyssning. Kan personlig övervakning (skuggning) eller andra åtgärder användas som alternativ, bör det ändå vara tillåtet med teleavlyssning, om alternativen skulle kräva en orimligt hög personalinsats eller vara förenade med avsevärd risk att den pågående utredningen avslöjas för tidigt. Utgångspunkten bör dock vara att i första hand pröva andra metoder.

Begreppet synnerlig vikt innebär alltså i detta sammanhang att situationen ska göra infiltrationsoperationen nödvändig. Nödvändiga uppgifter ska i princip inte kunna inhämtas med andra medel och det ska finnas skäl att räkna med att infiltrationsoperationen verk-

ligen kan leda till att man erhåller information av central betydelse för utredningen.

Utöver kravet på synnerlig vikt uppställs i paragrafen även ett krav på att skälen för att utföra en straffbelagd gärning uppenbart uppväger det men som gärningen kan innebära för allmänna eller enskilda intressen. Detta led, som kan sägas innebära att en kvalificerad proportionalitetsprövning ska göras, innebär att det, för att tillstånd ska kunna ges, inte ska råda någon egentlig tvekan om att skälen för att utföra gärningen är starkare än relevanta motstående intressen. Bestämmelsen syftar i denna del till att tillse att tillstånd att begå annars brottsliga gärningar ges bara när den bakomliggande intressekonflikten klart utfaller till straffrättens nackdel och signalerar alltså att en inte obetydlig restriktivitet ska upprätthållas.

I det nu diskuterade kravet ligger inte bara en intresseavvägning utan också ett krav på att själva åtgärden, dvs. i det här fallet förövandet av de annars brottsliga gärningarna, är nödvändig, dvs. att man inte kan uppnå syftet med åtgärden på annat sätt (jfr t.ex. Fitger, kommentaren till 24 kap. 1 § tredje stycket RB). Detta krav kommer också direkt till uttryck i 1 § första stycket.

Förundersökning

3 §

I förundersökning prövas frågor om tillstånd till utförande av straffbelagda gärningar av rätten på ansökan av åklagaren.

Paragrafen, som har behandlats ovan i avsnitt 6.4.6, anger hur en fråga om tillstånd att begå annars brottsliga gärningar inom ramen för en förundersökning ska prövas. Enligt bestämmelsen prövas frågor om utförande av en annars straffbelagd gärning av rätten på ansökan av åklagare i egenskap av förundersökningsledare.

Underrättelseverksamhet

4 §

I en undersökning för att förebygga, förhindra eller upptäcka brottslig verksamhet prövas frågor om tillstånd till utförande av straffbelagda gärningar av Nämnden på ansökan av polismyndigheten.

I bestämmelsen anges hur en fråga om tillstånd att begå annars brottsliga gärningar inom ramen för underrättelseverksamhet ska prövas. Enligt bestämmelsen prövas frågor om utförande av en annars brottslig gärning av Nämnden på ansökan av polismyndigheten.

Gemensamma bestämmelser

5 §

> Ett tillstånd ska innehålla uppgifter om vilken infiltrationsoperation tillståndet avser, under vilken tid tillståndet ska gälla och vilka gärningar som tillståndet avser. Ett tillstånd ska vidare förenas med de villkor som behövs för att tillgodose att enskildas personliga integritet eller allmänna eller enskilda intressen i övrigt inte i onödan kränks.
>
> Tiden för ett tillstånd får inte bestämmas längre än nödvändigt och inte heller överstiga tre månader från dagen för beslutet.

I bestämmelsen, som har behandlats ovan i avsnitt 6.4.7, anges vad ett tillstånd ska innehålla, vilket naturligtvis också får betydelse för hur en ansökan bör utformas.

Ett tillstånd ska för det första innehålla grundläggande uppgifter om vilken infiltrationsoperation tillståndet avser samt under vilken tid tillståndet gäller. Enligt andra stycket får tiden för ett tillstånd inte bestämmas längre än nödvändigt och det får heller inte överstiga tre månader från dagen för beslutet.

Vidare ska tillståndet innehålla uppgift om vilka gärningar tillståndet avser. Gärningarna, eller de grupper av gärningar det kan bli fråga om, ska preciseras så långt det i den aktuella situationen är möjligt och det bör normalt krävas att gärningarna preciseras genom angivande av författning samt vilka kapitel, eller om det rör sig om enstaka gärningar, vilka lagrum som kan överträdas.

Vilken precision som är nödvändig för att möjliggöra en prövning torde kunna variera något beroende på vilken typ av gärning det är fråga om. Om en ansökan t.ex. avser tillstånd att begå en gärning som innefattar ett konkret intrång i enskilds intresse (t.ex. ett hemfridsbrott) torde i regel större precision krävas än om ansökan avser en gärning som endast innefattar ett abstrakt faremoment (t.ex. en överträdelse av föreskrifter på livsmedelsområdet). Likaså torde viss precision krävas för att det ska vara möjligt att bedöma om en gärning innefattar sådan medverkan i mindre mån som avses i 23 kap. 5 § BrB.

6 §

> Om det inte längre finns skäl för utförandet av en straffbelagd gärning ska beslutet omedelbart hävas. Har beslutet fattats av rätten får det hävas även av åklagaren. Har beslutet fattats av Nämnden får det hävas även av polismyndigheten.

Paragrafen innebär att ett beslut om att tillåta utförandet av en straffbelagd gärning ska hävas när det inte längre finns skäl för beslutet. Beslutet ska kunna hävas av såväl av den ansökande som den beslutande myndigheten.

I situationen där ett tillstånd meddelats i underrättelseverksamhet men operationen övergår till förundersökning ska åklagaren omedelbart informeras om att infiltrationsoperationen pågår samt om det beslut om rätt att begå annars brottsliga gärningar som finns. I en sådan situation har åklagaren en rätt och skyldighet att häva ett beslut som inte längre bör gälla. Om infiltrationsoperationen i en sådan situation delvis ska fortsätta inom underrättelseverksamheten avser åklagarens hävningsbeslut endast den del av operationen som ryms inom förundersökningen.

7 §

> En gärning som vidtas inom ramen för en sådan infiltrationsoperation för vilken ett tillstånd enligt 1 § har meddelats, utgör inte brott under förutsättning att gärningen
>
> 1. är direkt jämförbar med någon av de gärningar som avses i tillståndet, och
> 2. uppfyller de allmänna krav som följer av 1 och 2 §§.

Bestämmelsen som har behandlats ovan i avsnitt 6.4.9 innebär att den ansvarsfrihet som tillkommer en gärning som omfattas av ett tillstånd utsträcks till att gälla också gärningar som är direkt jämförbara med de som avses i tillståndet. I sak betyder detta att de gärningar som anges i ett tillstånd kommer att ges en normerande karaktär och fungera som ett slags måttstock för vad som inom ramen för en viss operation kommer att vara tillåtet att göra.

För att en gärning ska vara tillåten förutsätts att den är jämförbar med en gärning som avses i tillståndsbeslutet, dvs. att gärningen framstår som utbytbar med de som avses i tillståndet, samt att den uppfyller de allmänna förutsättningar som gäller för meddelande av tillstånd enligt 1 och 2 §§ i detta kapitel. Detta betyder

att också de krav som följer av 2 § och som normalt bedöms av beslutsmyndigheten vid meddelandet av ett tillstånd ska vara uppfyllda för att ansvarsfrihet ska kunna medges.

Vid bedömning av om en gärning kan anses vara jämförbar med en som avses i tillståndet ska hänsyn tas till gärningens straffvärde, till vilka skyddsintressen som träds för när men också till gärningens karaktär.

Jämförbarhet bör sålunda kunna anses föreligga om gärningarna är straffvärdemässigt likvärdiga och skyddsintressena bakom de överträdda bestämmelserna är likartade, t.ex. om tillståndet avser brott mot livsmedelslagstiftningen och polismannen senare blir tvungen att begå brott mot annan lagstiftning av administrativ karaktär.

Jämförbarhet bör emellertid också kunna föreligga när gärningen till sin karaktär är jämförbar med den som avses i tillståndet. Om tillstånd t.ex. har getts att delta vid förflyttning och förvaring av narkotika och det senare visar sig att transporten inte innehåller narkotika utan stöldgods bör medverkan till häleri anses vara en gärning jämförbar med medverkan till narkotikabrott. För att gärningar av olika slag ska kunna anses jämförbara på detta sätt bör normalt förutsättas att skillnaden i straffvärde inte är betydande.

Som framgår av bestämmelsen fordras i tillägg att gärningen uppfyller de krav som följer av 1 och 2 §§. Detta innebär att ansvarsfrihet förutsätter att gärningen är sådan att tillstånd skulle ha beviljats om gärningen funnits med i den ursprungliga tillståndsansökan. Om tillstånd har sökts men till viss del inte beviljats kan bestämmelsen alltså inte tillämpas i förhållande till de gärningar för vilka tillstånd inte beviljats.

8 §

> Vad som i detta kapitel föreskrivs om utförande av en straffbelagd gärning ska tillämpas även på en gärning som kan föranleda sanktionsavgift.

Bestämmelsen har behandlats ovan i avsnitt 6.4.4. Enligt bestämmelsen ska reglerna i kapitlet tillämpas också på en gärning som kan föranleda sanktionsavgift. Detta innebär att ett tillstånd inte bara kan avse gärningar som är straffbelagda, utan också sådana som endast – eller vid sidan av den straffrättsliga sanktionen – kan föranleda påförande av sådana administrativa avgifter med bestraffande karaktär som numera går under benämningen sanktionsavgifter.

7 kap. Biträde av enskilda

1 §

> Vid åtgärder enligt 2 eller 4 kap. får polisen, om det finns särskilda skäl, ta biträde av enskilda. Detsamma gäller vid infiltrationsverksamhet och andra provokativa åtgärder än de som avses i 5 kap.

Bestämmelsen motsvarar den för närvarande oreglerade möjlighet som redan finns för polisen att ta biträde av enskilda personer. Den omfattar både åtgärder under förundersökning och i underrättelseverksamhet.

Med enskilda personer avses sådana personer som inte är anställda vid någon av de brottsbekämpande myndigheterna, dvs. i vardagligt tal privatpersoner.

Som framgått ovan tar regleringen sikte på situationer när polisen vid genomförande av en åtgärd tar biträde av en enskild. Den träffar följaktligen inte situationer där den enskilde själv beslutar att vidta åtgärden. Bedömningen av om det är fråga om en biträdessituation eller en situation där den enskilde agerar självständigt måste göras mot bakgrund av omständigheterna i det enskilda fallet. I linje med vad som sagts ovan bör emellertid enbart den omständigheten att polisen tillhandahåller viss teknisk utrustning i sig inte vara tillräckligt för att anse att det är polisen som genomför åtgärden.

Det krav på särskilda skäl som uppställs motsvaras av de förutsättningar för anlitande av enskilda personer som framgår av praxis och har tydliggjorts genom bl.a. uttalanden inom ramen för i JO:s och JK:s tillsynsverksamhet. Detta innebär att det för att särskilda skäl ska föreligga så måste anlitandet av enskilda ske med stor försiktighet och endast i undantagsfall. Vidare krävs för att särskilda skäl ska anses föreligga att det finns anledning att anta att en polis inte skulle ha kunnat användas för uppdraget.

Bestämmelsen har motiverats i avsnitt 8.3.1.

2 §

> Vad som föreskrivs i 2 kap. 2 § om företrädare för myndigheten ska, när en enskild lämnar biträde enligt 1 §, i stället gälla den enskilde.

Paragrafen innebär att det – när en enskild lämnar biträde vid dold eller vilseledande upptagning av ljud t.ex. genom att bära en kroppsburen mikrofon – är tillräckligt för att ljudupptagning ska få ske att

den enskilde deltar i det samtal, sammanträde eller sammankomst som är föremål för ljudupptagningen i stället för en företrädare för myndigheten.

3 §

Vid åtgärder enligt 5 eller 6 kap. samt 9 kap. 1 § får polisen, om det finns synnerliga skäl, ta biträde av enskilda. Sådant biträde får endast avse åtgärder som syftar till att en polisman ska kunna genomföra de åtgärder som avses i tillståndet.

Bestämmelsen ger befogenhet för polisen att ta biträde av enskilda vid åtgärder enligt lagförslagets 5 och 6 kap., dvs. särskilda provokativa åtgärder och annars brottsliga gärningar. Den omfattar även Säkerhetspolisens användning av särskilda provokativa åtgärder i underrättelseverksamheten enligt 9 kap. 1 §. Bestämmelsen har motiverats i avsnitt 8.3.3.

I bestämmelsen uppställs ett krav på synnerliga skäl för att polisen ska få ta biträde av enskilda. Detta krav medför att anlitandet av privatpersoner ges stränga restriktioner och hänger samman med den komplexitet som omger frågorna kring särskilda provokativa åtgärder och möjligheten att utföra annars brottsliga gärningar. Synnerliga skäl enligt bestämmelsen kan föreligga t.ex. om en polisman behöver biträde för att komma in i en sluten kriminell sammanslutning, där det kan vara i princip omöjligt att komma in för den som saknar en viss etnisk härkomst eller en omvittnat kriminell bakgrund.

Att det ska handla om att biträda polisen innebär att den enskilde inte själv ska agera som provokatör eller delta i brottslig verksamhet. Syftet med biträdet ska i stället normalt vara att introducera en polisman och på sådant sätt möjliggöra för polismannen att utföra de särskilda provokativa åtgärderna enlig lagförslagets 5 kap. eller de annars brottsliga gärningarna enligt lagförslagets 6 kap.

För Säkerhetspolisen gäller dock vissa särskilda förutsättningar enligt 9 kap. 5 §.

4 §

Frågor om biträde av enskilda prövas av den beslutsinstans eller beslutsfattare som enligt 2, 4–6 eller 9 kap. har att besluta om åtgärden.

Av bestämmelsen framgår att det är den beslutsinstans eller beslutsfattare, t.ex. förundersökningsledare eller domstol, som har att besluta om åtgärden i sig som även prövar frågor om biträde av enskilda i anslutning till åtgärden.

8 kap. Nedläggning av förundersökning

1 §

Förundersökning får läggas ned om det finns anledning att anta att det genom förundersökningens fortsatta bedrivande eller genom lagföring av brottet skulle uppstå en påtaglig risk för att avslöja, eller på annat sätt äventyra syftet med, en infiltrationsoperation. Om brottet kan antas medföra strängare straff än böter krävs dock att det är uppenbart att

1. brottet avser sådan gärning som, om den bedöms enligt regleringen om medverkan till brott, skulle utgöra medverkan i mindre mån enligt 23 kap. 5 § brottsbalken, eller
2. brottet har ett avsevärt lägre straffvärde än det brott eller den brottsliga verksamhet som infiltrationsoperationen riktar sig mot.

Om förutsättningar för att lägga ned en förundersökning enligt första stycket föreligger redan innan en sådan har inletts, får det beslutas att förundersökning inte ska inledas.

Beslut enligt denna bestämmelse meddelas av åklagaren. Beslut får meddelas endast under förutsättning att något väsentligt allmänt eller enskilt intresse inte åsidosätts.

Bestämmelsen har behandlats i avsnitt 9.5.

I bestämmelsens första stycke införs en möjlighet att lägga ned en förundersökning, om det behövs för att inte avslöja en infiltrationsoperation. För att denna möjlighet ska kunna användas krävs att det genom förundersökningsarbetet eller lagföringen skulle uppstå en påtaglig risk för att avslöja eller på annat sätt äventyra syftet med en infiltrationsoperation. I samband med att fråga om att lägga ned en förundersökning uppkommer, måste en bedömning göras av den aktuella brottslighetens straffvärde i förhållande till straffvärdet för den brottslighet som infiltrationsoperationen tar sikte på. Möjligheten att lägga ned en förundersökning kommer främst att komma till användning vid förundersökningar rörande bötes-

brottslighet. Det ges dock även vissa möjligheter att lägga ned en förundersökning även om strängare straff kan bli aktuellt. Det rör sig om två typsituationer, dels om brottet avser sådan gärning som, om den bedöms enligt regleringen om medverkan till brott, skulle utgöra medverkan i mindre mån enligt 23 kap. 5 § BrB, dels när förundersökningen rör ett brott med ett avsevärt lägre straffvärde än det brott eller den brottsliga verksamhet som infiltrationsoperationen riktar sig mot

Av andra stycket framgår att beslut får fattas om att en förundersökning inte ska inledas om det finns förutsättningar för att lägga ned en förundersökning enligt första stycket föreligger redan innan en sådan har inletts. Stycket motsvarar vad som gäller vid nedläggning av förundersökning enligt 23 kap. 4 § RB.

I tredje stycket anges att det är åklagare som beslutar att lägga ned eller inte inleda förundersökning i dessa fall. Av 10 § åklagarförordningen framgår att det i vissa fall endast är vissa åklagare i chefsställning som får besluta om att lägga ned eller inte inleda en förundersökning. Denna begränsning, som Utredningen om förundersökningsbegränsning har föreslagit ska avskaffas (se SOU 2010:43), är inte tillämplig i förevarande fall. Beslut att lägga ned eller inte inleda en förundersökning kan alltså fattas av alla åklagare.

Av tredje stycket följer vidare den grundläggande förutsättningen för beslut om att lägga ned eller inte inleda förundersökning är att något väsentligt allmänt eller enskilt intresse inte åsidosätts genom beslutet. En motsvarande bestämmelse finns avseende åtalsunderlåtelse i 20 kap. 7 § RB. Begreppen allmänt intresse och enskilt intresse är svårdefinierade och får prövas från fall till fall. I förarbetena har angetts olika exempel på vad som kan falla under begreppen, se vidare betänkandet Förundersökningsbegränsning (SOU 2010:43) s. 38 ff. med där gjorda hänvisningar.

9 kap. Särskilda bestämmelser för Säkerhetspolisen

Särskilda provokativa åtgärder i underrättelseverksamhet

1 §

Säkerhetspolisen får, utöver vad som framgår av 5 kap. 1 §, vidta åtgärder som kan förmå en person som omfattas av en undersökning för att förebygga, förhindra eller upptäcka allvarlig brottslighet, att begå en brottslig gärning. Åtgärderna får vidtas endast om det behövs för

att få fram uppgifter som det finns särskild anledning att anta kan bidra till att förebygga, förhindra eller upptäcka den allvarliga brottsliga verksamheten.

Åtgärderna får vidtas endast om det är av synnerlig vikt för undersökningen.

Bestämmelsen innebär att Säkerhetspolisen ges rätt att vidta provokativa åtgärder inom ramen för sin underrättelseverksamhet.

Den yttre ramen för bestämmelsens tillämplighet blir det uppdrag som Säkerhetspolisen har enligt förordningen (2002:1050) med instruktion för Säkerhetspolisen samt att det krävs att åtgärden behövs för att få fram uppgifter som det finns särskild anledning att anta kan bidra till att förebygga, förhindra eller upptäcka allvarlig brottslig verksamhet. Åtgärderna får alltså inte vidtas i andra delar av Säkerhetspolisens verksamhet än sådan som syftar till att förebygga, förhindra eller upptäcka allvarlig brottslighet. Beträffande innebörden av kravet på allvarlig brottslighet, se kommentaren till 5 kap. 1 §.

Den personkrets som kan utsättas för en provokation avgränsas genom att åtgärden måste rikta sig mot en person som omfattas av undersökningen, dvs. ärendet i underrättelseverksamheten. Personkretsen begränsas vidare genom att det framgår att åtgärderna endast får vidtas om det behövs för att få fram uppgifter som det finns särskild anledning att anta kan bidra till att förebygga, förhindra eller upptäcka allvarlig brottslig verksamhet.

Av andra stycket framgår den ytterligare begränsningen att åtgärderna får vidtas endast om det är av synnerlig vikt för undersökningen. Beträffande innebörden av kravet på synnerlig vikt, se kommentaren till 5 kap. 1 §.

2 §

Frågor om tillstånd till särskilda provokativa åtgärder i underrättelseverksamhet prövas av Nämnden efter ansökan av Säkerhetspolisen.

Bestämmelsen har behandlats ovan i avsnitt 5.3.5 och innebär att frågor om provokativa åtgärder i Säkerhetspolisens underrättelseverksamhet ska prövas av Nämnden på ansökan av Säkerhetspolisen.

3 §

Om det inte längre finns skäl för de provokativa åtgärderna ska beslutet omedelbart hävas.

Bestämmelsen har samma innebörd som 5 kap. 3 §. I detta fall är det Nämnden eller Säkerhetspolisen som ska häva beslut som det inte längre finns skäl för.

4 §

Bestämmelsen i 5 kap. 4 § ska tillämpas också på åtgärder enligt 1 §.

Bestämmelsen har behandlats ovan i avsnitt 5.3.8. Dess innebörd är att bestämmelsen i 5 kap. 4 § (straffrihetsregeln) ska tillämpas också på provokativa åtgärder enligt detta kapitel.

Biträde av enskilda

5 §

Säkerhetspolisen får i fall som avses i 7 kap. 3 §, om det finns synnerliga skäl, ta biträde av enskilda även avseende andra åtgärder än sådana som syftar till att en polisman ska kunna genomföra de åtgärder som avses i tillståndet.

Bestämmelsen innehåller en utvidgning av möjligheterna för Säkerhetspolisen att ta biträde av enskilda i förhållande till vad som föreskrivs i 7 kap. 3 §. Åtgärderna kan gälla sådana provokativa åtgärder som regleras i 5 kap. eller 9 kap. 1 §, eller annars brottsliga gärningar enligt 6 kap. Utvidgningen innebär att enskilda kan lämna biträde även vid andra åtgärder än sådana som syftar till att en polisman ska kunna genomföra en provokativ åtgärd eller annars brottslig gärning. En enskild person kan således i dessa situationer lämna Säkerhetspolisen biträde i större omfattning än vad som gäller för övriga brottsbekämpande myndigheter.

10 kap. Dokumentation och granskning

1 §

Åtgärder enligt denna lag ska dokumenteras. Av dokumentationen ska framgå

1. vem som har fattat beslutet om åtgärden,
2. grunden för beslutet och tidpunkten när det har fattats,
3. vem eller vilka som har deltagit i åtgärden,
4. vem eller vilka som åtgärden har riktat sig mot,
5. tiden för åtgärden, samt
6. vad som i övrigt har förekommit vid åtgärden.

Bestämmelsen innehåller föreskrifter om dokumentation av åtgärder enligt denna lag och uppräkningen motsvarar i sak vad som enligt 27 § polislagen gäller för dokumentation vid omhändertaganden, husrannsakan m.m. som vidtas i enlighet med den lagen.

2 §

En upptagning eller uppteckning som har gjorts vid en åtgärd enligt denna lag ska granskas snarast möjligt.

Upptagningar eller uppteckningar ska, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna och uppteckningarna är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet ska de bevaras så länge det behövs för detta ändamål. De ska därefter förstöras.

Trots vad som sägs i andra stycket får uppgifter från upptagningar och uppteckningar behandlas i enlighet med vad som är särskilt föreskrivet i lag.

Paragrafen innehåller bestämmelser om hur upptagningar eller uppteckningar från åtgärder enligt denna lag ska hanteras. Begreppet ”uppteckning” får även anses omfatta t.ex. sådana anteckningar som en polisman upprättar efter att under en infiltrationsoperation ha varit inne i någons bostad.

En upptagning eller uppteckning ska enligt första stycket granskas så snart det är möjligt.

Enligt andra stycket första meningen ska de delar av upptagningar eller uppteckningar som är av betydelse för utredningen av brott bevaras till dess förundersökningen avseende brottet har lagts ned eller avslutats eller, om åtal väckts, målet avgjorts slutligt. Om det kommer fram uppgifter om brott som redan är föremål för en

förundersökning, ska uppgifterna bevaras på samma sätt som gäller för uppgifter i den förundersökning som föranlett åtgärden. Om upptagningarna eller uppteckningarna är av betydelse för att i underrättelseverksamheten förebygga, förhindra eller upptäcka brottslig verksamhet ska de bevaras så länge de behövs för det ändamålet.

När upptagningarna och uppteckningarna inte längre ska bevaras, ska de förstöras.

11 kap. Överklagande m.m.

Gemensamma bestämmelser

1 §

Beslut enligt denna lag får verkställas omedelbart.

Av bestämmelsen framgår att beslut enligt denna lag får verkställas omedelbart. Detta gäller oberoende av vilken instans som fattat beslutet.

Förundersökning

2 §

Har i förundersökning beslut om åtgärd enligt denna lag fattats av annan än rätten ska beslutet prövas av rätten, om den som är föremål för åtgärden begär det. Begäran om sådan prövning ska göras skriftligen eller muntligen hos åklagaren eller undersökningsledaren. Åklagaren eller undersökningsledaren ska utan dröjsmål överlämna ärendet till rätten.

Bestämmelsen reglerar möjligheten att begära rättens prövning av beslut om åtgärder enligt denna lag. Möjligheten att begära rättens prövning gäller beslut som fattats i en förundersökning. För beslut som fattats i underrättelseverksamheten gäller vad som föreslås i 5 §. Den som är föremål för en åtgärd kan begära att beslutet upphävs eller ändras, t.ex. genom att förses med inskränkande föreskrifter. En begäran om prövning av ett beslut ska göras hos åklagaren om det är åklagaren som fattat beslutet eller annars hos undersökningsledaren. Begäran kan vara skriftlig eller muntlig. Vid en muntlig begäran ska åklagaren respektive undersökningsledaren anteckna behövliga uppgifter om begäran. Det ankommer sedan på åklagaren

respektive undersökningsledaren att överlämna ärendet till rätt domstol. Någon tidsgräns för begäran om rättens prövning har inte angetts.

3 §

I fråga om överklagande av rättens beslut enligt denna lag tillämpas bestämmelserna i rättegångsbalken om överklagande av rättens beslut i brottmål i fråga om en åtgärd som avses i 25–28 kap. samma balk.

Bestämmelsen anger vad som gäller för överklagande av rättens beslut och överensstämmer med vad som föreskrivs i 14 § andra stycket lagen om hemlig rumsavlyssning.

Enligt bestämmelsen får rättens beslut om åtgärder enligt denna lag överklagas på samma sätt som gäller för tvångsmedel i 25–28 kap. RB. Det innebär att rättens beslut om tillstånd överklagas särskilt (49 kap. 5 § 6 RB). Om rätten under förundersökningen avslår en begäran om tillstånd, anses beslutet vara slutligt och kan då överklagas enligt 49 kap. 3 § första stycket RB. Om ett beslut om en åtgärd enligt denna lag förenas med inskränkande föreskrifter kan även dessa överklagas. Av 52 kap. 7 § tredje stycket RB framgår att hovrätten kan inhibera verkställigheten vid ett överklagande.

4 §

Den som i förundersökning har varit utsatt för en åtgärd enligt 2 kap. 5 § ska underrättas som åtgärden.

I fråga om sådan underrättelse, tidpunkten för underrättelsen och undantag från underrättelseskyldigheten tillämpas 27 kap. 31 § andra och tredje styckena, 32 och 33 §§ rättegångsbalken. Underrättelsen ska även innehålla uppgift om platsen för åtgärden.

Bestämmelsen motsvarar vad som i 27 kap. 31 § RB föreskrivs om underrättelseskyldighet vid hemlig teleavlyssning och hemlig teleövervakning.

I första stycket föreskrivs att den som inom ramen för en förundersökning har varit utsatt för sådan särskilt ingripande åtgärd enligt 2 kap. 5 § som avser ljudupptagning av samtal, bildupptagning av hem eller korrespondens, eller lokalisering av person ska underrättas om åtgärden. Skyldigheten att underrätta den som utsatts för åtgärden gäller även när denne är en juridisk person. För

motsvarande åtgärder som vidtas i underrättelseverksamheten finns ingen motsvarande underrättelseskyldighet, se vidare avsnitt 12.4.

På motsvarande sätt som enligt 15 § lagen om hemlig rumsavlyssning ska, enligt andra stycket, regleringen i rättegångsbalken tillämpas när det gäller fråga om den närmare regleringen av underrättelsen, tidpunkten för underrättelsen och undantag från underrättelseskyldighet.

Underrättelseverksamhet

5 §

> Har i underrättelseverksamhet beslut om åtgärd enligt denna lag fattats av annan än Nämnden ska beslutet prövas av Nämnden, om den som är föremål för åtgärden begär det. Begäran om sådan prövning ska göras skriftligen eller muntligen hos polismyndigheten. Polismyndigheten ska utan dröjsmål överlämna ärendet till Nämnden.
>
> Nämndens beslut får inte överklagas.

Paragrafen innehåller i första stycket bestämmelser om möjligheten att begära Nämndens prövning av beslut om åtgärder enligt denna lag. Möjligheten att begära Nämndens prövning gäller beslut som fattats i underrättelseverksamheten. För beslut som fattats i förundersökning gäller vad som föreslås i 2 §. Den som är föremål för en åtgärd kan begära att beslutet upphävs eller ändras, t.ex. genom att förses med inskränkande föreskrifter. En begäran om prövning av ett beslut ska göras hos polismyndigheten. Begäran kan vara skriftlig eller muntlig. Vid en muntlig begäran ska polisen anteckna behövliga uppgifter om begäran. Det ankommer sedan på polismyndigheten att överlämna ärendet till Nämnden. Någon tidsgräns för en begäran om Nämndens prövning har inte angetts.

En begäran om Nämndens prövning ska kunna avse både frågan om polisen hade befogenhet att fatta ett visst beslut och en prövning av beslutets innehåll.

Av andra stycket framgår att Nämndens beslut enligt denna lag inte får överklagas.

12 kap. Tillsyn

1 §

I lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet finns bestämmelser om Säkerhets- och integritetsskyddsnämndens tillsyn på eget initiativ och på begäran av enskild.

Paragrafen innehåller en erinran om att Säkerhets- och integritetsskyddsnämnden har tillsyn över de brottsbekämpande myndigheternas verksamhet.

Den tillsyn som Säkerhets- och integritetsskyddsnämnden ska utöva omfattar de brottsbekämpande myndigheternas användning av metoderna ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person, identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, eller störning av kommunikation med sådan utrustning, annars brottsliga gärningar samt särskilda provokativa åtgärder. Tillsynen omfattar inte åklagares beslut att lägga ned eller inte inleda förundersökning med stöd av inhämtningslagens 8 kap., se avsnitt 12.5.

13 kap. Tillämplighet för andra brottsbekämpande myndigheter

1 §

Följande bestämmelser gäller även i brottsbekämpande verksamhet hos Tullverket.

1. Ljudupptagning av samtal, bildupptagning av hem eller korrespondens samt lokalisering av person (2 kap. 2–5 §§)
2. Identifiering eller störning av mobil elektronisk kommunikationsutrustning m.m. (3 kap 2–4 §§)
3. Installation av lokaliseringsutrustning (4 kap. 7 §)
4. Särskilda provokativa åtgärder (5 kap. 1 §)
5. Biträde av enskilda (7 kap. 1 och 3 §§)

Vad som i denna lag är föreskrivet om polismyndighet eller polisman ska vid utövande av befogenhet enligt första stycket även gälla Tullverket respektive tjänsteman vid Tullverket.

Paragrafen innehåller i första stycket en förteckning över vilka åtgärder enligt den föreslagna lagen som kan vidtas av Tullverket i myndighetens brottsbekämpande verksamhet. Det rör sig om åtgärder enligt 2 kap. (ljudupptagning av samtal m.m.), identifiering eller

störning av mobil kommunikationsutrustning m.m. enligt 3 kap., åtgärder enligt 4 kap. 7 § (installation av lokaliseringsutrustning) samt särskilda provokativa åtgärder enligt 5 kap. Vidare framgår att Tullverket även får ta biträde av enskilda enligt 7 kap. för de åtgärder som faller inom myndighetens befogenheter.

Av andra stycket framgår att det vid tillämpningen av befogenheter enligt första stycket ska gälla motsvarande för Tullverket som gäller för polismyndighet. Vidare framgår att det gäller motsvarande för tjänsteman vid Tullverket som för polisman.

2 §

Följande bestämmelser gäller även i brottsbekämpande verksamhet hos Kustbevakningen.

1. Bildupptagning av hem eller korrespondens samt lokalisering av person (2 kap. 3–5 §§)
2. Installation av lokaliseringsutrustning (4 kap. 7 §)
3. Biträde av enskilda (7 kap. 1 §)

Vad som i denna lag är föreskrivet om polismyndighet eller polisman ska vid utövande av befogenhet enligt första stycket även gälla Kustbevakningen respektive tjänsteman vid Kustbevakningen.

Paragrafen innehåller i första stycket en förteckning över vilka åtgärder enligt den föreslagna lagen som kan vidtas av Kustbevakningen i myndighetens brottsbekämpande verksamhet. Det rör sig om bildupptagning och lokalisering av person enligt 2 kap. 3–5 § samt åtgärder vid installation av lokaliseringsutrustning enligt 4 kap. 7 §. Vidare framgår att Kustbevakningen även får ta biträde av enskilda enligt 7 kap. för de åtgärder som faller inom myndighetens befogenheter.

Av andra stycket framgår att det vid tillämpningen av befogenheter enligt första stycket ska gälla motsvarande för Kustbevakningen som gäller för polismyndighet. Vidare framgår att det gäller motsvarande för tjänsteman vid Kustbevakningen som för polisman.

3 §

Bestämmelserna om bildupptagning av hem eller korrespondens i 2 kap. 3 och 5 §§ gäller även i brottsbekämpande verksamhet hos Skatteverket.

Vad som i denna lag är föreskrivet om polismyndighet eller polisman ska vid utövande av befogenhet enligt första stycket även gälla Skatteverket respektive tjänsteman vid Skatteverket.

Paragrafen innehåller i första stycket en förteckning över vilka åtgärder enligt den föreslagna lagen som kan vidtas av Skatteverket i myndighetens brottsbekämpande verksamhet. Befogenheten som ges avser åtgärder för bildupptagning av hem eller korrespondens enligt 2 kap. 3 § och sådan bildupptagning enligt 2 kap. 5 § som anses vara särskilt ingripande.

Av andra stycket framgår att det vid tillämpningen av befogenheter enligt första stycket ska gälla motsvarande för Skatteverket som gäller för polismyndighet. Vidare framgår att det gäller motsvarande för tjänsteman vid Skatteverket som för polisman.

15.2 Förslaget till lag om ändring i rättegångsbalken

27 kap. 11 §

> Om den från vilken beslag sker inte är närvarande vid beslaget, *ska* han *eller hon så snart det kan ske utan men för utredningen* underrättas om det och om vad som har skett med det beslagtagna. *Har* en försändelse hos ett befordringsföretag tagits i beslag, *ska underrättelsen lämnas till mottagaren och även till avsändaren, om denne är känd*.

Paragrafen överensstämmer med förslaget i BRU:s betänkande Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74). Den reglerar underrättelseskyldigheten för de brottsutredande myndigheterna sedan föremål har tagits i beslag. Även i fortsättningen ska mottagaren och en känd avsändare underrättas om åtgärden så snart det kan ske utan men för utredningen. Genom den föreslagna ändringen av bestämmelsen ska underrättelse lämnas vid den tidpunkten även i andra fall. Om den från vilken beslag sker inte är närvarande vid beslaget ska han, så snart det kan ske utan men för utredningen, underrättas om åtgärden. Tidigare fanns ingen möjlighet att ta hänsyn till kollusionsfaran, dvs. risken för att det uppkommer men för utredningen, eftersom underrättelsen skulle lämnas utan dröjsmål. Någon ändring i sak har inte skett för det fallet att en försändelse hos ett befordringsföretag har tagits i beslag. Frågan om underrättelseskyldighet vid beslag har behandlats i avsnitt 7.3.3.

15.3 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. *Nämnden ska också utöva tillsyn över brottsbekämpande myndigheters användning av åtgärder enligt 2–7 och 9 kap. lagen (0000:00) om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet.*

Nämnden ska även utöva tillsyn över polisens behandling av personuppgifter enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister. Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § polisdatalagen och 12 § lagen om polisens allmänna spaningsregister.

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Genom ett tillägg i paragrafens första stycke införs en ny mening som reglerar omfattningen av den tillsyn Säkerhets- och integritetsskyddsnämnden ska utöva vad gäller inhämtningsåtgärder enligt den föreslagna lagen.

Den tillsyn som Säkerhets- och integritetsskyddsnämnden således ska utöva omfattar de brottsbekämpande myndigheternas användning av metoderna ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person, identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, eller störning av kommunikation med sådan utrustning, annars brottsliga gärningar samt särskilda provokativa åtgärder. Tillsynen omfattar inte åklagares beslut att lägga ned eller inte inleda förundersökning med stöd av inhämtningslagens 8 kap.

Tillsynen får bedrivas på samma sätt som Säkerhets- och integritetsskyddsnämndens tillsyn för närvarande bedrivs när det gäller användande av hemliga tvångsmedel och kvalificerade skyddsidentiteter. Det innebär bl.a. att domstolarnas handläggning av och beslut i ärenden om tillstånd till åtgärder enligt inhämtningslagen inte omfattas av nämndens tillsyn.

15.4 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap. 19 §

Den tystnadsplikt som följer av 5–13 §§ inskränker rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare. *Detsamma gäller för uppgift om ljud- eller bildupptagning, lokalisering av person, identifiering eller störning av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, tillträde till vissa utrymmen, särskilda provokativa åtgärder, annars brottsliga gärningar och biträde av enskilda enligt lagen (0000:000) om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver vad som anges i andra stycket följer av 7 kap. 3 § första stycket 1, 4 § 1–8 och 5 § 3 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 1 yttrandefrihetsgrundlagen.

I paragrafen regleras vilka tystnadsplikter som har företräde framför principen om meddelarfrihet.

Genom ett tillägg i paragrafens andra stycke klargörs att rätten att meddela och offentliggöra uppgifter rörande vissa inhämtningsåtgärder enligt den föreslagna lagen inskränks. De åtgärder som avses med den inskränkta rätten att meddela och offentliggöra uppgifter är metoderna ljudupptagning av samtal, bildupptagning av hem eller korrespondens, lokalisering av person, identifiering av mobil elektronisk kommunikationsutrustning eller annan utrustning för radiokommunikation, eller störning av kommunikation med sådan utrustning, tillträde till vissa utrymmen i samband med infiltration eller för att installera lokaliseringsutrustning, särskilda provokativa åtgärder, annars brottsliga gärningar samt biträde av enskilda.

Innebörden av tillägget är att samma inskränkningar i rätten att meddela och offentliggöra uppgifter som redan nu gäller vid användandet av hemliga tvångsmedel ska gälla för de uppräknade metoderna.

15.5 Förslaget till förordning om ändring i förundersökningskungörelsen (1947:948)

13 b §

Målsäganden *ska* tillfrågas om han eller hon vill bli underrättad om beslut om att förundersökning inte *ska* inledas eller att en inledd förundersökning *ska* läggas ned, beslut om att åtal inte *ska* väckas, tidpunkt för huvudförhandling i målet samt dom i målet.

Första stycket ska inte tillämpas om beslut har fattats att förundersökning ska läggas ned eller inte inledas enligt 8 kap. 1 § lagen (0000:00) om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet.

Ändringarna i paragrafens första stycke är redaktionella.

Genom ett nytt andra stycke klargörs att en målsägande inte ska bli tillfrågad om han eller hon vill bli underrättad om vissa beslut i samband med en förundersökning, om beslut har fattats att förundersökning ska läggas ned, eller inte inledas med stöd av 8 kap. 1 § i den föreslagna lagen om särskilda inhämtningsåtgärder. En underrättelse skulle i sådana fall kunna omintetgöra hela infiltrationsoperationen men också kunna medföra en påtaglig fara för inblandade personers liv och hälsa.

15.6 Förslaget till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

14 §

Förbud gäller mot att inneha elektriska eller elektroniska anläggningar som, utan att vara radioanläggningar, är avsedda att sända radiovågor i annat syfte än som avses i 3 kap. 14 § första stycket lagen (2003:389) om elektronisk kommunikation.

Detta förbud gäller inte sådana anläggningar som behövs i verksamhet som bedrivs av *Rikspolisstyrelsen*, *polismyndigheterna*, *Tullverket*, Försvarsmakten, Försvarets radioanstalt eller Försvarets materielverk.

Post- och telestyrelsen får efter ansökan av Kriminalvården besluta att förbudet inte *ska* gälla viss sådan anläggning som behövs i en anstalt eller ett häkte inom kriminalvården för att hindra otillåten mobiltelefonkommunikation, om anläggningen kan användas utan att skadlig störning uppstår utanför anstalten eller häktet.

Genom ett tillägg i andra stycket upptas även Rikspolisstyrelsen, polismyndigheterna och Tullverket bland de myndigheter som är undantagna från förbudet att inneha störsändare.

Ändringen i tredje stycket är enbart språklig.

15.7 Förslaget till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

3 §

Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

Myndigheter	Register
åklagarmyndigheter	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och hemlig rumsavlyssning, diarier över förundersökningar som rör brott mot rikets säkerhet, *samt diarier över förundersökningar där en fråga om att lägga ned eller inte inleda en förundersökning enligt 8 kap. 1 § lag (0000:00) om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet prövats.*

Genom ändringen i paragrafen kommer åklagarmyndigheternas diarier över förundersökningar där en fråga prövats om att lägga ned eller inte inleda en förundersökning enligt 8 kap. 1 § lagen om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet behandlas på samma sätt som tvångsmedelsdiarier.

Särskilt yttrande

av experten Tomas Nilsson

De frågor som utredningen har haft att ta ställning till är utomordentligt centrala vid prövningen av vad som från proportionalitets- och rättssäkerhetssynpunkter är godtagbart i den brottsbekämpande verksamheten.

Såväl regeringsformen som den Europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna, medför krav på en reglering av vissa polisiära metoder. En sådan reglering har visat sig, ur flera aspekter, vara komplicerad när det gäller såväl ändamålsöverväganden som utformningen av lagtext och förarbeten.

Användningen av infiltratörer, informatörer och provokation, liksom av tekniska inhämtningshjälpmedel och tvångsmedelsliknande åtgärder, är förenad med en mängd rättssäkerhetsaspekter. Justitieombudsmannen har i ett granskningsärende 2008-06-25 (diarienummer 1772-2007) redogjort för flera centrala frågeställningar när det gäller särskilt användningen av infiltratörer, informatörer och provokativa åtgärder. Även utredningen har belyst dessa problemställningar.

Om man ska tillåta s.k. okonventionella arbetsmetoder i de brottsbekämpande myndigheternas verksamhet bör utgångspunkten vara – som utredningen också har funnit – de krav som Europakonventionen och regeringsformen uppställer.

Det finns naturligtvis också starka skäl i övrigt att beskriva och reglera vissa integritetskänsliga metoder (jfr ovan nämnda JO-beslut). En genomgående hållning bör därvid vara att detta sker med stor restriktivitet. En sådan inställning är för övrigt bäst förenlig med de allmänna principer som anses böra gälla för tvångsmedelslagstiftning och annan reglering av arbetsmetoder för brottsbekämpning.

Något oundgängligt eller ens starkt behov av en reglering av annat, mera tillåtande, innehåll har heller inte den öppna polisen eller övriga myndigheter förmått beskriva på ett övertygande sätt.

Jag har funnit utredningens förslag i följande avseenden vara av sådant innehåll att de inte framstår som godtagbara vid den avvägning som jag har angivit som utgångspunkt. Jag är naturligtvis medveten om att detta ställningstagande kan, och bör, leda till att färre infiltrationsoperationer kommer att genomföras än vad som blir fallet med utredningsmajoritetens förslag. Det har emellertid sagts från de brottsbekämpande myndigheternas sida att den osäkerhet som under ett antal år har ansetts gälla kring dessa metoder, har lett till en påtaglig återhållsamhet i användningsfrekvensen. Någon allvarligt negativ effekt för beivrandet av brottsligheten, som kan visas bero på denna omständighet, har dock inte beskrivits. Inte heller inhämtade internationella jämförelser föranleder mig till annan bedömning. I vissa hänseenden skulle utredningens förslag gå längre och medge större befogenheter än vad som gäller i jämförbara länder.

Annars brottsliga gärningar samt Nedläggning av förundersökning (6 kap. och 8 kap. i föreslagen lag)

Om polisen ska kunna genomföra framgångsrika infiltrationsoperationer kan ibland krävas att den infiltrerande polismannen begår gärningar som utgör brott eller som kan föranleda sanktionsavgifter. Om detta ska kunna medges utan lagföringskonsekvenser bör emellertid regleringen göras snävare än i förslaget. Införandet av sådana bestämmelser innebär en avgörande förändring i förhållande till vad som för närvarande gäller.

En begränsning bör således ske till, förutom, sanktionsavgifter, gärningar som inte kan antas föranleda annan påföljd än böter. Att också låta gärningar omfattas som – om de bedöms enligt reglerna om medverkan till brott, skulle utgöra medverkan i mindre mån enligt 23 kap. 5 § brottsbalken – är alltför långtgående. Hänvisningen till nämnda bestämmelse i brottsbalken kan mycket lätt medföra betydande tolkningssvårigheter och en alltför vittgående tillämpning. Denna bestämmelse i brottsbalken är, trots att den funnits under mycket lång tid, närapå ständigt föremål för olika uppfattningar från åklagare, försvarare och slutligen även domstolen, i rättegångar där tillämpningen förs på tal.

Bestämmelserna i brottsbalken om handlande i nöd och nödvärn samt bestämmelser i Polislagen ger härutöver tillräckligt utrymme för att bemästra de situationer av aktuellt slag som – liksom hittills – kan uppkomma.

Bestämmelserna om Nedläggning av förundersökning bör korrespondera med regleringen av Annars brottsliga gärningar.

Biträde av enskilda (7 kap. i föreslagen lag)

Vad det här handlar om är inte användande av privatpersoner som informatörer utan om att involvera privatpersoner vid, redan eljest, komplicerade och svårreglerade polismetoder som ljud- och bildupptagning, tillträde till vissa utrymmen, särskilda provokativa åtgärder samt utförande av straffbelagda gärningar.

I utredningen har belysts ett flertal av de olika problem, dilemman och tillämpningssvårigheter som framträder när dessa metoder skall tillämpas. I det tidigare nämnda JO-beslutet (diarienummer 1772-2007) dras slutsatsen att ”ett samarbete med privatpersoner enbart i rena undantagsfall kan vara befogat samt att det under inga omständigheter kan accepteras att polisen har ett organiserat samarbete med privatpersoner i syfte att provocera fram brottsliga handlingar”.

Jag delar denna ståndpunkt och anser att utredningsförslaget inte tillgodoser denna mycket restriktiva inställning till biträde av enskilda personer.

Det bör vidare i detta sammanhang nämnas, förutom den probleminventering som skett, att ytterligare en aspekt är värd att beakta, nämligen de påfrestningar som en privatperson utsätts för när denne utnyttjas som biträde i dessa sammanhang.

Konsekvensen kan bli att den enskilde under mycket lång tid, även efter infiltrationsoperationens slut, undandras från möjligheten att leva ett normalt liv – med familjebildning, arbete, vardagligt umgänge och öppet boende m.m. – på grund av de risker som dessa åtgärder för med sig. Rekryteringen av dessa individer sker dessutom inte sällan när de befinner sig under tillbakaträngda livsomständigheter såsom häktade, efterspanade eller eljest under press från de brottsbekämpande myndigheterna.

Under alla omständigheter råder aldrig något objektivt jämbördigt eller jämställt förhållande mellan den myndighet som anlitar privatpersonen och denne själv. Det humanitära utnyttjandet som

detta innefattar, föreligger typiskt sett inte om enbart polispersonal anlitas för nu aktuella operationer.

Övrigt

Man kan naturligtvis på goda grunder diskutera om Säkerhetspolisen ska ges ett utökat utrymme för provokativa åtgärder och biträde av enskilda, utöver den reglering som eljest föreslagits. Med hänsyn till de särskilda förhållanden som råder för Säkerhetspolisen och då insatsen typiskt sett inte är ägnad att leda till tillvaratagande av bevis som senare framläggs i en rättegång mot en person, kan ett vidgat utrymme för dessa åtgärder möjligen försvaras.

Utredningen föreslår inte att systemet med offentliga ombud, som eljest tillämpas vid beslut om hemliga tvångsmedel, ska införas. Om utredningens förslag i övrigt skulle leda till lagstiftning bör dock denna rättsäkerhetsåtgärd komma i tillämpning i vart fall när fråga är om s.k. särskilt ingripande åtgärder enligt 2 kap. 5 § respektive 3 kap. 4 § i den särskilda lagen.

Någon skyldighet att till riksdagen redovisa användningen av särskilda inhämtningsåtgärder, motsvarande vad som gäller för användningen av hemliga tvångsmedel, föreslås inte av utredningen. Även i detta avseende är jag av avvikande uppfattning. Någon skarp gräns för nu föreslagna åtgärder, i förhållande till användningen av hemliga tvångsmedel, föreligger inte. Det är väsentligt, inte minst för tilltron till den polisiära maktutövningen, att varje praktiskt genomförbar möjlighet till insyn och kontroll från medborgarnas sida tillvaratas. I vart fall bör redovisningsplikten gälla de åtgärder som jag ovan föreslagit ska omfattas av systemet med offentliga ombud.

Kommittédirektiv

Vissa polisiära arbetsmetoder

Dir. 2007:185

Beslut vid regeringssammanträde den 20 december 2007

Sammanfattning av uppdraget

En särskild utredare ska, med särskilt beaktande av rättssäkerhets- och integritetsskyddsaspekterna, förhållandena i andra länder och det internationella brottsbekämpande samarbetet, överväga vissa straffprocessuella och polisrättsliga frågor angående de brottsbekämpande myndigheternas dolda spanings- och utredningsverksamhet.

Utredaren ska bl.a.

- överväga i vilken utsträckning tjänstemän vid de brottsbekämpande myndigheterna bör ha möjlighet att i samband med s.k. infiltrationsoperationer ta del i planering och annan förberedelse eller utförande av vissa brott, när detta är nödvändigt för att förhindra eller avslöja allvarlig brottslighet,
- överväga i vilken utsträckning polisens och tullens rapporterings-, anmälnings- och ingripandeskyldighet samt åklagarnas åtalsplikt bör gälla i fråga om brott som kommer till myndigheternas kännedom i samband med infiltrationsoperationer,
- överväga i vilken utsträckning de brottsbekämpande myndigheterna bör kunna använda sig av olika slag av provokativa åtgärder för att förmå en gärningsman att röja sig,
- överväga förutsättningarna för att i samband med infiltrationsoperationer gå in i annans bostad eller vidta andra åtgärder som i polisens eller tullens vanliga verksamhet hade krävt beslut om tvångsmedel,

- överväga en ändamålsenlig författningsreglering av sådan användning av tekniska spaningsmetoder som utgör ett intrång i enskildas integritet eller av andra skäl bör lagregleras,
- i ett delbetänkande överväga behovet av mer ändamålsenliga regler om inhämtningen av uppgifter om telemeddelanden, abonnemang eller mobiltelefoner inom polisens och tullens underrättelseverksamhet och under förundersökningar innan det finns någon skäligen misstänkt gärningsman, och
- utifrån övervägandena lägga fram de förslag till lagändringar som han eller hon finner lämpliga.

Uppdraget ska redovisas slutligt senast den 31 maj 2009.

Bakgrund

I arbetet med att upptäcka och beivra brott är det ibland nödvändigt att använda straffprocessuella tvångsmedel eller andra särskilda arbetsmetoder. Sådana metoder kan ibland innebära påtagliga ingrepp i enskildas personliga sfär. Av rättssäkerhets- och integritetsskyddsskäl är det av största vikt att metoder av detta slag ges en ändamålsenlig utformning och att regelverket kring metoderna utformas så att den enskildes rättssäkerhet kan tryggas och riskerna för missbruk minimeras. När det övervägs om det är lämpligt att införa nya sådana metoder eller att utvidga tillämpningsområdet för befintliga metoder ska den s.k. proportionalitetsprincipen beaktas. Det innebär att behovet alltid måste vägas mot det integritetsintrång som användandet av metoden kan innebära för den enskilde. Dessutom måste det säkerställas att den enskildes rättssäkerhet kan upprätthållas och att eventuellt missbruk eller annan felaktig användning av metoderna kan upptäckas och beivras samt att den enskilde har rimliga möjligheter att utnyttja den rätt till ersättning som kan föreligga. Detta gäller även vid överväganden om behovet av att i lag eller annan författning ange närmare förutsättningar för i viss mån redan använda arbetsmetoder.

En arbetsmetod som aktualiserar frågor av detta slag är s.k. infiltration av kriminella grupper och nätverk. Infiltrationsoperationer av både enklare och mer kvalificerat slag har under senare år fått ökad betydelse, i synnerhet i det internationella samarbetet mot gränsöverskridande och organiserad brottslighet som också

svensk polis och tull deltar i. I operationerna deltar poliser och andra tjänstemän som uppträder under fiktiva identiteter och antagna roller (*undercover operations*). Sedan den 1 oktober 2006 kan svenska poliser på ansökan av anställningsmyndigheten tilldelas s.k. kvalificerade skyddsidentiteter. I Sverige saknas emellertid författningsbestämmelser om hur infiltrationsoperationer ska gå till. Det är därför inte alltid tydligt exempelvis vad en polisman, som har infiltrerat en kriminell grupp, får göra i samband med infiltrationsoperationen. I flera andra länder finns det däremot sådana bestämmelser. Det förekommer att bestämmelser av detta slag ger en polisman befogenhet att under infiltration handla på sätt som, om befogenheten inte hade funnits, hade utgjort brott.

Även andra former av kvalificerad dold spaning har ökat i betydelse i det internationella samarbetet, inte minst användningen av olika slag av tekniska spaningsmetoder. Dessa metoder har med den nya informationsteknologin utvecklats mycket snabbt. Till en allt lägre kostnad kan en allt större mängd ljud och bilder tas upp och liksom annat slag av information bevaras och behandlas. Som exempel på tekniska spaningsmetoder av detta slag kan nämnas användandet av kroppsmikrofoner och övervakning med hjälp av burna kameror. Ett annat exempel på en teknisk spaningsmetod är s.k. pejling, som innebär att det är möjligt att följa exempelvis ett fordons geografiska position och förflyttning på avstånd. Inte heller dessa arbetsmetoder är lagreglerade. Metoderna anses emellertid kunna användas i viss utsträckning utan särskilt lagstöd.

Bl.a. den snabba utvecklingen av mobil telefoni har inneburit nya tekniska möjligheter att genomföra pejling och liknande metoder. Därtill förekommer att de tekniska systemen för mobiltelefoni numera registrerar bl.a. mobiltelefoners position och andra uppgifter om telemeddelanden. Det förekommer också att polisen och tullen, i syfte att kartlägga brottslig verksamhet och i övrigt arbeta brottsförebyggande, med tillämpning av bestämmelsen i 6 kap. 22 § första stycket 3 lagen (2003:389) om elektronisk kommunikation begär ut uppgifter om telemeddelanden från operatörerna. Det kan vara fråga om uppgifter om vilka samtal som har förekommit, däremot inte uppgifter om innehållet i samtalen. Såväl tekniken kring elektronisk kommunikation som polisens och tullens underrättelseverksamhet har genomgått stora förändringar under senare år. Mot den bakgrunden har det uppkommit frågor bl.a. om den angivna bestämmelsen numera är ändamålsenligt utformad. En utredning har nyligen lämnat förslag till hur ett EG-direktiv om lagring av

trafikuppgifter ska genomföras i svensk rätt. Förslaget innebär att uppgifter ska lagras hos operatörerna i ett år (SOU 2007:76). Även mot den bakgrunden finns det anledning att överväga förutsättningarna för utlämnande av uppgifter om telemeddelanden.

Åtgärder som företas inom ramen för dold spanings- och utredningsverksamhet, däribland infiltrationsåtgärder och olika slag av tekniska spaningsmetoder, kan innebära ingrepp i enskildas personliga sfär. Åtgärderna genomförs i hemlighet eller på så sätt att de som utsätts för åtgärderna vilseleds om åtgärdernas verkliga innebörd. De som utsätts för åtgärderna har således inte möjlighet att, såsom vid öppen tvångsmedelsanvändning, få åtgärderna prövade av domstol eller på annat sätt. Inte minst infiltrationsåtgärder kan i vissa fall ge upphov till så betydande rättssäkerhets- och integritetsskyddsfrågor att starka skäl talar för en lagreglering för sådana fall. En sådan lagreglering skulle också ligga i linje med Europarådets ministerkommittés rekommendation (Rec [2005] 10) om användandet av särskilda undersökningsmetoder i fråga om allvarlig brottslighet inbegripet terroristhandlingar. Medlemsländerna rekommenderas där att med lagstiftning och tillhandahållande av resurser möjliggöra användningen av särskilda undersökningsmetoder men även att säkerställa judiciell eller annan oberoende kontroll av användningen av dessa metoder.

En särskild metod att skaffa bevisning om brott är s.k. provokation. I andra med Sverige jämförbara länder har tjänstemän vid de brottsbekämpande myndigheterna getts uttryckliga befogenheter att företa provokativa åtgärder som, om sådana befogenheter inte hade funnits, hade utgjort brott. Det kan handla om att polisen aktivt förmår en brottsmisstänkt person att begå ett brott som röjer att han eller hon har begått eller håller på att begå ett annat, mera allvarligt brott. Riksåklagaren har nyligen, efter samråd med Rikspolisstyrelsen och Tullverket, tagit fram riktlinjer för handläggning av provokativa åtgärder och därigenom väsentligt stärkt de brottsbekämpande myndigheternas beredskap och möjligheter att genomföra effektiva och rättssäkra provokationsoperationer (se Riksåklagarens riktlinjer 2007:1 Handläggning av provokativa åtgärder, men även RättsPM 2007:4 Provokativa åtgärder). I Sverige finns det dock inte någon uttrycklig författningsreglering av i vad mån de brottsbekämpande myndigheterna får använda sig av provokationer eller av den straffrättliga betydelsen av att ett brott kommit till efter provokation. Viss provokation anses enligt allmänna principer vara tillåten (s.k. bevisprovokation), medan annan provoka-

tion anses vara otillåten (s.k. brottsprovokation). Gränsen mellan det ena och det andra slaget av provokation är emellertid inte alltid lätt att bestämma och tillämpa i konkreta fall. Det finns inte heller i den juridiska doktrinen någon i alla delar enhetlig syn på denna gränsdragning liksom inte heller på frågor om myndigheternas rapporterings-, anmälnings-, ingripande- och åtalsplikt samt straffansvar för en framprovocerad gärning (se SOU 2003:74 s. 113 ff.). Av rättssäkerhetsskäl finns det anledning att överväga en lagreglering även i denna del. Också effektivitetsskäl kan tala för en lagreglering.

Uppdraget

Deltagande i andras brottsliga aktiviteter

Svensk polis eller tull har i dag inte någon uttrycklig befogenhet att i samband med infiltrationsoperationer företa åtgärder som utgör en brottslig handling. En polisman som har infiltrerat en kriminell gruppering som förbereder t.ex. ett grovt rån eller ett grovt narkotikabrott kan emellertid behöva göra sig skyldig till straffbara gärningar om han eller hon ska kunna delta i förberedelserna för brottet, trots att deltagandet egentligen syftar till att förhindra att det planerade brottet fullbordas.

Ett annat problem som kan uppkomma i samband med infiltrationsåtgärder sammanhänger med att svensk polis som huvudregel är skyldig att rapportera, anmäla och ingripa mot brott som kommer till dess kännedom och att svenska åklagare som huvudregel är skyldiga att väcka åtal när konstaterade brott hör under allmänt åtal. Har en polisman infiltrerat en kriminell gruppering, kan de tjänstemän som deltar i operationen vara skyldiga att rapportera och även ingripa mot ett mindre brott som kan konstateras i samband med operationen, trots att rapporteringen med åtföljande ingripande och åtal kan medföra att polismannens identitet röjs och att hela infiltrationsoperationen därmed går om intet. Visserligen anses gripande, förhör och andra åtgärder kunna skjutas upp genom s.k. interimistisk passivitet, men det ska då säkerställas att ett ingripande sker vid ett senare tillfälle.

Den nuvarande ordningen innebär således att tjänstemän vid svenska brottsbekämpande myndigheter inte kan infiltrera kriminella grupperingar i många situationer där detta synes ha kunnat

göras i andra länder. Därmed minskar svensk polis möjligheter att delta i det internationella samarbetet och det brottsbekämpande arbetet riskerar att hämmas.

Mot den redovisade bakgrunden finns det anledning att överväga behovet av lagregler som ger tjänstemän vid svenska brottsbekämpande myndigheter bättre möjligheter att infiltrera kriminella grupper och som samtidigt klarlägger förutsättningarna för infiltrationsoperationer. I dessa överväganden bör ingå en noggrann analys av lämpligheten av olika slag av infiltrationsåtgärder, en bedömning av åtgärdernas effektivitet för brottsbekämpningen, de eventuella risker från rättssäkerhets- och integritetsskyddsperspektiv som sådana åtgärder kan medföra och behovet av förhands- eller efterhandskontroll av åtgärderna. Vidare bör utredaren överväga dels de straffrättsliga konsekvenserna för de medverkande, dels avgränsningen av de handlingar som medverkan får avse med hänsyn till handlingarnas typ och allvarlighet.

Utredaren ska därför

- inhämta information om förekommande lagreglering och praxis i de övriga nordiska länderna och de ytterligare länder som bedöms vara relevanta för utredningsuppdraget,
- överväga i vilken utsträckning tjänstemän vid de brottsbekämpande myndigheterna i samband med kriminalunderrättelseverksamhet eller under förundersökningar bör kunna infiltrera kriminella grupperingar och därvid delta i planering, annan förberedelse eller utförande av brott,
- överväga i vilken utsträckning tjänstemän vid de brottsbekämpande myndigheterna vid infiltrationsoperationer bör kunna ta hjälp av enskilda privatpersoner, också när dessa förutsätts ta del i brottslig verksamhet,
- överväga om det finns anledning att begränsa polisens och tullens rapporterings-, anmälnings- och ingripandeskyldighet samt åklagarnas åtalsplikt avseende brott som uppmärksammas i samband med infiltrationsoperationer i den utsträckning det behövs för att angelägen brottsbekämpande verksamhet inte ska skadas,

- överväga rättssäkerhets- och integritetsskyddsfrågor, bl.a. huruvida tillstånd till mera långtgående infiltrationsåtgärder bör krävas i förhand och om särskild intern eller extern kontroll över åtgärderna kan behövas i efterhand, och
- utarbeta nödvändiga författningsförslag.

Provokativa åtgärder

Svensk polis och tull har redan i dag visst utrymme att vidta s.k. provokativa åtgärder. Åtgärderna måste dock utformas så att de inte kommer i konflikt med någon straffbestämmelse eller andra författningar. Bland annat får en provokativ åtgärd inte innebära anstiftan till brott. Någon författningsreglering om vad som utgör en tillåten respektive otillåten provokation i brottsbekämpande syfte finns dock, som ovan har nämnts, inte.

Inte minst erfarenheterna från andra länder visar att provokativa åtgärder, också av ett mer kvalificerat slag, kan vara en värdefull metod för att avslöja svårutredd och allvarlig brottslighet. Det förhållandet att de straffrättsliga förutsättningarna för provokativa åtgärder inte är fastslagna i lag minskar dock metodens användbarhet för svenskt vidkommande. Detta medför också risker från rättssäkerhetssynpunkt, såväl för brottsmisstänkta som för polismän och andra tjänstemän inom den brottsbekämpande verksamheten.

Det finns därför anledning att överväga införandet av en lagreglering som tydliggör i vilken utsträckning de brottsbekämpande myndigheterna ska ha möjlighet att företa provokativa åtgärder. Övervägandena bör innefatta även frågan om det bör få förekomma provokation som framkallar ett brott som, om provokationen inte hade förekommit, aldrig hade begåtts. Övervägandena ska föregås av en analys av provokativa åtgärders lämplighet i bl.a. ett rättssäkerhets- och integritetsskyddsperspektiv samt en bedömning av åtgärdernas effektivitet för brottsbekämpningen.

Utredaren ska därför

- inhämta information om rättsläget i de övriga nordiska länderna samt övriga länder som bedöms vara relevanta för utredningsuppdraget,

- analysera Europadomstolens praxis i denna fråga, särskilt vad avser rätten till en rättvis rättegång enligt artikel 6 i Europakonventionen,
- mot bakgrund av hur provokativa åtgärder används i andra länder, det internationella samarbetet och Europakonventionens krav överväga i vilken utsträckning de svenska brottsbekämpande myndigheterna bör kunna använda provokativa åtgärder,
- särskilt överväga i vad mån det bör få förekomma sådan provokation som i dag inte är lovlig och som kan leda till att den provocerade personen begår ett brott som, provokationen förutan, inte hade begåtts,
- överväga hur ett framprovocerat brott bör bedömas straffrättsligt och i vad mån det bör omfattas av polisens och tullens rapporterings-, anmälnings- och ingripandeskyldighet och åklagarens åtalsplikt,
- överväga rättsäkerhets- och integritetsskyddsfrågor, bl.a. i vilken utsträckning det bör krävas förhandstillstånd till mer kvalificerade provokationsåtgärder och om särskild intern eller extern kontroll kan behövas i efterhand, och
- utarbeta nödvändiga författningsförslag.

Tvångsmedelsliknande situationer

Varje medborgare är enligt regeringsformen skyddad gentemot olika slag av intrång från det allmänna, t.ex. husrannsakan. Skyddet får inskränkas men endast under vissa i regeringsformen angivna förutsättningar. Bestämmelserna om husrannsakan och andra straffprocessuella tvångsmedel utgör exempel på sådana inskränkningar. En infiltrationsoperation i underrättelsesyfte eller inom ramen för en förundersökning utgör i och för sig inte ett sådant intrång som avses i regeringsformen. Infiltrationen kan emellertid ge upphov till effekter som står effekterna av straffprocessuella tvångsmedel nära. Det sammanhänger med att de polismän som deltar i infiltrationen döljer att de är poliser och uppträder under fiktiva identiteter och i antagna roller. Det kan t.ex. inträffa att en polisman som har infiltrerat en kriminell gruppering i samband med operationen blir inbjuden till en bostad och det står klart att inbjudan aldrig hade lämnats om polismannens rätta identitet hade varit känd. Situa-

tionen kan då – i synnerhet om polismannen antar inbjudan i syfte att skaffa sig kunskap om förhållandena inne i bostaden – komma att likna situationen vid en husrannsakan. Ett annat exempel är att en polisman i samband med en infiltration får tillgång till föremål som han eller hon inte hade fått tillgång till om hans eller hennes rätta identitet hade varit känd. Den situationen kan uppvisa vissa likheter med beslag.

I andra länder har det införts särskilda bestämmelser för situationer av detta slag. I svensk rätt saknas sådana särskilda regler såväl när infiltration företas inom ramen för förundersökningar om brott som när den sker inom ramen för polisens underrättelseverksamhet.

Utredaren ska därför

- inhämta information om vad som i detta avseende gäller i övriga nordiska länder samt andra länder som bedöms vara relevanta för utredningsuppdraget,
- överväga förutsättningarna för att i samband med infiltrationsoperationer vidta åtgärder som i polisens vanliga verksamhet skulle ha krävt ett beslut om användande av tvångsmedel,
- överväga rättsäkerhets- och integritetsskyddsfrågor, bl.a. vem som bör fatta beslut om åtgärderna i olika situationer, och
- utarbeta nödvändiga författningsförslag.

Författningsreglering av tekniska metoder

Vid infiltrationsoperationer, men även vid andra slag av polis- eller tulloperationer, används olika tekniska metoder för att inhämta och bevara information. Det handlar främst om tekniska metoder för att ta upp bild och ljud med kameror och mikrofoner eller bestämma ett föremåls geografiska position genom s.k. pejling.

I de fall användningen av en teknisk metod utgör ett ingrepp i det skydd som regeringsformen och Europakonventionen ger den enskilde mot intrång från det allmännas sida ska användningen ha stöd i lag för att vara tillåten. På det straffprocessuella området har detta skett genom att sådan användning har reglerats som ett tvångsmedel. Tekniska metoder kan dock användas på många olika sätt och all användning av sådana metoder i brottsbekämpande syfte utgör inte ett sådant ingrepp i enskildas sfär som kräver stöd i

lag. Ibland kan användningen av en viss teknisk metod förutsätta något slag av ingrepp, t.ex. en husrannsakan som möjliggör anbringandet av pejlingsutrustning i ett fordon. Detta ingrepp kan i sådana fall vara att anse som ett tvångsmedel, även om en användning av pejlingsutrustningen i sig inte skulle behöva vara det.

I sitt delbetänkande Skyddet för den personliga integriteten (SOU 2007:22) redovisar Integritetsskyddskommittén de utredningar som tidigare har lämnat olika förslag till ytterligare lagreglering av användning av tekniska spaningsmetoder. Kommittén anser för sin del att det i ett integritetsperspektiv finns starka skäl att förorda att integritetskänsliga spaningsmetoder blir föremål för en reglering. Kommittén pekar på några aspekter som den anser är viktiga att beakta vid en översyn som tar sikte på en sådan reglering, bl.a. bör regleringen vara så teknikneutral som möjligt och undvika att uttömmande ange vilka metoder som avses.

Mot den redovisade bakgrunden bör det övervägas i vad mån användning av skilda slag av tekniska spaningsmetoder innebär sådana påtagliga intrång i enskilds sfär att användningen bör regleras i lag.

Som angetts i det föregående förekommer det att de brottsutredande myndigheterna med stöd av 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation begär ut vissa uppgifter om telemeddelanden från operatörerna. Beredningen för rättsväsendets utveckling har i ett delbetänkande (SOU 2005:38) föreslagit bl.a. att den nämnda bestämmelsen ska upphävas och att det i stället i rättegångsbalken ska införas bestämmelser om användning av hemlig teleövervakning innan det finns någon som är skäligen misstänkt för brott. I delbetänkandet föreslås också att myndigheterna ska kunna få ut abonnemangsuppgifter inklusive uppgifter om vem som har haft en viss IP-adress vid ett visst tillfälle, även vid misstanke om brott som i det aktuella fallet endast bedöms föranleda ett bötesstraff. En i viss mån motsvarande bestämmelse finns redan i dag i 6 kap. 22 § första stycket 2 lagen om elektronisk kommunikation. Den bestämmelsen är dock mera begränsad, bl.a. därför att den kan tillämpas enbart vid utredning om brott som kan föranleda annan påföljd än böter. Delbetänkandet har remissbehandlats och förslagen bereds inom Regeringskansliet. Det kan emellertid redan nu konstateras att det finns ett operativt behov av att kunna inhämta vissa uppgifter om telemeddelanden även inom ramen för polisens och tullens underrättelseverksamhet. Situationen liknar då ofta förhållandena under ett tidigt förundersökningsskede. Det är därför inte tillfyllest att ersätta nuvarande bestämmelse i 6 kap. 22 §

första stycket 3 lagen om elektronisk kommunikation med en reglering i rättegångsbalken. Inom ramen för polisens underrättelseverksamhet kan det också finnas ett behov av att få tillgång till abonnemangsuppgifter. Mot den bakgrunden finns det anledning att i ett sammanhang överväga behovet av ändamålsenliga regler om inhämtande av uppgifter *dels* inom polisens och tullens underrättelseverksamhet, *dels* under förundersökningar innan det finns någon skäligen misstänkt gärningsman. Utredaren ska därför

- inhämta information om rättsläget i övriga nordiska länder samt de övriga länder som bedöms vara relevanta för utredningsuppdraget,
- göra en analys av Europadomstolens praxis till den del denna kan vara av betydelse för användningen av tekniska spaningsmetoder, särskilt vad avser rätten till privatliv enligt artikel 8 i Europakonventionen,
- överväga i vad mån den användning av tekniska metoder som i dag förekommer hos de brottsbekämpande myndigheterna bör regleras i lag och därvid även, efter en bedömning av åtgärdernas effektivitet för brottsbekämpningen, överväga om en sådan reglering bör medge vissa ingrepp som annars förutsätter beslut om straffprocessuella tvångsmedel, bl.a. i samband med att teknisk utrustning ska installeras,
- överväga behovet av författningsreglering när det gäller polisens och tullens möjligheter att inhämta uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel i syfte att identifiera viss teknisk utrustning, t.ex. en mobiltelefon,
- överväga behovet av mer ändamålsenliga regler om olika former av inhämtning av uppgifter om telemeddelanden, abonnemang och mobiltelefoner (t.ex. uppgifter om vilka telefonnummer eller telefoner som har haft kontakt med en viss basstation under en tidsperiod, s.k. basstationstömning, eller uppgifter om vilka telefonnummer eller telefoner som har haft kontakt med ett visst telefonnummer eller en viss telefon under en tidsperiod eller uppgifter om vem som har haft en viss IP-adress vid ett visst tillfälle) dels inom polisens och tullens underrättelseverksamhet, dels under förundersökningar innan det finns någon skäligen misstänkt gärningsman,

- överväga rättsäkerhets- och integritetsskyddsfrågor, bl.a. vem som bör fatta beslut om användning av tekniska metoder i olika situationer, och
- utarbeta nödvändiga författningsförslag.

Vid utarbetandet av lagförslag ska utredaren så långt möjligt välja en teknikneutral reglering. Utredaren ska vidare utgå från att den nuvarande bestämmelsen i lagen om elektronisk kommunikation som tar sikte på de brottsutredande myndigheternas tillgång till elektronisk kommunikation i brottsutredningar (se 6 kap. 22 § första stycket 3) ska ersättas med en annan lagreglering. Utredaren ska också utgå från att det ska vara möjligt för de brottsutredande myndigheterna att få tillgång till abonnemangsuppgifter (se 6 kap. 22 § första stycket 2), inklusive uppgifter om vem som har haft en viss IP-adress vid ett visst tillfälle, även vid misstanke om brott som i det konkreta fallet bör föranleda ett bötesstraff (jfr förslaget i SOU 2005:38).

Andra frågor

Om det bedöms ändamålsenligt och ryms inom tiden för uppdraget, får utredaren ta upp och lämna förslag i andra frågor som aktualiseras under utredningsarbetet.

Ekonomiska konsekvenser

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Samråd och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och inom EU.

Under genomförandet av uppdraget ska utredaren samråda med de brottsbekämpande myndigheterna och andra myndigheter i den utsträckning som utredaren finner lämpligt.

Utredaren ska i ett delbetänkande senast den 19 juni 2008 redovisa resultatet av sina överväganden när det gäller polisens och tullens möjligheter till inhämtning av uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel samt inhämtning av uppgifter om mobiltelefoner, telemeddelanden och abonnemang inom polisens och tullens underrättelseverksamhet och under förundersökningar innan det finns någon skäligen misstänkt gärningsman.

Uppdraget i övrigt ska redovisas senast den 31 maj 2009.

(Justitiedepartementet)

Kommittédirektiv

Tilläggsdirektiv till Polismetodutredningen (Ju 2008:01)

Dir. 2008:91

Beslut vid regeringssammanträde den 3 juli 2008

Ändrad redovisningstidpunkt för uppdraget

Med stöd av regeringens bemyndigande den 20 december 2007 tillkallade chefen för Justitiedepartementet en särskild utredare med uppdrag att överväga vissa straffprocessuella och polisrättsliga frågor angående de brottsbekämpande myndigheternas dolda spanings- och utredningsverksamhet och att lägga fram de förslag till lagändringar som utredaren finner lämpliga (dir. 2007:185). Utredningen har antagit namnet Polismetodutredningen (Ju 2008:01). Enligt uppdraget ska utredaren i ett delbetänkande redovisa resultatet av sina överväganden när det gäller dels polisens och tullens möjligheter till inhämtning av uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel, dels inhämtning av uppgifter om mobiltelefoner, telemeddelanden och abonnemang inom polisens och tullens underrättelseverksamhet och under förundersökningar innan det finns någon skäligen misstänkt gärningsman. Delbetänkandet ska lämnas senast den 19 juni 2008. Uppdraget i övrigt ska redovisas senast den 31 maj 2009.

Uppdraget till den särskilde utredaren ändras på så sätt att delbetänkandet inte behöver innehålla redovisning av utredningens arbete när det gäller polisens och tullens möjligheter till inhämtning av uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel. Den delen av uppdraget ska i stället redovisas i samband med den slutliga redovisningen.

Uppdraget ändras även på så sätt att tidpunkten för redovisningen av delbetänkandet flyttas fram till den 31 december 2008 och tidpunkten för slutbetänkandet till den 1 oktober 2009.

(Justitiedepartementet)

Expert report to the Inquiry on Certain Police Methods

by Professor Iain Cameron

1 Introductory remarks

I have been asked to provide a report analyzing the case law of the European Court of Human Rights relating to the issues, first of surveillance by technical means, and second, of the use of infiltration. The focus in both cases is on examining which methods of surveillance and infiltration require regulation by law and the degree of precision of this regulation.[1] The present report, however, is not a systematic comparison of the existing regulation of surveillance in Sweden with the Convention standards, even if I, on occasion, do take up such compliance issues.

A few introductory points are in order. Elaborating useful "forward-looking" rules from the "backward-looking" case law of the Court is not an easy task. The Court's case law should be seen as an accumulation of general principles. The generality of the principles involved tends to reduce its value in specific concrete situations. The Court takes both admissibility decisions and issues judgments. In general, the Court's reasoning in admissibility decisions is considerably briefer and less developed than its reasoning in judgments (one relevant exception being the *Weber and Saravia* case, dealt with below). In the absence of a judgment, one has to build an analysis on the basis of admissibility decisions. The Court develops its principles over time, only rarely overruling earlier cases, but instead distinguishing these. Thus, there can be a degree of inconsistency between earlier and later case law.[2]

The concepts used in the Convention are autonomous. This means that the fact that a particular state measure is not regarded as an interference in private life according to a state constitution and laws does not necessarily mean that it is also so regarded from the perspective of the Convention. Even though Convention concepts are autonomous, the Court has rarely taken the opportunity to elaborate upon the meaning of a particular Convention concept, but has, up until relatively recently, attempted to limit explicitly its discussion to the case in hand. This caution showed by the Court is

[1] I would like to thank my colleagues Torbjörn Andersson, Thomas Bull, Johan Boucht and Magnus Ulväng for helpful comments made on an earlier draft of this report. Any errors etc. remaining are my responsibility. This report was written in February 2010 and thus takes up practice up to this time. At the time it was published, December 2010, I made certain changes in order to take into account two important judgments (the Uzun and Kennedy cases) which had been issued during the period February–November 2010.

[2] Judgments have a higher status than admissibility decisions, but where a judgment is later qualified by an admissibility decision the result is that the legal position is uncertain, especially where the Court's reasoning is not always clear.

partly because the Court was not intended to act as (and does not – yet – have the legitimacy to act as) a fully-fledged constitutional court. However, its "constitutional" functions are increasing, and the Court is becoming more "pedagogical" in style. It now tends to begin its treatment of a case by recounting the applicable general principles, as derived from its case law, before applying these to the facts in the case.

In reaching a conclusion that something is, or is not, in accordance with the Convention, the Court tends to aggregate all the relevant factors. A law, or legal mechanism, which is regarded as deficient in formulation (e.g. because it is imprecise) may nonetheless be corrected by a safeguard (e.g. because it compensates for the risk of abuse caused by the imprecision). It is thus very important to take into account the whole context of a judgment. States A and B may have the same, or more or less the same, formulation of a particular state power. However, the safeguards in the law, or the ways these are applied, may vary between the two states. This can mean that safeguard X – which was of crucial importance in finding that state A's laws were acceptable – is missing in state B, or exists on paper, but is not applied in practice, with the consequence that state B is found in violation of the Convention.[3]

In this respect one can note that states party to the ECHR are obliged to take into account cases concerning other states. Under ECHR Article 46, states only "undertake to abide by the final judgement of the Court *in any case to which they are parties*". However, the general obligation under Article 1 to "secure to everyone within their jurisdiction the [Convention] rights and freedoms" means that the national legislator, and the national courts, cannot ignore cases concerning other states. Having said this, the room for interpretation the national legislator, and national judge, has in applying a judgment concerning another state will be larger, because the differences between the two factual situations (the instant case, and the case dealt with by the ECtHR) will usually be greater.

A national legislator, faced with ECtHR case law concerning other states, can be tempted to regard as unsettled the issue of whether or not its law is in conformity with the Convention. It might

[3] Obviously it is vitally important that the Court fully understood the respondent state's laws and practices. If and when it bases its judgment on a misunderstanding of these, it not only undermines the value of the case as a source of law for the respondent state, but for all the other contracting parties too.

want to wait for a judgment on the issue against its own state, or at least a clear Grand Chamber judgment (one of the main ideas behind the Grand Chamber being to provide coherence in the ECtHR case law). However, to do this is to stretch its obligations to fulfill Article 1 in good faith.

It must be remembered that the ECHR is intended as a minimum standard.[4] In a situation where relatively clear ECtHR case law indicates strongly that laws or practices are not in conformity with the Convention, the correct approach for the national legislator is not to "balance on the boundary" of what is permissible.[5] This applies particularly to a legislator which wishes earnestly to avoid putting its judiciary in the position of having to "re-write" major pieces of legislation found to breach the Convention.[6] A state's ambition to ensure that there is no doubt that it complies with its obligations under the Convention should be also strengthened by the fact that the Court applies a "teleological" interpretative method. This method means that rights are constructed so as to be relevant to the needs of society today, which in turn means that the demands placed upon states can increase with time.

As shown below, the "accordance with the law" standard in the Court's case law has been developed as a safeguard against misuse of power. Here one should be aware that important safeguards can be "implicit" in a state's legal culture. However, the Court is in a poor position to judge the efficacy of legal cultural safeguards.[7] Whatever the formal legal safeguards in a state's system, the police and the prosecutor, as a result of professionalism, training etc. may in practice adhere to high ethical standards in investigating crime. But the Court simply put, has so far found it difficult to say openly to

[4] In this respect I should note that a strengthening of the constitutional protection of personal integrity (RF 2:6) (prop. 2009/10:80) will enter into force 1 January 2011. "everyone is vis a vis the state protected against significant interferences with personal integrity, if this occurs in the absence of consent and involves surveillance or monitoring an individual's personal relations" (var och en gentemot det allmänna [är] skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden").

[5] Cf. SOU 2001:25, s. 331 "balansera på gränsen till vad som kan tänkas strida mot grundläggande mänskliga rättigheter".

[6] This was made clear repeatedly in the travaux préparatoires to the incorporation statute, Prop. 1993/94:117. The Swedish courts, for their part, demand "clear support" in the ECtHR's case law before they are prepared to "overturn the applicable Swedish law" See NJA 2000 s. 622, NJA 2004 s. 840, and NJA 2010 s.268 I-II.

[7] Cf Cameron, 2000, p. 258 "In practice, the value of an external monitor will mainly depend on the political climate in which he or she works, the dedication of the office holder and the competence of his or her staff. These are fairly intangible things on which to form an opinion, far away in Strasbourg. As already mentioned, the Court is relatively ill-equipped to judge whether *formal* safeguards are *real* safeguards, and it knows it."

state A, when it finds state A's laws and practices to be in violation of the Convention, "we did not find State B's system in violation of the Convention, because State B's police are better trained, better resourced and relatively well behaved: but your police are none of these things".

Besides, even if they work well most of the time, legal culture safeguards can come under pressure in a variety of ways and can change with time. This is another reason for formalizing and making explicit such safeguards. In this respect I can note that within the EU, police and prosecutorial cultures are increasingly coming in contact with each other over national borders. There is an obvious need of increased international cooperation in dealing with transboundary crime. Assistance within the EU is increasingly being based on the principle of mutual recognition. The idea is that the police and prosecutor should be able to offer their colleagues in other EU states the same measures they use themselves in investigating and prosecuting crime. Joint investigation teams, while still rare, are becoming more common. In these circumstances, it is not enough to rely upon national legal cultural safeguards. There is a heightened need for improved clarity in the text of the applicable law, and for explicit statutory safeguards against misuse.

In the present report, I have set out the explicit standards set by the Court. Where these are not clear, I have tried to extrapolate these, working on the logic of the Court's case law as a whole and my own knowledge of the area. I have tried faithfully to identify which parts of my report consist of Court standards, and which parts consist of my interpretation of these.

2 A typology of surveillance and something on infiltration

Surveillance and data accessing are increasingly growing together. As far as digital data is concerned it is difficult to distinguish between "stored" and "transmitted" data, as the form and content of the data stored in one computer system can be very quickly changed, or even automatically updated, by communications from another computer. This in turn means that it can, in practice, be difficult to distinguish "search" of the data bank from "interception" of communications. Moreover, insofar as the product of surveillance becomes part of police data banks, the Convention sets out require-

ments concerning the legal framework for the regulation of these data banks. Even these requirements are relevant for this report. I have not, however, dealt with these in detail.

For the purposes of the present report, it is useful to distinguish between eight technical surveillance methods. The first of these is *bugging*, the use of concealed microphones to pick up conversations to which the monitor is not a party. The second and third are *secret* respectively *overt (open) visual surveillance* meaning the use of an apparatus for monitoring *and recording* pictures. A sub-group here is the use of sophisticated imaging, such as microwave radar, or infra-red cameras, to pick up activity within buildings or in other difficult surveillance situations. Such an apparatus can be steered manually or remotely. The fourth type of surveillance is the use of a microphone and recording device to monitor a conversation in which the monitor participates. The conversation being recorded can be over a telephone line or in a private or public place ("human wires" or *participant audio surveillance*). The participation in the conversation is open, but the recording is not. Thus, the surveillance is still secret. The fifth is the video equivalent of the fourth type, i.e. the use of a concealed visual recording device to document an event to which the monitoring person is party (*participant video surveillance*). The fourth and fifth types of surveillance can naturally be combined. The sixth type is the *monitoring of the content of telecommunications* to which the monitor is not party. This used to be called telephone tapping, although "telecommunications" now also covers radio and microwave/satellite communications media, and fax, e-mail and other forms of communications between or via computers. The seventh type of surveillance involves identifying the circle of persons or telecommunications addresses with which the target communicates (*metering information*). The eight type of surveillance obtains what can be called *location information*, indicating the physical location of a thing, or a person. This can involve the physical planting of a bug which sends a radio signal indicating location. The use of movement sensors would also fall under this. However, there can be an overlap between the seventh and eight categories in that tracking a target's use of a mobile phone or a laptop computer, used for communicating with the internet, will give both location information and information on who, or what, the target is communicating with. A mobile phone, when switched on, or a laptop, when connected to the internet, sends periodic signals to the nearest transceiver stations. The target's

position can then be plotted, with more or less accuracy, depending on the strength of the signal vis-à-vis the nearest transceiver stations. Location information can also be obtained from the target's use of different types of plastic cards containing computer chips or electromagnetic tape which send electronic signals to public or private data banks. These signals have the side effect of indicating the target's location (e.g. withdrawals from cash machines, entry into a zone which requires a key card, lending of books in a library). When I wish to refer to both the seventh and eight categories, I use the term "interception of teledata".

It should be stressed that power, like water, tends to seek the point of least resistance. When one area of surveillance has been subjected to tight control, or a total prohibition, there is a risk that the police and security services seek the same information in other ways. This should reinforce the importance of regulating the whole area of state surveillance.[8]

Although I have distinguished between these different methods, these should not be seen as water-tight categories. As well as requiring different types of equipment, the above surveillance categories can be distinguished on the basis of whether they are employed after the event, or are contemporaneously to it (in "real time"). For example, metering information is post hoc. Planting of a bug indicating location occurs in real time, whereas, at least at the present state of technological development, most other forms of location information (withdrawals from cash machines etc.) can only be obtained some time after the event.

As regards infiltration, the following can be said. Infiltration can be described as a "special investigation technique", involving the use of informers (private persons) or undercover agents (police, customs etc. officials) to obtain information from suspects and others on planned, past or on-going offences. The boundary line between infiltration and "ordinary" police work, which can also involve secret visual or aural observation and the use of informers, is not hard and fast.

Infiltration is a necessary part of the police arsenal in dealing with crime, especially organized crime. However, when a private person is used to penetrate a suspected criminal activity, a variety of accountability problems arise. Informers' activities can be subject to varying degrees of (lack of) control from their police

[8] Cf. Lustgarten and Leigh 1994, p. 44.

"handlers". And with both undercover agents and informers, problems arise from the perspective of the *Rechtsstaat* when they participate actively in crimes.

The American sociologist Marx distinguished between four different types of police work on the basis of two criteria: the overtness of the actions and their deceptive or non-deceptive nature.[9] This gives a four-fold typology: *overt and non-deceptive* (which covers much conventional police work), *overt and deceptive*, (e.g. where a suspect is tricked by police officers into providing a confession), *covert and non-deceptive* (e.g. surveillance operations) and *covert and deceptive*. This fourth category would cover "undercover" police operations by either police agents acting with false identities and/or informers being operated by police agents.

A third criterion can be added: the interaction between investigating authorities on the one hand and witnesses, suspects and third parties on the other, to give a six-fold typology.[10] On this classification, the use of informers would fall within the category of "secret investigations with interaction but without deception" whereas the relationship between a police officer who conceals his or her identity and a suspect or potential offender would be regarded as "secret investigations with interaction and with deception". These classifications are of some use in understanding whether, and if so, how, different types of undercover operation can infringe privacy. However, too much weight should not be put on them. For example, there will almost invariably be an element of deception involved when informers are deliberately used to infiltrate a criminal organization. The suspect/potential offender may know the true identity of the person s/he is talking to, but will not know that this person is informing for, and/or acting on the instructions of, police officers.

3 The approach of the Court to Article 8

In general, the Court approaches cases which raise issues under Article 8 in the following way. First, it considers whether the action complained of falls within the scope of the right in question, and whether it infringes this right. Having found that the right has been infringed, it proceeds to consider whether the action taken by

[9] Marx, 1988, pp 11–13. Cf. Helmius, 2000, p. 28, who instead employs a scale of measures on the basis of the level of interference with personal integrity.
[10] See Council of Europe, 2005, referring to Valkaneer, 2000, p. 24.

the state falls within one of the accommodation clauses, i.e. whether it has been taken in the furtherance of a legitimate aim. Next, it determines whether the infringement could be said to be "in accordance with the law". The fourth and final step taken by the Court is to determine whether the infringement was "necessary in a democratic society". The Convention organs treat steps three and four as successive hurdles. This means that where they find that a measure complained of is not "in accordance with the law", then they usually do not proceed to examine whether the measure satisfies the requirements of "necessity in a democratic society".[11]

4 Generally on the concept of law in the Court's case law

The Court has stated that the two terms "prescribed by law" (in Articles 9, 10 and 11) and "in accordance with the law" (in Article 8 should be treated in the same way.[12] The Court held in Sunday Times v. UK that the "law" includes common law rules as well as statutes and subordinate legislation.[13] The Court has even accepted that a collective agreement can constitute "law" in the context of the Nordic tradition of leaving the regulation of the labour market to employees and employers organizations.[14] The Court stated in the Sunday Times case that to qualify as "law" a norm must be adequately accessible and formulated with sufficient precision to enable the citizen to regulate his conduct.[15] This is not a mere formal requirement. It also relates to the quality of the law in question. In Silver and others v. UK the Court made it clear that a law which "allows the exercise of unrestrained discretion in individual cases will not possess the essential characteristics of foreseeability and thus will not be a law for present purposes. The scope of the discretion must be indicated with reasonable certainty." The Court has also stated that adequate *safeguards* also must exist against *abuse* of

[11] See, e.g. the cases of Malone v. UK, Huvig v. France and Kruslin v. France, discussed below. See however, Kennedy v. UK, below
[12] A single expression is employed in the French text (prévue par la loi). Silver and others v. UK, 25 March 1983, A/61, para. 85. See further, van Dijk and van Hoof, 2006, p. 336. Although the phrase as such occurs in Articles 8-11, other articles in the Convention also implicitly or explicitly condition state interference with a right on a "law".
[13] Sunday Times v. UK, para. 47.
[14] Wretlund v. Sweden, No. 46210/99, Decision 9 March 2004 (Obligation on employee at nuclear plant to undergo drug test: inadmissible).
[15] Ibid. at para. 49.

the discretion established by law.[16] While these need not be written into the text of the law itself, the law must at least set up the conditions and procedures for the interference.[17] There is thus an overlap between the "law" requirements, the requirement of "necessity in a democratic society" and the requirement of effective remedies in Article 13.[18] For example, the degree of foreseeability required before a measure taken by the state in dealing with surveillance could be said to satisfy the requirements of "accordance with the law" can also serve as a safeguard against abuse of power (which relates to the "necessity" of the measure. Sometimes the Court chooses to focus upon the safeguards under the "necessity" requirement.[19] This may be done where there is room to doubt whether the functioning of the safeguards in practice corresponds to how they look on paper. On most occasions, however, the Court seems to find it easier to make a finding that the state has failed to comply with the "law" requirement.

The requirements of foreseeability and accessibility will vary according to the content of the law, the field it is designed to cover and the number and status of the addressees. In Groppera Radio v. Italy, for example, the "law" was an ordinance directed to radio companies which referred to technical provisions of certain international treaties in the field of telecommunications. The Court nonetheless considered that the addressees had, or ought to have had, access to the expert help necessary to understand its content.[20] In Rekvenyi v. Hungary one of the questions was whether a constitutional provision prohibiting the police to engage in political activity was sufficiently clear to be "foreseeable" in the absence of implementing norms. The Court considered that it was.[21] In the area of the criminal law and criminal procedure, other cases where the adressees are ordinary citizens and the intervention in individual rights is serious, the potential for abuse of power is greater, and the Convention organs have occasionally been more demanding.[22]

[16] See, e.g., Silver and others v. UK, paras 88–89.
[17] Klass v. FRG, No. 5029/71, Report of 9 March 1977 para. 63. Kruslin v. France, 24 April 1990, A/176-A, para. 35, Huvig v. France, 24 April 1990, A/176-B, para. 34.
[18] See Ruiz, 1997, pp. 183–184.
[19] See S and Marper v. UK, Nos 30562/04 and 30566/04, 4 December 2008, and the Bykov case considered below. I consider that this is a better approach than trying to fit in safeguards into the concept of "accordance with the law" which the Court has taken before in a number of earlier cases such as Rotaru v. Romania, No. 28341/95, 4 May 2000.
[20] Op. cit. para. 68.
[21] 20 May 1999.
[22] Compare Sunday Times v. UK, para. 49 and Maestri v. Italy, No. 39748/98 17 February 2004 with Cantoni v. France, 15 November 1996.

The Court is, however, aware of the difficulties of formulating laws. In Gorzelik and Others v. Poland,[23] the Court stated that "it is a logical consequence of the principle that laws must be of general application that the wording of statutes is not always precise. The need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. The interpretation and application of such enactments depend on practice … It must also be borne in mind that, however clearly drafted a legal provision may be, its application involves an inevitable element of judicial interpretation, since there will always be a need for clarification of doubtful points and for adaptation to particular circumstances. A margin of doubt in relation to borderline facts does not by itself make a legal provision unforeseeable in its application. Nor does the mere fact that such a provision is capable of more than one construction mean that it fails to meet the requirement of 'foreseeability' for the purposes of the Convention. The role of adjudication vested in the courts is precisely to dissipate such interpretational doubts as remain, taking into account the changes in everyday practice".[24]

Beyond the references to foreseeability and the need to frame laws and elaborate safeguards to avoid misuse of power, the Court has not elaborated in any detail what underlying values are protected by the "accordance with the law" requirement. The requirement is often seen as an expression of the "rule of law". However, insofar as it goes beyond the idea of rule *by* law, the content of the rule *of* law concept is the object of dispute. Basically, it seems to mean what the writer wishes it to mean and as such, it is of limited theoretical value.[25] Behind the idea of *statutory* law I would say are three values, foreseeability/stability, democratic legitimacy and institutional competence. As regards the first of these, the principle of norm hierarchy, expressed in Swedish law by RF 8:18, is that statutes can only be amended by statutes. A statutory regulation is thus both more stable and more transparent than regulation by means of subordinate legislation. As regards the second of these, little need be said. The idea of democracy is the steering principle of mainstream Western political organization for almost 100 years (and of huge influence in Western political thinking long before that).

[23] No. 44158/98, 17 February 2004.
[24] Ibid, at paras 64-65 (references omitted).
[25] Cf. Loughlin 2009.

The third value relates to the time and expertise which the parliament has at its disposal to devise appropriate general rules, and the completeness of the debate (taking into account all the relevant factors) which accompanies, or should accompany, discussion of legislative proposals. The Court has in the past paid insufficient attention to the value of regulation by statute law when it has considered the rule of law concept. There are presumably two reasons for this. First, as noted above, the Court accepts that general rules inevitably require judge-made law to interpret and develop them. Moreover, the UK and Ireland are "common law states" which accept, indeed welcome, that a large area of the law is judge made. One cannot "invalidate" large parts of the legal systems of two of the founding members of the Council of Europe. Second, in every European state, whether it has a parliamentary or presidential system of government, there is a very large amount of non-parliamentary produced legislation which is based either on delegated powers from the parliament or primary legislative authority for the government by virtue of the constitution.[26] However, as shown below, the Court, in the area of secret surveillance, has now begun to insist on *statutory* regulation of the area as a whole.

5 What is an interference with Article 8?

5.1 The content of Article 8

Article 8 guarantees four separate rights although there is a considerable amount of overlap between them. The same state measure can interfere in both e.g. "family" and "private" life or "home" and "correspondence".[27] "Family life" is not directly relevant to the present study, but the other three rights are. Article 8 refers to the right to "respect" for the listed rights. This means that not every measure *affecting* a listed right is an *interference* with that right.[28] I should also stress that the fact that something is found to interfere with (or "infringe") one of the Article 8 rights does not mean that it *violates* the article, simply that the infringement must be justified.

[26] Cf RF 813.
[27] One can argue that where the same measure constitutes an interference in both private life and the home it should be even more closely scrutinized. Cf. Ovey and White, 2006, p. 218 "the fact that [the rights] are grouped together in the same article strengthens the protection given by that article, because each right is reinforced by its context".
[28] Harris, et al. 2009 p. 381.

5.2 Home and correspondence

5.2.1 Generally

The "home" can extend to business premises under certain circumstances.[29] The planting of a listening device in the home[30], or using an agent or informer equipped with a listening device ("participatory recording" or "wearing a wire")[31] in the home is clearly an interference with Article 8(1). The "home" has been held to include a garage owned by the target in another locality than his home and another person's home which the target was visiting.[32] It seems fairly clear on the basis of this case law that even other types of listening devices, capable of picking up sounds at a distance, which are not physically *placed* in the home but are *directed* at it, will constitute an interference with the home.[33] Similarly, it may "safely be said" that the directing of visual surveillance against a person who is, at the time, in his/her home will be an interference with

[29] Niemietz v. Germany, 16 December 1992, A/251-B, paras 27–33. The Court also said in this case (which concerned search of a lawyer's office and seizure of documents) that "private life" can similarly include business activities. This approach is obviously sensible. The internet and developments in communication technology mean that many people can as easily work in their homes. The Court has confirmed this approach in a number of subsequent cases, e.g. Buck v. Germany, No. 41604/98, 28 April 2005. In Stés Est and others v. France, No. 37971/97, 16 April 2002, the Court went so far as to apply the protection of the "domicile" to the premises of legal persons "Building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises" (at para. 41).

[30] See the earlier Commission cases of Redgrave v. UK, No. 20271/92, decision inadmissible of 1 September 1993 and Govell v. UK, No. 27237/95, Report of 14 January 1998, Khan v. UK, No. 35394/97, ECHR 2000-V, paras 26-28 Chalkley v. UK, No. 63831/00, 2 June 2003.

[31] Heglas v. Czech Republic, No. 5935/02, 1 March 2007 (inadequacy of legal framework at the time regulating body-mounted listening devices and metering data), Bykov v. Russia, No. 4378/02, 21 January 2009.

[32] See respectively Hewitson v. UK, No. 50015/99, 27 May 2003 and Armstrong v. UK, No. 48521/99, 16 July 2002. See also Vetter v.France, No. 59842/00, 31 May 2005 (placement of microphones by police in the home of a person the target was visiting). On the other hand, in Hartung v. France, No. 10231/07, 3 November 2009, an actor's dressing room was not regarded as part of his "home". In *Bykov* the government argued that the guest house where the participatory bugging took place (see further below) was not part of the applicant's "home". The Court stated simply that the applicant's right to private life had been interfered with.

[33] Cf. the US cases concerning scanning residences from outside with thermal cameras in order to pick up unnaturally high heat emissions, which might indicate the presence of sodium lighting, used in growing marijuana plants, US v. Robinson, 62 F. 3rd 1325 (11th Cir. 1994) and US v. Kyllo, 9630333v2 (9th Cir. 1998). However, the US constitution 4th Amendment protects primarily against "warrantless searches", and in both cases, this practice was found not to constitute such a search.

Article 8(1).[34] However, as discussed below, such measures will, in most situations, also constitute an interference with private life.

"Correspondence" includes not simply mail and telephone usage[35], but also telegraphs, faxes and e-mail and internet usage.[36] Correspondence is not qualified by "private life" either, and includes therefore all sorts of correspondence, including that sent to and from the workplace.[37] In Halford v. UK the Court concluded that phone calls made on a closed telecommunications network, on business premises, fell within the notions of private life (and correspondence) and so could be protected from interception by Article 8.[38] The case concerned a senior police officer who had been passed over for promotion on a number of occasions and who had brought proceedings before an industrial tribunal alleging sexual discrimination. She later suspected that both her work and home telephone had been tapped in an attempt to obtain information useful against her in these proceedings. The respondent state admitted that her office telephone had been tapped. The Court noted that Halford had received no warning that her office telephone would be subject to interception, and that her "reasonable expectation of privacy" was reinforced by the facts that she had sole use of her office, that she had two telephones, one of which was specifically designated for her private use and that her employer had assured her in a memorandum that she could use her office telephones for the purposes of preparing her sex discrimination case.

A similar approach was taken in Amann v. Switzerland where the applicant, a businessman, had calls intercepted from his business premises[39] and in Copland v. UK which involved monitoring of a public employee's telephones and internet access at work.[40] Like the situation in Halford, the Court placed in Copland emphasis on the applicant's reasonable expectation of privacy: she had not been informed that her internet etc. usage could be monitored.

---

[34] Naismith, 1996, at p. 152. See further the Court's case law regarding photographing a person outside of the home discussed below.
[35] The Convention organs also accepted early on that the tapping of telephones was an interference with "correspondence". See Klass v. FRG, 6 September 1978, A/28, para. 40.
[36] See PG and JH v. UK, No. 44787/98, 25 September 2001, para. 42, Copeland v. UK, No. 62617/00, 3 April 2007 and Liberty v. UK, No 58243/00, 1 July 2008, below. As regards the issue of covert access to data located on a person's computer, or on a server, and not being transmitted, see below.
[37] PG and JH, ibid. and Niemietz, para 32.
[38] Halford v. UK, 25 July 1997, paras 42–46.
[39] 16 February, 2000, discussed further below.
[40] Op cit.

Still, it is clear that the Court considers that "correspondence" can be carried out outside of the home, and it must also be protected outside of the home.[41] In addition I can note here that the protection of correspondence has implications for associations. Whereas an association as such (as compared to its members) may not have a right to private life, it does have the right to correspondence.[42]

As regards obtaining information on the circle of persons or telecommunications addresses with which the target communicates (so called *metering information* or telecommunications data), the Court held as far back as 1986 in Malone v. UK that this is an interference with private life.[43] It should be noted that the type of data available from "metering" has changed considerably, with the advent of mobile phones and the internet. Mobile phones now give location data (considered below) and monitoring internet surfing gives information on the websites visited. I discuss later the type and degree of regulation required for accessing this data.

The Court has moreover stated that the *mere interception of telephone calls* in itself constitutes an interference with private life.[44] The fact that no *use* is made of the recordings is irrelevant. The Court has also stated, in connection with strategic surveillance (below) that the mere existence of this constitutes an interference with private life/correspondence of the affected persons (who may be a large part of the population). Similarly, one can argue that the data retention requirement for telecommunications traffic introduced by EC directive in itself constitutes an interference with private life.[45] The fact that a person knows that records of his or her internet surfing will now be made available to the police, and not simply be kept by his/her service provider for billing purposes, may well have an effect on the sites which they visit.

---

[41] The advent of mobile phones and laptop computers anyway makes it unrealistic to draw a distinction between telephone tapping and mail interception "inside" and "outside" the home.
[42] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No 62540/00, 28 June 2007 (Association could claim to be directly affected by a law which allows the use of secret surveillance measures, breach of Article 8).
[43] Malone v. UK, paras 83-88. The Committee of Ministers has also taken the position that this information should be confidential, except where it is necessary to reveal it for reasons of national security, law enforcement etc. Protection of personal data in the area of telecommunications services, with particular reference to telephone services, Recommendation no. R(95)4, para. 4.
[44] Kopp v. Switzerland, 25 March 1998, para. 37, see below.
[45] See Breyer, 2005. See further the discussion of why private persons' access to teledata does not raise the same sort of private life issues below in section 5.3.

There are three issues which require a more detailed treatment as far as "home" and "correspondence" are concerned. The first issue is when the state facilitates participatory audio surveillance.

5.2.2 Participatory audio surveillance

The regulation of this area has varied from state to state depending inter alia on whether the consent of all participants in a conversation is necessary before a tort or crime of revealing confidences is committed, or whether it is enough that one participant consents.[46] Prior to the Bykov case (dealt with below, in section 5.2.3), the leading Convention case on the issue was A. v. France. In this case, an informer had notified a high ranking police officer that he had been hired by the applicant, A., to kill someone. He offered to make a telephone call to the applicant and to record the conversation. The policeman agreed. The call was made in the policeman's office and recorded with a police tape recorder. The Court of Cassation had ruled in 1989, concerning a similar case, that only a judge could authorise the recording of a telephone conversation. The police could not do this by themselves during a preliminary investigation. The French government accordingly conceded that there was no basis under French law for the recording. The Court thus predictably found that the recording was not "in accordance with the law." The point of interest is, however, that the Court considered that, where the state *facilitates* this, a recording of a conversation by one private party was an interference with another party's right to correspondence. The approach was confirmed in the later case of M.M. v. Netherlands.[47] This case concerned the recording of a person's incoming, rather than outgoing, calls. A distinction can be drawn between simply facilitating the recording of incoming calls and the situation where the state could be said to have contributed to the making of incriminating statements, by encouraging one participant (A) in the conversation to ring up the other (B), and provided A with equipment to record any incriminating statements made by B.[48]

[46] For a brief comparison of the laws of five states in this respect see Joubert and Bevers, 1996, pp. 157–170. In Sweden, the crime of eavesdropping can only be committed by a person not party to the conversation (Criminal Code, Chapter 4, section 9a).
[47] No. 39339/98, 8 April 2003. See also the Bykov and Heglas cases, op. cit.
[48] See the dissenting judgment by Mrs Palm in the case and the separate judgment by Mr Mejyer in the later case of Van Vondel v.the Netherlands, Nos 38258/03 25 October 2007 See also two decisions of the Swedish ombudsman (JO 1996 dnr 1953-1995 and JO

The majority of the Court, however, seemed to make no such distinction, and one must assume that the majority does not regard it as a basis for justifying leaving unregulated the facilitating of recording of incoming calls. By way of comment, nowadays, the easy availability of equipment capable of making good quality recordings of telephone conversations would seem to render unnecessary any police involvement other than simply advising a person to record any threatening etc. calls. However, insofar as the police consider it useful to be able to facilitate in any way the recording of calls it seems clear that the Convention requires legal authority to do this.

One question which falls under this heading is whether it is necessary to have positive statutory authorization before giving the police access to a recorded telephone conversation between an individual and the emergency services (SOS Alarm). On the one hand, the person is, or should be, aware that such a conversation will be recorded. On the other, the recording is made for a specific purpose (to facilitate quick identification of exactly what the emergency is, and where it is occurring). In this respect, the situation resembles the situation of obtaining location or other teledata information from a phone operator (considered below in section 5.3.4).

5.2.3 Infiltration of the home

The second issue concerns whether sending an informer or an undercover agent into a person's home but without "wiring" them to make an audio or visual recording nonetheless constitutes an interference with that person's home. As shown below, private life extends outside of the home. Thus infiltration even outside the home can raise Convention issues. However, the arguments that the Convention requires regulation of infiltration are at their strongest when it involves entry into the suspect's, or a third party's, home.

One question here is whether the Court's judgment in the *Bykov* case constitutes a new approach. Previously, in Lüdi v. Switzerland,[49] the Court did not consider that the use of an undercover officer to approach the applicant to buy drugs was an interference with the

1997/98:118) which criticised state employees for recording their conversations with (abusive) private individuals without informing them of this. The ombudsman considered this breached the prescribed by law requirement in Article 8.

[49] No. 12433/86, 15 June 1992.

applicant's privacy. The Court appeared to take an approach similar to that taken by the US Supreme Court,[50] namely that a person engaged in criminal activity (X) implicitly waives his or her privacy when talking to another person (Y) as X should be aware that Y may be an informer or an agent.[51] Although the use of informers and undercover agents has arisen several times before the Court since the *Lüdi* case, to my knowledge, the issue of the use of infiltrators has arisen, but the question has always concerned the Article 6 issue (fairness of trial) rather than the Article 8 issue of whether the activity in itself constituted an interference with the home and/or private life. For example, in Ramanauskas v. Lithuania,[52] a Grand Chamber case dealing with agents provocateur, the Article 8 issue did not arise. There was an explicit statutory basis for the use of "operational simulation models" and the authorization procedure required the permission of the Prosecutor General or his/her deputy.

I think that the following points should be made. I do not think too much weight should be placed on *Lüdi*. The case was in 1992 and the Court treated the issue perfunctorily. Organized crime activities have apparently increased in European states since this time, and it is reasonable to assume that the use of informants and undercover agents to infiltrate organized crime has also increased. The problems involved in the use of informants and undercover agents have also become better known. For example, an infiltrator can be given access to premises by criminals unaware that s/he is working for the police. When unobserved, s/he is in the position to secure the same goals as an operation involving the use of traditional coercive open or covert measures (entry onto premises, search, seizure). Such measures, the Court has emphasized many times, must be under judicial control. However, by "outsourcing" these to an infiltrator, or by using an undercover agent, the way is opened to avoid existing safeguards.

As regards the link between surveillance and infiltration, a link which was present in the Bykov case, it is possible to make a distinction between the situation where a conversation with an informer/agent is recorded and a situation where it is not. In the former

[50] See Hoffa v. US, 385 US 293, 302 (1966) and Illinois v. Perkins, 496 US 292, 300 (1990). See further Ross, 2007, p. 505.

[51] "Mr Lüdi must therefore have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him" at para. 40.

[52] No. 74420/01, 5 February 2008. For examples of other recent cases see Sallinen and Others v. Finland, No. 50882/99, 27 September 2005 and Taxquet v. Belgium, No. 926/05, 13 January 2009.

situation, the recording will usually have a greater or much greater evidential value at a subsequent trial (some systems may not even allow the submission of an agent, or an informer's testimony regarding the content of a conversation with the accused). Having said that, the question is whether this distinction is relevant to the issue of the infringement of the home. In both cases, the person has obtained entry to the home, and the possibility to converse with the target, by using (active or passive) deception.

Different types of system of crime investigation and crime prosecution operate in European states. In some systems, e.g. the United Kingdom, under the Regulation of Investigative Powers Act 2000, the police themselves decide on the use of covert human intelligence sources, even where this involves infiltration of the home. One can also have a system under the control of the prosecutor, who, depending upon the constitutional system in question, can belong to either the executive or the judicial branch. A third method of control over infiltration measures is to require the approval of an investigating judge. This third method is likely to be perceived by the Court as the strongest type of control. Certainly, in *Lüdi*, the Court placed weight on the fact that the operation was under the control of an investigative judge. The Court may conceivably be less demanding as regards the explicitness of statutory authorization for infiltration where the judiciary is involved in authorizing infiltration which involves entry into the home (even if the reality of this control may vary from state to state).

One can argue that, in Sweden, the public prosecutor has a strong duty of objectivity, and, in many respects provides an equivalent level of protection to that of an investigating judge. Nonetheless, s/he is, constitutionally speaking, part of the executive power. Moreover, the Prosecutor General is a government appointee. The Prosecutor General, or a chief prosecutor, does not have power to influence how a subordinate prosecutor reaches his or her decision in an individual case, but does have the power to take over the case or reallocate the case to another prosecutor. In practice, by virtue of the constitution (RF 11:7, after 1 January 2011, RF 12:2) the Swedish prosecutor has strong guarantees of independence from direct government control in an individual case. Moreover, the Code of Judicial Procedure (see in particular Chapter 20) directly gives a prosecutor in charge of a case the decision-making power over that case and Swedish legal culture (backed up by strong constitutional protection of freedom of Information and freedom of expression)

provides protection against improper removal of a prosecutor from an individual case by the Prosecutor General. However, it should be admitted that, on paper, the structural safeguards in Sweden are relatively weak.

But in any event, the Swedish prosecutor is not in charge of all investigations into crime or even the majority of these. Even as regards more serious crime, where the prosecutor will invariably be involved, the prosecutor might well come in at a later stage, after an infiltration operation has been run by the police.

As mentioned, in the UK, precisely because the police themselves decide upon infiltration the decision was taken in 2000 to introduce an explicit statutory basis for all use of covert human intelligence sources, together with a code of practice and a system of hierarchical authorization and control within the police.[53] The UK system also deals with the problem of establishing the threshold of "infiltration", in other words, of distinguishing this from "ordinary" use of informers or plain-clothed police simply observing people or crime scenes. One naturally does not have to choose the British model. A variety of models can be used, but the important thing would appear to be the criteria of direction and control.

Another relevant issue to take into account is the state's rules for excluding evidence to ensure the fairness of the trial. While the issue of statutory regulation is separate from the issue of fair trial, the two issues are nonetheless clearly linked in that it is the end result in which the Court is interested. Thus, something must be said about it, even if I do not need to go into this issue in any detail

[53] The UK Covert Human Intelligence Sources Code of Practice provides that:
4.1 Under section 26(8) of the 2000 Act a person is a source if: (a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c); (b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or (c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
4.2 A source may include those referred to as agents, informants and officers working undercover.
4.3 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
4.4 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as mentioned in paragraph 4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
4.5 The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.
(at p. 20, http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/human-cop2835.pdf?view=Binary

in the present report. The Court ruled in Teixeira de Castro v. Portugal[54] and subsequently in a number of other judgments and decisions[55] that when an infiltration operation has been used, the trial court must consider whether this undermines the fairness of the trial. Where police undercover agents or informers have gone so far as to behave as agent provocateur, the evidence must be excluded. As regards the question of leading evidence which has been obtained in breach of a substantive right under the Convention, so far it seems that only where evidence has been obtained by torture will this *automatically* mean that the trial violates Article 6.[56]

Thus, the Court – so far – has excluded the "fruits of the poisonous tree doctrine" as a means of compelling the police to comply with substantive Convention rights. The Court is aware that, like procedures for authorizing infiltration, evidential systems vary considerably from state to state. The Court is also aware that the efficacy of the mechanisms states have for ensuring that the police follow the rules vary considerably, as do the sanctions on the police for not following the rules. But the very fact that the fruits of the poisonous tree option has been excluded argues for the Court, in future, taking a tougher approach on the issue of statutory regulation of infiltration which is within the scope of Article 8, or on the borders of it.

As it is the end result which is important, the Court may be prepared to give a "freer hand" as regards to a system with strong guarantees at the trial stage (and, correspondingly, less of a free hand to a system which does not exclude evidence). This is supported by the recent case of Uzun v. Germany,[57] concerning the covert placing of a GPS receiver into a car, where the Court weighed in subsequent court discretion to exclude evidence at the trial stage in its analysis of whether the German regulation of GPS as a location device was "in accordance with the law".[58]

---

[54] 9 June 1998.

[55] See in particular, Sequeira v. Portugal No. 73557/01, ECHR 2003-VI, Taal v. Estonia, No. 13249/02, 22 November 2005, Vanyan v. Russia, No. 53203/99, 15 December 2005, Eurofinacom v. France (dec.), No. 58753/00, ECHR 2004 VII, Khudobin v. Russia, No. 59696/00, 26 October 2006.

[56] See Jalloh v. Germany, No. 54810/00 11 July 2006 (GC) and Gäfgen v. Germany, No. 22978/05, 1 June 2010 (GC), the latter case dealing with the effect on admissibility of evidence of threats of physical harm made by police interrogators.

[57] No. 35623/05, 2 September 2010.

[58] At para. 71. See also Khudobin v. Russia, op. cit. "the Court recalls that a clear and foreseeable procedure for authorising investigative measures, as well as their proper supervision, should be put into place in order to ensure the authorities' good faith and compliance with the proper law-enforcement objectives…. In the present case the police operation had been

Here, one can note that while there is practice from the Swedish courts on the issue of maintaining equality of arms and otherwise ensuring fair trial, including cases concerning agents provocateur,[59] the basic principle of Swedish evidence is the free admissibility of evidence. While it may sometimes be necessary to exclude evidence, simply put, I would say that it is not desirable to make this a "standard" part of the Swedish trial system.

There are other reasons for regulation. The principle of legality which applies for prosecution would also seem to entail some form of regulation of the situation where an informer or undercover agent breaks the law as part of an infiltration operation. And there are obviously drawbacks from the perspective of legal security (*rättssäkerhet*) in focusing on safeguards at the trial stage, as many infiltration operations may never get to trial. Finally, as already mentioned, the increased international cooperation (particularly assistance based on the principle of mutual recognition) means that there is a heightened need for improved clarity in the law, and for explicit safeguards against misuse.

Thus, while it cannot be said that the Convention case law at this stage definitely requires a statutory basis for infiltration operations which affect (if not actually interfere with) the home, the factors sketched out above argue for introducing this in Swedish law. The sensible approach is to provide for a "layered" system of authorization, whereby infiltration operations which affect the home (or private life outside the home, see below) in a minor way might only require a higher level of police authorization (i.e. a decision by a senior officer). Operations affecting the home or private life outside the home in a more major way would require prosecutorial authorization and, conceivably, even judicial authorization.

As regards involving the prosecutor in the process, one can argue that intelligence gathering is something for the police, and it is first when it becomes "evidence" that the prosecutor should be involved. But this distinction is not always strong in practice. I think there is a definite value in requiring prosecutorial authorization as regards

---

authorised by a simple administrative decision of the body which later carried out the operation. It transpires from the materials of the case that the text of that decision contained very little information as to the reasons for and purposes of the planned "test buy". Furthermore, the operation was not subjected to judicial review or any other independent supervision. In the absence of a comprehensive system of checks accompanying the operation … the role of the subsequent supervision by the trial court became crucial."

[59] See e.g. RH 1995:32, NJA 1996 s 649, RH 1997:95, NJA 1998 s 204, NJA 2003, s. 323, NJA 2007 s 1037, NJA 2007 s 547, NJA 2009 s 475.

the most "serious" infiltration. There is a value in making the police "go outside of the house" to convince a person who is "one stepped removed" from the investigation of the need to take a particular measure. While the police are expected to obey the law, it is fair to say that the prosecutor, by reason of her training, peer group and organizational pressure, is expected to, and does, hold herself to a very high level of law obedience.[60] Moreover, the prosecutor is used to balancing restrictions in rights against the need for effectiveness in crime investigation and prosecution. I do not need to go more into these issues. Suffice to say that a variety of different types of regulation are possible here. A layered system of authorization is not inflexible. Even for infiltration operations at the "serious" end of the scale, emergency situations can obviously arise (spontaneous opportunities for infiltration etc.). But these are unlikely to be the norm and they can be handled by some system of retrospective authorization.

As to whether involving the prosecutor is sufficient in the event that the Court later makes it clear that infiltration can breach the protection of the home/private life, I can note that, according to the Court's case law, the Swedish prosecutor does not suffice as a sufficiently independent control over arrest and detention.[61] Moreover, it is true that there are weaknesses on paper in the Swedish prosecutor's independence from executive control. However, there is no doubt about the prosecutor's independence from the *police*, nor about the prosecutor's ultimate ability to control the police in the context of an investigation (*förundersökning*) when and if she wants to do so. Finally, the standards as regards Article 8 are more variable than those of Article 5. As far as concerns infiltration of the home not involving recorded surveillance (considered further below), it *may* be sufficient to give the infiltration a statutory basis, and establish the first two layers of authorization and control namely authorization by a senior police officer and authorization by a prosecutor – as long as the trial court, applying the principle of proportionality, has the discretion to exclude evidence obtained in an "unfair fashion" in subsequent proceedings.

On the other hand, in the recent Uzun case, the Court explicitly stressed that it was prepared to accept such a system sketched out above (i.e. no judicial authorization) only because the covert placing of a GPS receiver into a car, involved a lesser degree of interference

[60] See also below, section 6.4 on the value of precise rules.
[61] McGoff v. Sweden, 26 October 1984, A/83.

in privacy (considered further in section 5.3.4). The implication is then that the authorization of major interferences in privacy require stronger, i.e. judicial, controls.

5.2.4 Strategic surveillance of radio-borne communications

The third issue relates to the interception of either the content of telecommunications traffic or telecommunications data carried by radio waves. This can be either of specific communications, or general "strategic" bulk surveillance. An argument can be made that, as the "ether is free", there can be no expectation of privacy when radio is used. Thus, any interceptions of telecommunications traffic carried by radio waves cannot involve an interference with Article 8(1). As regards bulk interception of telecommunications data, or of strategic surveillance of the content of conversations, one can in addition argue that there is no identification, or at least, no initial identification, of the identity of the people communicating, and so no interference with private life or correspondence.

There is some support for this proposition in older case law. In B. C. v. Switzerland, the applicant had used a cordless phone which transmitted on a radio frequency reserved for civilian and military aviation traffic. This was an offence under Swiss law. The Swiss telecommunications authority recorded his conversations and used radio directional finding to locate his phone. The Commission considered that, as the applicant chose to employ a device using a wavelength reserved for purposes other than private telephone communications, his conversations were "thus accessible to other telecommunications users and so can scarcely be classified as … private".[62]

However, this case is no longer authority (if it ever was) for regarding interception of normal mobile phones, transmitting on lawful frequencies, as not being an interference with Article 8.[63] There is a huge difference nowadays between the vast numbers of people

[62] No. 21353/93, 80 DR 101 (1995) at p. 105. The Commission also added that the contents of the intercepted messages were not revealed. This last point can be misleading bearing in mind the Court's view in Malone, that the state retaining even metering information in the absence of statutory authority was a violation of Article 8. Another case concerning unlawful mobile phones was decided by the Court, but the issue here was only the lawfulness of the search of the applicant's home (Caminzind v. Switzerland, 19 December 1997).

[63] There is another case, X. and Y. v Belgium, No. 8962/80, decision of 13 May 1982, where the Commission left open the question as to whether radio communications between two people could be protected by Article 8.

who communicated by "radio" today and the very small numbers of people who communicated by short wave radio in the 1980's. Anyone with a mobile phone or using a cordless internet computer connection is communicating by "radio". Moreover, even cable borne telecommunications can be routed via microwave. However, one cannot argue, as with short wave radio, that a person using a laptop or a mobile phone "knows" that he or she can be listened to. Microwave radio traffic in digital form is not capable of being picked up and understood by anyone with a radio receiver. It would make a mockery of a system for tightly regulating monitoring of cable borne traffic if one can circumvent this system by intercepting the content of messages at the point when these are converted into microwaves.[64] Moreover, as shown below, the Court does not regard whether or not a "reasonable expectation" exists to be conclusive to the issue as to whether something is an interference with private life.

Even if correctly decided at the time, the BC case is no longer good law. In the two recent cases concerning the issue, Liberty v. UK and Weber and Saravia *v.* Germany the Court drew no distinction between on the one hand, the interception of telecommunications data or the content of communications carried by cable and on the other hand, the same types of interception of microwave borne traffic. In both cases, interceptions had taken place of both cable and microwave traffic. In both cases the Court considered that the interceptions involved an interference with correspondence/private life. It should also be noted that the Court in Weber and Saravia also found that the transmission of data from intercepts to, and their use by, other authorities constituted a *separate* interference with the targets' rights under Article 8, as did the destruction of the data, and the refusal to notify the targets.[65]

[64] One can even envisage the construction of communications systems which build in such a microwave component for precisely this purpose, even though this is probably technically and economically speaking impracticable.

[65] Op.cit, para. 79. In Liberty and others, the Court contented itself with stating that it "considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied" (para. 57).

5.3 Private life

5.3.1 Generally

Whereas correspondence and the home are relatively simple to understand, "private life" is difficult to define. The Court in fact considers that it is a "broad term not susceptible to exhaustive definition".[66] It has so far contented itself with stating what it includes; "activities of a professional or business nature", "the right to establish and develop relationships with others even in a public context", "the physical and psychological integrity of a person", "the right to … personal development and the right to establish details of their identity as individual human beings."[67] As will be shown below, a wide approach to the concept of private life is not necessarily problematic for public authorities, as the Court can balance this by a flexible approach to the issues of accordance with the law and necessity in a democratic society. In the context of surveillance, a wide approach to privacy does certainly not mean that surveillance cannot occur. The Court made it clear as far back as Lüdi v. Switzerland that a suspected criminal cannot argue that his or her conversations are absolutely protected against recording.[68]

As regards surveillance, it can be said that the underlying reason why the Convention protects privacy is because privacy is necessary for the development and maintenance of an individual's personality.[69] But at stake is also the culture of the society itself. To take a simple example, what sort of society will you foster if you expect people to "watch what they say" every time they answer their mobile phone?

Another argument relates to level of intrusion. While covert electronic surveillance is, in one sense, less direct and humiliating than more traditional state intrusions on privacy such as an overt, disruptive search of the home, in another sense it is more intrusive than such a search because it usually lasts longer, is more indiscriminate and open-ended and affects more people.[70] Moreover, when the product of covert electronic surveillance is used, e.g. in security

[66] Peck v. UK, No. 44647/98, 28 January 2003, at para. 57.
[67] Moreham, 2008, p. 45 and references therein.
[68] Lüdi v. Switzerland, op cit.
[69] As de Hert puts it: "The fundamental right to be human is touched and threatened if all our actions are being scrutinized, because of the simple fact that we behave differently when we are observed", de Hert, 1997, p. 560, footnotes omitted. The Convention jurisprudence on the matter began with the famous "Icelandic Dogs" case, X v. Iceland, No. 6825/74, 5 DR 86 (1976).
[70] Lustgarten and Leigh, 1994, p. 51.

screening, or to justify more overt and intrusive state measures (e.g. arrest, search of a house) it will obviously affect the targeted person. The product may give an accurate picture of the situation – that the target is involved in crime – or it may give an inaccurate picture. Either way, the potential it has for deeply affecting a person's life means that it must be subject to controls.

While some issues are very clear from the Court's case law, there are four which require a more detailed treatment. The first three of these issues concern *when*, and *under what conditions*, aural, visual and location-information surveillance of a person in a public place, or a private place not forming part of the "home", are covered by private life? The fourth question relates to whether access to personal information on a person which is stored on a computer not his or her own involves an interference with that person's private life. In the following sections I consider these issues. As explained below, I think it is possible to draw a distinction between photographing/secret visual surveillance on the one hand and secret audio surveillance on the other. I therefore begin with visual surveillance, which is also the topic which deserves the most detailed treatment.

5.3.2 Private Life in non-private zones: visual surveillance

The Court has found on a number of occasions that visual surveillance in public places – still camera pictures or moving pictures – can constitute an interference with private life. The Court has stated that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".[71] The initial approach of the Convention organs to the issue of visual surveillance in public places is shown in Friedl v. Austria.[72] This case concerned police observation of demonstrators, and the Commission held that simply photographing a person in a public place is not an interference with private life.[73] The Commission stated that three factors were

[71] Perry v. UK, No. 63737/00, 17 July 2003at para. 37.
[72] Friedl v. Austria, No. 15225/89, report adopted 19 May 1994. The case was settled before the Court. The government paid compensation to the applicant, and agreed to destroy the photographs taken.
[73] One can argue that the freedoms of expression and assembly set out in Articles 10 and 11 should be part of the interpretative context here. These rights are of particular importance for open societies (cf. RF 1:1 st. 2). Photographing by the police can undoubtedly affect a person's willingness to take part in a protest, even if this measure does not go so far as to restrict the right. This in itself strengthens the argument that, while photographing of

relevant in deciding whether there was an interference with private life: first, "whether the taking of photographs amounted to an intrusion into the individual's privacy, whether it related to private matters or public incidents, and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public".[74] The first factor seems to beg the question but can presumably be connected to the idea of a "reasonable" or "legitimate expectation of privacy". Where people meet in a public place they can attempt to conceal the fact of their meeting by choosing a remote, quiet, dark or deserted area. But the risk of being seen will almost invariably exist. Telephoto lenses mean that even meeting places chosen some distance from other people can be observed. One can argue that there will rarely be a "legitimate expectation" of not being seen. However, a "legitimate expectation" of privacy is obviously a shifting standard. The continual sophistication of surveillance technology means that, soon, objectively speaking, a person can never have a "legitimate expectation" of total privacy. Thus, I would say that too much weight should not be put on this factor. As shown below, nor does the Court.

In any event, it was clear in Friedl v. Austria that the photographs were taken openly, not secretly and the activity – the demonstration – was *meant* to be seen. Moreover, the photographs taken were not used to identify individuals. The Commission accordingly found no interference with private life. As shown below, however, subsequent cases have sharpened the requirements on states.

In Murray v. UK, the applicant was arrested in her home by soldiers who suspected her of involvement in terrorism.[75] She was later photographed at a detention centre, without her knowledge or consent. The Court stated that this taking of photographs was an interference with the applicant's private life. The fact that the applicant had been taken from her home was presumably important to this finding, but so too was the fact that the photographing occurred without her knowledge. However, another important factor was the use to which the photograph was put, as part of an individual file. Similarly, in Tsavachidis v. Greece, the applicant had been systematically "shadowed" and observed by state agents and extensive

demonstrators must be possible, it should require positive lawful authority. Further consideration of this issue is outside of the scope of the present report.

[74] Ibid, at para. 48.

[75] 28 October 1994, A/300-A.

information had been collected on his activities. The Commission considered this to be an interference with private life.[76]

In P.G. and J.H. v. UK the Court confirmed the approach in Tsavachidis and stated that: "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."[77]

In Allan v. UK,[78] a person suspected of a crime who had refused to answer questions was surreptitiously filmed and recorded in his cell and the prison visiting area. This was regarded as an interference with his private life.[79]

In other cases, the Court has laid weight on the *unexpected* or *unreasonable* use of film and photographs which were taken of publicly observable activities. Perry v. UK concerned a person who had been filmed by CCTV cameras in a police custody room, in order to obtain film for use in an identity parade. He knew, or at least could be assumed to have known about the CCTV cameras, but the Court considered that "there is no indication that the applicant had any expectation that the footage was being taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial".[80] It was

[76] No. 28802/95, 28 October 1997. The case obviously has implications for any form of systematic and covert state collection of publicly available information on an individual. See below.
[77] At para. 57
[78] No. 48539/99, 5 November 2002.
[79] See also Van Der Graaf v. Netherlands, No. 8704/03, Decision 1 June 2004. Placement of detainee under permanent camera surveillance for a two week period was an interference with private life, but in the circumstances justified as in accordance with the law and necessary in a democratic society: inadmissible.
[80] Op. cit. at para. 41. The Court added: "The normal use of security cameras *per se* whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8(1) …Here, however, the police regulated the security camera so that it could take clear footage of the

thus an interference with private life. Police use of filmed identity parades was regulated not by a statute but by a simple code of practice. However, the national court (at Peck's trial) had found that the police had not complied with this code. The Court found therefore that the interference was not "in accordance with the law".

Peck v. UK concerned a person who had been filmed on CCTV cameras on a street and whose behaviour indicated that he intended to commit suicide. The footage enabled CCTV operatives to alert the police in time and who helped saved his life. The footage was later distributed to the press by the local authority where the filming took place as part of a public relations exercise designed to show the benefits of CCTV surveillance, something which caused the applicant considerable distress. The Court stated that "The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life".[81] However, the Court added that "On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations."[82] It went on to find that the retention of the data did give rise to an infringement of private life. There was a clear statutory power for the local authority to use CCTV. However, the Court found a violation of Article 13 (effective remedies) because the applicant had no effective means of challenging the retention and dissemination of the images taken.

Another case in which a violation was found was Sciacca v. Italy.[83] This was because of the absence of a legal basis for the handing over to the press by the police of a photograph of a person under house arrest.

The case of von Hannover v. Germany[84] can also be mentioned. This concerned a positive duty upon the state to prevent the publi-

applicant in the custody suite and inserted it in a montage of film of other persons to show to witnesses for the purposes of seeing whether they identified the applicant as the perpetrator of the robberies under investigation. The video was also shown during the applicant's trial in a public court room …This ploy adopted by the police went beyond the normal or expected use of this type of camera, as indeed is demonstrated by the fact that the police were required to obtain permission and an engineer had to adjust the camera. The permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant."

[81] At para. 59. The Court referred to Herbecq and Another v. Belgium, Nos.32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92.

[82] Ibid.

[83] No. 50774/99, 11 January 2005.

[84] No 59320/00, 24 June 2004.

cation of photographs taken by paparazzi and as such is not directly applicable to open or covert photographing by the police. However, the case is further support for the view that one can clearly have a private life in public. The Court referred to the photographing of the applicant when she was engaged in activities of a "purely private nature". The German constitutional court had considered that where the applicant objectively speaking had sought a secluded area, then she had a right to privacy and it had accordingly considered that it was permissible not to permit the publication of photographs of her in such an area. However, other photographs could be published. The Court however, stated that the public "does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public."[85]

Reklos and Davourlis v. Greece[86] concerned the photographing of a newborn baby without the prior agreement of his parents and the retention of the negatives. The Court found this to be in violation of Article 8. It stated (at para. 40) that "A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image. Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person. As a person's image is one of the characteristics attached to his or her personality, its effective protection presupposes, in principle and in circumstances such as those of the present case … obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published. Otherwise an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image."[87]

[85] At para. 76. See now RF 2:6 st. 2 (after 1 January 2011).See also Verliere v. Switzerland, 28 June 2001.
[86] No. 1234/05, 15 January 2009.
[87] Where there is a countervailing interest, in particular, freedom of expression, then the two interests have to be balanced. The Court has repeatedly disproved decision of the Austrian courts to restrict journalists' publishing of photographs of politicians on the basis that the

Lastly, another case can be mentioned, Wood v. Commissioner of Police for the Metropolis.[88] While this is an English case, it has some relevance, because the Court of Appeal applies Article 8 of the Convention (which, as in Sweden, is incorporated into law). The case concerned the police taking of a photograph of a prominent campaigner against the arms trade at a demonstration. The police had feared that there might be violence at the demonstration. This did not materialize. The basis for the taking of photographs was the common law (i.e. not statutory) power of the police to maintain public order. The appellant in the case was aware of the photograph and subsequently requested that it be destroyed, but the police refused. The Court of Appeal did not consider that the mere taking of the photograph engaged Article 8. However, the circumstances indicated that there was no basis for bringing a prosecution against the applicant either for his acts at the time, or for his acts at a subsequent demonstration shortly after. The photograph appeared to be being retained for general intelligence purposes, as it identified the appellant and some of his acquaintances. The Court of Appeal considered that the photographs together with the fact that they were retained without explanation involved an interference with privacy.

The Court proceeded to rule that the common law power to maintain public order was sufficient legal basis for taking the photograph and so it was "in accordance with the law". However, the majority of the court considered that there was a lack of proportionality in the retention of the photographs. LJ Dyson considered that, where the aim in retaining photographs was protecting the community from public disorder or low-level crime, a more compelling justification had to be adduced than would be the case for retention of a photograph for the purpose of protection against terrorism or really serious criminal activity.[89]

Summarizing these cases, I think that the following can be said.[90] With a certain reservation for the Reklos and Davourlis case, which

politicians have intellectual property rights in their own images. See e.g. News Verlags GmbH & CoKG v. Austria, No. 31457/96, 2000, Krone Verlags GmbH & Co KG v. Austria, No. 34315/96, February 26 2002, Osterreichischer Rundfunk v. Austria, No. 35841/02 7 December 2006.

[88] [2009] EWCA Civ 414 (21 May 2009)
http://www.bailii.org/ew/cases/EWCA/Civ/2009/414.html

[89] At para. 86.

[90] I will not go into the question of weighing integrity protection against the constitutional rights to freedom of information and expression under Swedish law as far as recording of visual data by private persons, for private purposes is concerned.

can be interpreting as setting a new standard for simple photographing, it would appear that as regards both covert and overt photographing or filming by the police, by any technical means, it is not the activity in itself, but the retention of the record, or its insertion into a file, or its dissemination to other public authorities or private bodies which constitutes the interference with private life. Formally speaking, the origins of the photograph, film etc. are not important. The legal nature of the body actually engaged in the recording by technical means (photographing, filming etc.) public, quasi-public or private corporation, is irrelevant.[91]

Thus, for overt (open) filming or photographing, the police must be in a position to justify the retention of the photographs or films, when and if people complain about this. Accordingly, legal authority for the retention of visual records made with technical means together with safeguards (considered in the next section) must be put in place. For covert filming or photographing, the targets, and whatever other people are captured on film, will presumably not know about this. However, even here, there is an interference with private life as soon as the photographs are retained even if the "victim" does not complain. As people are not in a position to complain about these interferences some alternative form of oversight mechanism must exist. Some form of legal authority must also exist for the dissemination in any way of recordings made by technical means, whether overt or covert.

There is no evidence that the Court considers there is a distinction between digital or print retention of data. To draw such a distinction is likely to encourage the circumvention of rules. Having said this, digital storing of pictures obviously has the potential to increase greatly availability of the pictures, meaning a greater potential for unauthorized access and dissemination, with corresponding risks for damage to personal integrity.

One question which is not yet fully answered is whether the Court sets a threshold of "processing" the data on an individual level in the case of covert photographing. In other words, is it first when the photograph/film is put in a file opened on an individual that an interference with private life comes into being? The problem with such an approach is also that it allows circumvention, e.g.

[91] In e.g. Woods, the photographs were taken by a private photographer, contracted by the police. Using private bodies to collect visual, audio or other data can result in special problems of legal control, e.g. if one private corporation is used to carry out interception of communications services offered by another private corporation. Such problems can raise issues both as regards the quality of law (precision etc.) and as regards the working of safeguards.

"working" files, or "place" files or "theme" files can be created without definitive identification of individuals.

The Court referred to "permanent *or* systematic" records in Peck (my emphasis). Digital film or photographs are "permanent" as compared to CCTV which does not record, or where the recordings are automatically wiped by being recorded over after a few days. Such an interpretation would mean that any covertly or overtly taken digital images of even unidentified people which are transferred to a computer or printed out could be regarded as infringing these persons' private lives.

In one respect this seems unreasonable. There will be many situations in which the police have taken visual records of large groups of people, e.g. alleged football hooligans, or demonstrators committing offences of violence, where identification is only possible at a later, or much later stage. The police may have a fairly good idea who a particular demonstrator is, without being able definitively to identify him or her. The police can have good reasons for retaining such records for some time, pending definitive identification of the alleged offender.[92] In the circumstances, it seems unreasonable to regard there as being an ongoing interference in that person's private life, if the visual records are not individualized. On the other hand, existing data protection rules anyway require an evaluation to be made regarding the necessity of filing any personal data, before such filing is allowed.

Whatever the view that is taken on this point, one sees very quickly that there is an interference in that person's private life if this visual record of an as yet unidentified person is disseminated in any way – to the press definitely (see, e.g. the Sciacca case, above) but also conceivably to other authorities (e.g. social workers, as regards young people) or even private persons such as football supporter clubs (e.g. to ask for help in identifying the person in question) or the organizers of a protest demonstration (e.g. to warn them to be on the look out for this person who may wish to cause trouble). This is not to say that the police may not have good reasons for disseminating the visual record, nor that this is in breach of the Convention. These examples simply make it clear that a visual record of even an unidentified person can potentially involve an interference in private life.

[92] Where a conspiracy is long-term, such as can be the case for organized crime or security crime, the period can clearly be longer.

I would say that the sensible approach would be to concede that the police must be granted a large amount of discretion in determining at what point a visual record becomes sufficiently individualized to become an interference in private life. And precisely because there must be discretion, it is necessary to provide some form of external oversight and control of the working of this discretion.

The practical result of all this is that, while the actual recording of images – the pushing of the button – does not constitute an interference with private life, it might as well be the case that it is. This is because as soon as the button is pressed, the police must be in a position to point to legal authority for the retention of the record made to an external body entrusted with oversight of police records.

I should note that this does not mean that there is now a distinction between "old fashioned" police work – following people, noting their movements and circle of contacts etc. – and the same type of work carried out by technical means. Inter alia the Tsavachidis, Amman and Rotaru cases make clear that even the former constitutes an interference with private life, when it leads to the *systematic collection* of intelligence on a given individual.

5.3.3 Private Life in non-private zones: aural surveillance

A number of states have constitutional protection of the home, but not of "privacy" as such. This has been used to justify leaving recording conversations by technical means outside of the home unregulated, or at least, subjecting it to a lower degree of regulation. However, it seems now quite clear following *Bykov* that the Court regards this as an interference with private life. Although *Bykov* concerned participatory audio surveillance, there is no reason not to hold that *any* technical means to pick up conversations, e.g. directional microphones, or manually, or remotely, converting a mobile phone to a recording device and switching it on, will also involve such an interference. As mentioned, the Court held in *Kopp* that here the interference is constituted by the simple recording, whether or not it is used for anything (intelligence or evidence). This tougher approach can presumably be justified by the greater expectation of privacy that two people (A and B) can have if they are whispering to one another in a public square, at a distance from other people. Having said this, I should once again note how slippery this criterion is: when everyone has a mobile phone, which can be

turned into an aural, or visual, recording device at the flick of switch, this must presumably affect even A and B's "legitimate expectations" of privacy. It is, at any rate, sufficient to note that the Court clearly regards covert aural surveillance of a person outside the home as an interference in that person's "private life" whether or not that person can be said to have a "reasonable expectation of privacy".

5.3.4 Location information

I will turn now to location information. I can deal with this issue very briefly. As noted in section 2, this takes different forms. Mobile phones, even on standby, continually make available location information to base stations, allowing the general plotting of a person's movements. A mobile phone can also be remotely activated, allowing tracking even when the person possessing it considers that it is switched off. Key cards indicate where and when a person has entered given premises, or a zone. Bank cards indicate where and when a person has made a transaction. The development of RFID (Radio Frequency Identification) technology, whereby accessories or clothes can be "tagged" with electronic identifiers, means that a person having or wearing anything with such a tag can be located. Different types of sensor can be planted to register entry into, or movement in, a given area.

One can argue that certain types of location information, in particular, accessing ("emptying") of all traffic registered in a mobile base station during a particular period does not involve an interference with a *particular person's* private life. However, it is clear that the purpose and effect of the measure is to identify exactly which persons *could have been* present in a particular area at a given time.

One can nonetheless take the approach that information on where a person has been, or even, in real time, where that person is just now, should not usually be seen as sensitive. If I accept that my mobile phone operator can track me, or that my bank knows instantly where I am if I make an electronic transaction, then why is it an infringement of my privacy if the police also have access to this information?

This argument goes more to the *severity* of the interference, not whether it is an interference at all, and as such relates to the type and degree of regulation necessary, considered below. However,

two points can be made here. First, I have *chosen* to let my mobile phone operator, or bank, have access to this location information *for their purposes* (purposes which also serve my own – ease of communication and security in banking transactions).[93] A model of "concentric circles" of privacy can be used here.[94] The individual has an interest in determining, or at least influencing, who has access to such information, and for what purposes. I have not chosen to let the police, or the tax authorities, or my child's school, or my employment officer, know where I am at all times. The legislature may decide that the interests of society in letting the police find out, in an individual case, where a person has been or where s/he is now outweigh that person's interests in keeping his/her movements secret. But this is not the same thing as saying that s/he has no interest in keeping his/her movements secret from the police or any other state authority.

Second, the *systematic* collection of this information allows the state to build up a much larger picture of a person's private life than is possible for any private actor.

I conclude that if information on the numbers dialed and duration of a telephone call is an interference with private life, it would seem to follow that obtaining "location information" on a person, manually or remotely, by following mobiles, reading keycards etc. will also be interferences in private life.

The Court in the Uzun case has recently dealt with the question of whether the attaching of a location-sending device to a car, constitutes an interference with private life. A location device can give information equivalent to following a person's mobile phone, when it is planted in a person's private car. In the Uzun case, a GPS receiver was planted in the car of the applicant's accomplice, and this enabled the police to follow the two suspects and build up a picture of their movements over a period of three months. It also facilitated aural surveillance (shadowing) of them, which in turn made it possible to gather further evidence. The Court stated that "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's

[93] Cf The Court's statement in PG and JH, op. cit "metering, which does not *per se* offend against Article 8 if, for example, done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications which may be undesirable and illegitimate in a democratic society unless justified" at para. 42.
[94] See, e.g. Nagel, 1998.

conduct, opinions or feelings"[95] It nonetheless came to the conclusion that this did constitute an interference with private life.

One can argue that it does not automatically follow from the Uzun case that any and all uses of GPS receivers and similar devices involves an interference with private life. In Uzun the target was identified and the purpose was surveillance of this target. The situation is arguably different where a GPS receiver or other sensor is attached to an alarm or to an object hidden somewhere, say a hidden weapons cache, stolen goods, or a bag containing ransom money in a kidnap case. Having said this, where the sensor is connected to more sophisticated equipment which can involve identification, e.g. the device is capable of taking pictures when triggered, the situation could be different.

One can also distinguish the facts of the Uzun case from the planting of such a device in, e.g. a container, when the police or customs want to follow stolen, smuggled or counterfeit goods. The purpose here will most often be simply to follow the goods in question.

A third situation argubably different from the facts of the Uzun case is where the police assist the owner of a vehicle to secure the return of a stolen vehicle (or vice versa). Many expensive cars and trucks already have GPS devices fitted, which can be used as an anti-theft device, enabling the owner and/or the police to follow a stolen vehicle.

Nonetheless, even if one can argue that the use of a GPS receiver in such circumstances does not involve an interference with private life, it obviously facilitates visual observation.[96] And where permanent and/or systematic records are kept of such visual observation, then there is an interference. Moreover, there is the risk of abuse to think about: when one type of use of a GPS receiver is within the discretion of the police and another type is not, there are obvious dangers that the area of application of the former category is extended in practice. The sensible approach would seem to be to regulate all police uses of GPS receivers on a similar basis to teledata.

[95] At para. 52.
[96] Compare the points made above in section 5.2.2 regarding participatory audio surveillance.

5.3.5 Digital private spaces

The final issue in this section relates to whether it is an interference with a person's private life to access his or her "private space" on a server. It is clear from Copeland and other cases that the monitoring of a person's internet *access* will constitute an interference with his or her private life. I would say that this must extend to the police accessing files which are situated, physically, on a server owned by another person, or company, which may choose to permit the police access to the files. "Cloud computing" is becoming more common. Even today, many people keep private files, photographs, film etc. not physically on a computer located physically in their home, but on a server. This is safer in one sense, as the data cannot be accessed by another person, at least, by means of stealing the computer it is located on, and nor is it so vulnerable to fire and other accidents. It is also more convenient, as large amounts of data can be stored on the server and a person can access and work on the data wherever he or she is, e.g. an internet café.

One can argue that, with *any* internet use, a person *should* have no legitimate expectation of privacy. Certainly, this is the case when a person chooses to put data – film, pictures, text etc. – on a public billboard, or site such as Youtube. Here the data has deliberately been made available to anyone who has access to the internet, and no special authority is required for the police to make a copy of it (any more than such authority is necessary to photocopy a newspaper).

I have not made an empirical survey of peoples' subjective perceptions of privacy when they store data on *private* spaces on the internet. However, I suspect that most people believe that the information they keep on a server is confidential. If a person complies with the contractual agreement with the company owning the server (e.g. not to store pornographic material etc.) then he or she almost certainly feels that s/he has a legitimate expectation of privacy. The proof of this is that they are likely to react very negatively if the entity controlling the server disseminated this information to people other than those the person in question has authorized to access the data (e.g. outside the circle of "friends" in facebook). Personal data stored on servers may well be just as sensitive as other data, stored on one's own computer. Finally, an another argument for this approach is that the unauthorized accessing of such data belonging to another person, *wherever held*, is a criminal

offence under Swedish law.[97] It seems clear that to access such data also involves an interference with a person's private life.

6 Level and type of regulation requirements set by the Court's case law on accordance with the law

6.1 Generally

As already mentioned, the requirement under Article 8(2) that an interference be "in accordance with the law" is not purely formal. It relates to the quality of the law. In Klass v. FRG there was little debate on this point, as the German law in question, the "G10",[98] provided for a relatively detailed system of restricted interferences, applicable in defined circumstances.[99] In Klass v. FRG and a number of earlier Commission decisions, issues relating to the quality of law were considered as part of the question of the "necessity in a democratic society" of the measures. Most subsequent Court cases have, however, considered such issues under the heading of "accordance with the law".

The first telephone tapping case in which a violation of the accordance with the law requirement was found was Malone v. UK. In this case the British legislation at issue simply *recognised*, but did not actually grant, the authority of certain government ministers to authorise telephone tapping. The practice was subject to self-imposed administrative restraints, some specific, some vague.[100] The Court accepted the respondent government's contentions that the requirements of foreseeability must be lower in the case of secret surveillance. It obviously could not require that an individual know precisely when he or she would be subjected to surveillance, and so be in a position to adapt his or her conduct accordingly. Nonetheless, the Court stated that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially

[97] Criminal Code chapter 4, section 9c.
[98] *Gesetz zur Beschränkung des Brief-, Post und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz)*, hereafter "G10", 13 Aug 1968, BGBl. 1 S. 949. Each *Land* has its own G10 legislation *(Ausführungsgesetze zum G10 Gesetz)*. The description of the federal control system given below is applicable *mutatis mutandis* to the *Länder*.
[99] Klass report para. 63, Klass judgment paras 43 and 45.
[100] See Cameron, 1986, pp. 126, 129.

dangerous interference with the right to respect for private life and correspondence".[101] It added that "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power".[102] The Court proceeded to find that the British legislation on telephone tapping violated this requirement because it did not "indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities".[103] The Malone case led to the enactment of the UK of the Interception of Communications (IOC) Act 1985.[104]

In the British system at issue in Malone it was a government minister who authorized telephone tapping, without any judicial involvement. However even systems where the judiciary have approved telephone tapping have been found on several occasions to violate the Convention. The first of these cases were Kruslin v. France[105] and Huvig v. France[106]. The legal authority in French law for ordering telephone tapping (which was based on Article 100 of the Code of Criminal Procedure) was the subject of some dispute, but the Court was prepared to accept that there was a sufficient basis for this in French law, and that this practice was sufficiently accessible. But investigating magistrates had unlimited discretion to order telephone tapping. The Court found that this offended against the requirement of foreseeability, and that the practice was therefore not "in accordance with the law". Another example is Valenzuela Contreras v. Spain which concerned a telephone tap placed on the applicant at a time when the only clear basis for this was the constitution. There was no implementing statute. While the judge ordering the surveillance had in fact attempted to minimise the interference this would involve in the applicant's private life, the absence of clear provisions setting out requirements equivalent to those laid

[101] Malone v. UK, para. 67.
[102] Ibid. para. 68.
[103] Ibid. para. 79.
[104] This Act was an example of doing the absolute minimum necessary to comply with a Court judgment. When the UK incorporated the ECHR in its national law, meaning that the Convention compatibility of the IOC Act could be challenged before the British courts, it became a matter of urgency to replace it. This occurred in 2000, with the Regulation of Investigative Powers Act (RIPA).
[105] 24 April 1990, A/176-A.
[106] 24 April 1990, A/176-B.

down in Huvig and Kruslin v. France meant that the Spanish measure was not "in accordance with the law".

6.2 Foreseeability

The Court's case law on the requirement of legal "foreseeability" in this field is usefully summarized in its admissibility decision in paras 93–95 of Weber and Saravia.[107]

"93. .... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia, Leander v. Sweden*, 26 August 1987, A/116 para.51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia, Malone*, para. 67; *Huvig*, para. 29; and *Rotaru v. Romania* No. 28341/95, para.55, ECHR 2000-V]). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, 25 March 1998, *Reports* 1998-II, pp. 542–43, para. 72, and *Valenzuela Contreras v. Spain*, 30 July 1998, *Reports* 1998-V, para. 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, para. 64; *Huvig*, para. 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, para. 68; *Leander*, para. 51; and *Huvig*, para. 29).

[107] I have edited the excerpt. Similar recitations are found in Association for European Integration and Human Rights and Ekimzhiev, paras 75-77 and Liberty v. UK, para. 62. For the requirement of accessibility, see the Liberty case, discussed below.

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia, Huvig*, para. 34; *Amann,* para. 76; *Valenzuela Contreras*, para.46; and *Prado Bugallo v. Spain*, no. 58496/00, para. 30, 18 February 2003)."

6.3 Safeguards

Safeguards are necessary to ensure that the minimum standards of foreseeability set out above are complied with. In Association for European Integration and Human Rights and Ekimzhiev the Court stated that "in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection against arbitrary interference with Article 8 rights …The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."[108]

The Court has increasingly emphasized that there are two stages in the surveillance process, both of which must be subject to independent controls. The first is the authorization and the second involves the actual carrying out of the surveillance, and/or the follow-up process when the surveillance has ended.[109]

In Klass v. FRG, the Court expressed a clear preference for a system of judicial control over the authorization process, stating that "The rule of law implies, inter alia that an interference by the

[108] Op. cit at para. 77 (references omitted). The last part of the quotation is a repeat of what the Court stated in Klass v. FRG, at para. 50.
[109] See Iordachi, para. 42 and Association for European Integration and Human Rights and Ekimdzhiev, para. 84.

executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure".[110] However, it went on to find that, as far as concerns strategic surveillance, that the G10 commission was a sufficiently independent control mechanism.

In Popescu v. Romania,[111] the Court considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorizing body must be independent *and* that there should either be judicial control or independent control over the issuing body's activity.[112] Although in Romania there was supposedly supervision by a parliamentary oversight body, the Court considered this to be only in theory, not in practice and, in any event, of no relevance as a remedy, because the individual was never subsequently informed of the fact of the surveillance.[113]

The Court has stressed the need for *statute* law to govern large parts of the powers of secret surveillance. Case law, even where it lays down detailed standards and comes from the supreme, or constitutional court, is in itself not sufficient to regulate the area.[114] Having said this, the legal framework need not be *wholly* statutory. A degree of concretization of standards can be laid down in administrative regulations or authoritative case law.[115] This provides a degree of flexibility, which is necessary when the legislator wishes to regulate the area in a "technique-neutral" fashion (which in turn is moti-

[110] Klass para. 55. The Court continued "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge" (para. 56). The nature of the Convention system means that the Court is limited to hinting to states not then before it that they would be advised to change unsatisfactory laws. As hints go, this is pretty clear.
[111] No. 71525/01, 26 April 2007.
[112] Ibid. at paras 70-73.
[113] Ibid. "le contrôle du pouvoir législatif semblait plutôt théorique et, en tout cas, dépourvu d'effet pratique pour l'individu, dans la mesure où une personne mise sur écoute n'était pas censée prendre connaissance de l'existence de telles mesures secrètes à son égard" (at para. 77).
[114] See Heglas v. Czech Republic, op. cit, para. 74. The Court had earlier accepted concrete rules laid down by the Constitutional Court in Valenzuela Contreras v. Spain, para. 34 but this is no longer the case now.
[115] The Court went so far in Kopp v. Switzerland to find that case law, doctrine or administrative regulations, as long as they are sufficiently well known, can diverge somewhat from the wording of the law, without this violating the Convention (25 March 1998, paras 59–60). However, bearing in mind the greater awareness the Court has shown in more recent cases of the need to minimize abuse in this area, I doubt if it would take the same approach today.

vated by the need to avoid continual legislative changes to enable the police to keep pace with new technology).[116]

It follows from the case law (e.g. the Klass and Association for European Integration and Human Rights and Ekimzhiev cases) that the demands of foreseeability are separate from the need for safeguards, and remedies, even if the two sets of requirements are linked. The Court has putting an increased emphasis on safeguards presumably because it perceives that the list of factors to be set out in the statute will not in themselves serve to avoid abuse or overuse. For example, the requirement to set out the offences for which interception of telecommunications is permissible is in itself not so strong a safeguard as it might appear.[117] The definition of an offence is a matter for the national legislature. Within the weak limits of Article 7, an offence can be defined in relatively broad terms.[118] A requirement can be set in national law that a minimum penalty be applicable for an offence before telecommunications interception is available to investigate the offence. But this in itself is not a sufficient safeguard either, if the national legislature considers that a large proportion of all offences come up to this minimum threshold.[119] A statutory requirement that other methods of investigation are unlikely to be successful can in practice be taken seriously by the investigating and authorizing authorities, or be treated as a formality. Finally, the availability of telecommunications interception in practice is dependent upon both how the legislature frames the degree of suspicion necessary before the measure can be ordered, and how the investigating authorities and the authorizing bodies interpret this requirement. In Iordachi and Others v. Moldova,[120] the Court identified all of these problems.[121] It expressed the view that tele-

[116] Cf Skyddet för den personliga integriteten Bedömningar och förslag SOU 2008:3 s. 203 ”En reglering bör vidare vara så teknikneutral som möjligt och undvika att söka uttömmande ange vilka metoder som avses.”

[117] It should be added here that the Court accepts, for those states which have a separate civilian security service, without police powers, that telecommunications interception need not be linked to a specific criminal offence (something considered in more detail below).

[118] As regards the relatively loose standard of “law” applied by the Court in the context of Article 7, see Cantoni v. France, op. cit section 4, concerning the conviction of a supermarket manager for unlawfully selling pharmaceutical products.

[119] A trend of increasing penalty levels, partly influenced by harmonization desires at the European level, can contribute to this. See, in particular, the Framework Decision on Combating Terrorism which, in some EU states at least, had the result of considerably increasing the offences for which special investigative measures could be ordered.

[120] No. 25198/02, 10 February 2009.

[121] “It is made explicit that someone suspected of a serious, very serious or exceptionally serious offence risks in certain circumstances having the measure applied to him or her….Still, the nature of the offences which may give rise to the issue of an interception warrant is not, in the Court's opinion, sufficiently clearly defined in the impugned legislation. In particular,

communication interception in Moldova was being heavily overused and stressed that "telephone tapping is a very serious interference with a person's rights and that only *very serious reasons* based on a *reasonable suspicion* that the person is involved in *serious criminal activity* should be taken as a basis for authorizing it".[122]

A number of issues need more detailed treatment. As already indicated, one of these is concretizing the independent controls necessary in the follow-up stage, in other words, "the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed". The case law, particularly Kopp v. Switzerland, and Lambert v. France indicates that national law must provide adequate mechanisms for supervising what happens with "surplus information". This issue falls largely outside the scope of the present report, and I havealso discussed it elsewhere.[123]

The case of Kennedy v. UK[124] stands in contrast to the critical approaches shown in the Association for European Integration and Human Rights and Iordachi cases. The British system provides relatively limited safeguards, particularly in national security cases, where the "RIPA Commissioner" only performs a post-hoc check of the "paper work", the supporting documentation behind the applications approved by the responsible government minister. In practice, the time the Commissioner devotes to this task means that only a few cases chosen at random can be subject to any detailed study. Moreover, no follow-up check is made comparing the product of the interception with the documentation relied upon justifying the interception. The complaints body, the Investigatory Powers Tribunal ("IPT") has upheld hardly any complaints. Even bearing in mind the fact that very many complaints are likely to be groundless, the success frequency is remarkably low.

---

the Court notes that more than one half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception… It notes that Article 156 para. 1 of the Criminal Code uses very general language when referring to such persons and states that the measure of interception may be used in respect of a suspect, defendant or other person involved in a criminal offence. No explanation has been given as to who exactly falls within the category of "other person involved in a criminal offence" (paras 43–44)… The Court notes that the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising an interception. Nor does it contain safeguards other than the …that interception should take place only when it is otherwise impossible to achieve the aims" (para. 51).

[122] My emphasis, ibid. para. 51.

[123] See Cameron, 2000, pp. 106–109.

[124] No. 26839/05, 18 May 2010.

What nonetheless seems to have been decisive for the Court in the Kennedy case was that there was "no evidence of any significant shortcomings in the application and operation of the surveillance regime" (para. 162). The case thus supports the proposition that where the Court concludes there is a high degree of professionalism on the part of the police/security agencies in complying with the statutory rules for using surveillance, then a relatively limited control/oversight mechanism is acceptable.

I should note that I do not agree with this approach. I would argue that, to be credible watchdog, a control mechanism must have a mandate which allows it to study both the lawfulness *and* the merits of an application afterwards. It must have a minimum degree of competence and resources, e.g. to carry out inspections when and if this is deemed to be necessary. This more robust approach is advocated by inter alia the Venice Commission.[125] However, it seems clear that the Court pitches the test somewhat lower.

Fortunately, this is not an issue in Sweden. Follow-up controls have recently been created in Sweden in the form of the Security and Integrity Board and it is unnecessary to go into detail on the Convention requirements in this respect. It suffices to say here that the system put in place must involve not simply a rule that irrelevant conversations be destroyed, but close supervision by a competent external body, most suitably with some form of judicial competence, that this rule is complied with. This in turn will entail administrative routines for enabling the external body to investigate compliance, e.g. logging of all calls recorded, logging of staff present, closely controlled equipment, recordings made in such a way as to reduce the risk for subsequent editing etc.[126]

6.4 Issues for further discussion

There are two issues which I think should be discussed in the present report. The first is whether *all forms* of secret surveillance have to comply with the above requirements. One can argue that the

[125] Venice Commission, 2007, para. 165.

[126] Although rules must be in place and be observed, all deviations from such rules by the police or the authorizing body need not constitute a violation of the Convention, if the misuse or error is corrected by a higher court, e.g. by disregarding the evidence so obtained. See Remmers and Hamer v. Netherlands, No. 29839/96, decision of 18 May 1998. See, however, the less demanding

different types of surveillance mentioned earlier (aural, visual, location information) in different contexts and in different locations (the "home" and elsewhere) involve different levels of interference with privacy, and so different levels of foreseeability are permissible in the regulatory framework. The Court accepts differential levels of *safeguards*.[127] As noted above, in section 4, the Court accepts that differential levels of foreseeability are permissible in general depending upon the degree of interference involved in Convention rights. Recently, in Uzun it has confirmed that different levels of foreseeability are acceptable for different types of surveillance measure involving infringements of Article 8. It stated that the stricter principles (set out above) "are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations … It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above" (at para. 66). In the circumstances, it accepted the then existing general authorization to use "technical means" was sufficient legal basis for the measure. However, in reaching this conclusion, it took into account a variety of other safeguards which in practice restricted the use of these technical measures, in particular, the fact that they could only be used to investigate offences of a sufficient gravity, and, as already noted, that the domestic courts applied a proportionality test and could exclude evidence. (It can be noted that the German law was later amended to provide for judicial authorization to use GPS receivers, where the time period in question exceeds one month).

The purpose of defining powers with precision is to reduce the scope for misuse of, or overuse of, power. Other things being equal, the more the power in question interferes with privacy, the greater the potential damage to privacy if the power is misused or overused. It does seem thus reasonable to take the approach that operations and measures which involve a greater infringements of privacy should be provided for by clearer authority, and subject to more restrictions, than operations which involve lesser infringe-

[127] Cf. PG and JH, op. cit "What is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question" (at para. 46).

ments of privacy.[128] Precision focuses the minds of everyone involved in the investigation and authorization process on their responsibilities, which are ultimately backed up by the criminal offence of misuse of office. The same applies to providing for special authorization procedures – whether by senior police officers acting as "gatekeepers" or prosecutors – for the use of particular types of measure, either generally, or in situations which are perceived as being particularly sensitive.

Having said this, this principle of precision can only be a point of departure. The argument can be misused, e.g. to justify low levels of precision regarding measures which involve a small interference with each individual target's privacy, but because the measure is used extensively, the cumulative effect can be a large global interference. And one can also envisage situations in which a degree of imprecision in regulating a secret surveillance power can be compensated for by tighter post hoc controls. Not much guidance can be derived from the Court's vague reference in Uzun (referred to above, section 5.3.4) interferences which "disclose more information on a person's conduct, opinions or feelings". It is difficult authoritatively to rank the different types of secret state surveillance identified earlier on the basis of the degree of infringement each involves in privacy. This is partly because the notion of privacy can be assumed to vary from culture to culture and from time to time[129] even if some indications of "common European conceptions" can be derived from the compilations of state practice made by academics and the Council of Europe.[130] The second issue is, does the case law give any indications that a degree of difference in the amount and type of regulation is permissible depending upon the *purpose* for which surveillance is being undertaken – preventive or investigative – and/or the *underlying interests* to be protected – the prosecution of crime or the protection of national security? Another aspect of this issue is whether the case law permits identifies situations where even "privileged communications" can be monitored. The national security issue is closely related to the issue of the degree of accessibility and foreseeability required for strategic

[128] One judge in the English court of appeal judgment in Woods, op. cit, took this approach, but the other two – mistakenly in my view – disproved it. See also the McDonald Commission Report, p. 514, which drew the logical procedural consequence of the principle and argued that the more intrusive the technique, the higher should be the level of authorisation. However, this too relates to safeguards, not the level of precision.
[129] E.g. in one state, tax returns are highly confidential, in another they are not.
[130] See, in particular, Council of Europe, 2005.

surveillance, so the two can conveniently be treated together and I do this in section 6.6.

6.5 Differential standards for different forms of surveillance

To begin with, the Court made it clear in Bykov that bugging, whether or not participatory, involves at least the same level of interference with private life as does telephone tapping.[131] One can try to draw a distinction in the degree of the interference in private life between bugging in a private place and a public place, because of the allegedly reduced "reasonable expectation of privacy". But in many cases of bugging in public spaces the operation may well result in more, or even much more, "surplus information", that is, information concerning other people who may have nothing to do with the target. So even if the interference with the target's privacy may be less, I would say that the same, or more or less the same, legal framework should apply to both situations.

To turn now to the degree of regulation required for "teledata". The Court considered the British system in PG and JH. This involved, simply put, the police requesting the disclosure of the information from the telephone company. Where it refused to disclose this information, the police could request a court to issue an order compelling it to disclose it. The legal regulation of the system consisted of exceptions in the relevant statutes, permitting the telephone company to disclose the requested data to the police, without the penalty which would otherwise apply for revealing personal information. The Court noted that "the information obtained concerned the telephone numbers called from B.'s flat between two specific dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of them, were therefore strictly limited. While it does not appear that there are any specific statutory provisions (as opposed to internal policy guidelines) governing storage and destruction of such information, the Court is not per-

[131] "In the Court's opinion, these principles apply equally to the use of a radio transmitting device, which, in terms of the nature and degree of the intrusion involved, is virtually identical to telephone tapping" (at para. 79). Cf. SOU 2007:22, p. 182 and Vetter v. France where the court contented itself with noting that "comme les interceptions d'entretiens téléphoniques, les écoutes de conversations par le biais de la pose de micros représentent une *atteinte grave* au respect de la vie privée." (at para. 26, my emphasis).

suaded that the lack of such detailed formal regulation raises any risk of arbitrariness or misuse. Nor is it apparent that there was any lack of foreseeability. Disclosure to the police was permitted under the relevant statutory framework where necessary for the purposes of the detection and prevention of crime, and the material was used at the applicants' trial on criminal charges to corroborate other evidence relevant to the timing of telephone calls. It is not apparent that the applicants did not have an adequate indication as to the circumstances in, and conditions on, which the public authorities were empowered to resort to such a measure."[132]

In constructing the legal framework for authorizing, and controlling, the use of teledata I think it reasonable to take account of the dual purposes behind it, namely the obtaining intelligence and the obtaining of evidence. The two functions set out above are obviously closely related, as it is necessary first to identify the participants in a criminal conspiracy and then to amass evidence against them. Intelligence can later become evidence. Information that, e.g. A, according to his mobile, was at a certain location at a certain time period can be highly valuable circumstantial evidence, discrediting, or proving his version of events. It may well be that the intelligence function is more, or much more common as far as regards teledata. If the objective is simply obtaining intelligence, then it is the police who are the primary judge of whether teledata is needed, and what sort, and extent, of teledata is needed. The time period during which the investigation proceeds might also differ. The remedies available after the surveillance has ceased will also be different. There will be differences in the handling of "surplus information". Where the object of the surveillance is exploratory, to obtain information generally on a loose grouping of people, or a phenomenon, less information is likely to be regarded as "surplus" as compared to an investigation of a specific criminal offence committed, or planned, by a specific group. (Having said all this, the fact that the police know best what and how much intelligence is needed does not mean that they are best placed to judge whether the gain to the police investigation outweighs the loss to the human rights of the suspect and others caught up in the intelligence gathering operation – quite the contrary).

It is fair to say that the Court set low standards of "accordance with the law" in the PG and JH case. There was no judicial authori-

[132] At paras 46-47.

sation of the interception of teledata in the British system. The question is whether the Court has properly appreciated the type of information which can nowadays be obtained by intercepting teledata.[133] As already mentioned, one can argue that data relating to internet usage is more sensitive than mobile numbers called, which in turn is more sensitive than location information. There is some empirical evidence that people regard location information as the least sensitive type of information.[134] However, in practice, a person can be accessing the internet from his or her mobile, or using his or her laptop to make calls at the same time as he or she is surfing the net. Monitoring this usage, in realtime or afterwards, will give the monitor information on all three categories of data. It seems, then, unworkable to set different levels of precision and control for these three different types of data.

There seems to be no doubt that interception of teledata is a useful investigative and intelligence tool.[135] However, in Sweden the lack of availability of reliable information on how often and in what ways teledata interception has promoted the effectiveness of investigations and intelligence work, has made it difficult to measure *how* useful it has been and to weigh this against the interference in personal integrity this entails.[136] When an interception of teledata is made for intelligence purposes, one should be clear that the legality and proportionality of it will not be subject to any subsequent check in a criminal trial. Thus, some form of subsequent control is absolutely necessary to prevent misuse and overuse. The existence and proper functioning of the British controls over interception of teledata was not raised in the PG and JH case, nor did it arise in the Heglas case. However, I would say that the Court is very likely to note that some form of subsequent control system over teledata is necessary when and if it is confronted with this issue again. I will not go into the proposed Swedish system of subsequent control over this. However, I would like to note one thing. The problem of abuse of this measure is to be dealt with by the Security and Integrity Board reporting to the prosecutor. However, the issue of *overuse* is likely to be more serious matter in practice. When and if a pattern of overuse is detected by the Board, this is likely to emerge some

[133] Cf Lagerwall 2008, p. 64.
[134] van Loenen et al., 2008, p. 149.
[135] See e.g. Ianni 1990 and Krüpe-Gescher and Dorsch, 2005 (summarizing the results of a study of German practice carried out under the auspices of the Max Planck Institute in Freiburg).
[136] SOU 2007:22, p. 185.

time, or some considerable time, after the measures have terminated. A confirmed pattern of overuse must reasonably lead to criticism of the police authority involved. This imposition of accountability will have a forward-looking element in the sense of improving the system. However, there must also be a backward-looking element. It is unclear to me in what way the Security and Integrity Board is to react if it comes to the conclusion that *overuse* but not *abuse* has occurred. Where there is only a finding that overuse has occurred, and no imposition of accountability whatsoever, the risk is that the authorizing police will always "err on the side of caution" and favour overusing the interception of teledata because of the operational advantages this can give.

Lastly as far as this issue is concerned, I will deal with visual surveillance both outside and of the home. Although case law is lacking on the issue, I would argue that visual recorded surveillance of the home, or other "private space" such as a hotel room, should satisfy similar material standards as those which apply to telephone tapping or bugging. As noted above, the reason for requiring statutory authority (even though the Court has not spelled this out) is that major interferences in privacy should require the considered attention of the legislature. If the three types of surveillance are regarded as involving more or less the same level of interference in privacy, then the logical consequence is that the following issues should be set out in *statute* for visual surveillance of the home; the offences which may give rise to recorded visual surveillance of the home, the ways in which different categories of people (suspects, suspects' contact persons etc.) qualify for this measure being used against them, a limit on the duration of the visual surveillance of the home, the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.

As already made clear in the preceding sections, visual surveillance *outside* of the home has so far not, as such, been regarded by the Court as an interference with private life. However, retention of this data is very likely to be regarded as such an interference. The main case dealing with standards of retention of law enforcement data is S and Marper v. UK.[137] The case, where the Court, sat as a Grand Chamber, considered the retention of fingerprints and DNA

[137] Nos 30562/04 and 30566/04, 4 December 2008.

samples taken from a person suspected of a criminal offence. Under English law at the time, these may be retained indefinitely, even if, in the subsequent criminal proceedings, the suspect is acquitted. The Court began by considering whether the retention of three different categories of identifiers, namely fingerprints, cellular samples and DNA profiles[138] involved interferences with private life. The respondent government had argued that retention of this data did not interfere with the physical and psychological integrity of the persons concerned; nor their right to personal development. However, Court considered that stated that "given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with [private life]" (para. 73). As regards DNA profiles, the Court placed weight on the fact that the information contained in these allows the authorities to go beyond simple identification of people. As regards fingerprints, while these had less of an impact on private life, the "unique" information fingerprints "contained about the individual concerned allowing his or her identification with precision in a wide range of circumstances" meant that their retention without the individual's consent "cannot not be regarded as neutral or insignificant" and so this was also an interference with the right to respect for private life (paras 84–85).

A photograph or film can of a person can be regarded by the person it concerns as extremely sensitive, depending upon the subjectively perceived potential for embarrassment or even damage to personal interests dissemination of this record to the general public, or particular people, can cause. Or its dissemination can be regarded with indifference or even welcomed by the individual concerned. One cannot therefore say that *all* visual records in themselves contain the same potential for interference with private life as does *all* DNA samples. On the other hand, one can see a visual record as raising comparable issues to a fingerprint. Although it is naturally possible to draw distinctions between fingerprints and photographs, I would say that the same general points should apply.

The significance of the English system for retention of DNA and fingerprint records was that there was no mechanism in place for weighing the gain to the police in their work in detecting and investigating crimes against the interference the retention of these

[138] A DNA profile is obtained by analysing a reference sample from an individual. It consists of a set of numbers which can be put in the form of a barcode. This allows later automated matching of the profile with subsequent profiles.

records involved in private life. In S and Marper, the Court was "struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may retained irrespective of the nature or gravity of the offence or of the age of the suspect. Likewise, retention was not limited in time and there existed only limited possibilities for an acquitted individual to have the data removed from the nationwide database or to have the materials destroyed [and] there is no provision for independent review of the justification for the retention" (para. 119). The government had argued that simple retention of the data could not have any significant effect on the individuals concerned, but the Court disagreed. The Court considered that the presumption of innocence (set out in Article 6(2)) was relevant as part of the interpretative context, even if data retention was not as such a "voicing of a continued suspicion". The Court considered that there was a clear risk of stigmatization in the blanket retention of data, and that retention could be "especially harmful in the case of minors … given their special situation and the importance of their development and integration in society" (paras 122, 124). In this respect, the Court paid attention to the concerns voiced that young people and ethnic minorities are over-represented in the database. In conclusion, the Court ruled unanimously that the blanket and indiscriminate nature of the powers of retention of all three categories of personal information had failed to strike a fair balance between the competing public and private interests, and that there had been a violation of Article 8.

The implications of this for visual records seem to be as follows. As the police have the task of investigating and preventing crime, some degree of suspicion, of a past, or ongoing, or even future offence will provide sufficient basis for the retention of visual records which identify a given individual. Some sort of legal authority would seem to be necessary to keep photographic records of covertly photographed suspects, although there is nothing to indicate that the Court would require this to be in statute form.[139] The degree of suspicion necessary for justifying retention of records can reasonably be expected to vary according to the seriousness of the offence.[140] The need for investigative secrecy (at least as far as

[139] The applicable framework, the Code of Judicial Procedure and förordning (1992:824) om fingeravtryck m.m. only covers photographing of arrested persons. See also RPSFS 2005:12 - FAP 473-1.

[140] Cf Lord Justice Laws comment in Woods, op. cit at para 84 "the court is required to carry out a careful exercise of weighing the legitimate aim to be pursued, the importance of the right

ongoing and future offences are concerned, and for past offences which have not resulted in prosecution for some reason, but where reasonable suspicion against a person continues to exist) means that, in the case of covert visual records, the very fact that a record exists may be kept secret. As mentioned before, as the police must be given great discretion in this area, it is necessary to provide for some form of external control mechanism, capable of monitoring and influencing the general practice of retention. As this concerns operational decisions, only a body with a degree of expertise in weighing the investigative advantages against interferences in privacy will satisfy the Convention test of "necessity in a democratic society".[141] It is also necessary to provide a remedies system, capable of determining the proportionality of continued retention of a given record on an individual when and if that individual complains.[142] Again, it should be stressed, where there is a need for investigative secrecy in the individual case, the very existence, or non-existence, of a record can be kept secret from a complainant.

6.6 Proactive surveillance, national security surveillance and strategic surveillance

There is considerable, but not complete, overlap between the categories of proactive surveillance (meaning surveillance designed to prevent the commission of offences), national security surveillance and strategic surveillance. Different states provide for different types of surveillance depending upon whether they have a security agency with police powers or not (which tends to mean a stronger link between surveillance and offences) and whether or not they have a strategic surveillance capacity.

---

which is the subject of the interference and the extent of the interference. Thus an interference whose object is to protect the community from the danger of terrorism is more readily justified as proportionate than an interference whose object is to protect the community from the risk of low level crime and disorder." See also the approach of the BVerfG as regards dissemination of intelligence, noted in the next section.

[141] The purpose of the present report is to analyse the "accordance with law" requirement, so I will not go into this issue here. I should, however, note that in Segerstedt-Wiberg v. Sweden, No. 62332/00, 6 June 2006, the Court did not consider the Data Protection Board to be a sufficient *remedy* because it did not, in practice, question operational decisions to retain data by the security police. For a general treatment of the issue of controls see, Cameron, 2000, pp. 222–258.

[142] Cf. Segerstedt-Wiberg ibid. (violation of Article 13, because there was no body capable of determining the proportionality of permitting access to security files).

The Convention does not limit the possibility to interfere in Article 8 to the situation where there has been an offence, or an offence is ongoing. The wording of Article 8 expressly allows interferences in private life to prevent disorder or the future commission of offences. In Weber and Saravia for example, the Court accepted that the German system of strategic surveillance, which need not be linked to offences, could be justified for the prevention of crime and the protection of national security.[143]

As already indicated, the boundary line between "preventive" surveillance and "investigative" surveillance is not hard and fast: it depends upon how the crimes are formulated, and the associated national doctrines in the general part of the criminal law on inchoate crimes and participation in crime (conspiracy, preparation, attempt etc). Security crimes in particular tend to "begin" early in the sense that even preparatory steps can be criminalized.[144] The Court's case law emphasizes precision in formulation, that surveillance must be limited to the most serious offences and that safeguards must be adequate against abuse. Thus, it is a reasonable conclusion to draw from the Court's case law that surveillance should only be available for preventing either *serious damage to national security* or a *clearly defined* category of the *most serious* offences set out in a state's criminal code and concerning which there are *reasonable grounds* for fearing that these will occur and that surveillance will assist in preventing these. It is reasonable to assume that preventive surveillance will often, or at least occasionally, be based on speculative intelligence which does not satisfy criminal law standards of "reasonable cause" to suspect the commission of an offence. As such, preventive surveillance carries with it greater risks of abuse, and overuse. The power to engage in it must be as narrowly defined as possible but as the requisite degree of precision can not be secured, logically, greater safeguards must be available against abuse and overuse as compared to surveillance to investigative an already committed or ongoing offence.

There is obviously a margin of appreciation for each state in how it goes about framing the authorisation procedure. However, I can note that a simple proportionality test in the sense of weighing the gravity of the crime occurring against the interference with the private life of the suspect, and others caught up in the surveillance,

[143] Op. cit at para. 104.
[144] For a discussion of the criminalized stages involved in the offence of promotion of terrorism see Asp and Cameron 2009.

risks authorisation being routinely granted for very serious offences, even if, in the circumstances of the case, the actual gain to the investigation/prevention is very small or non-existence. Thus, it would seem sensible to condition preventive surveillance on the fulfilling of successive hurdles: that there is a high degree of likelihood that the target is engaged in serious crime *and* there is a high degree of likelihood that the secret surveillance being requested will assist in the /prevention of the offence.

As regards national security surveillance, the Court has accepted that this does not have to be linked to investigations of concrete criminal offences. This is because some states have civilian security agencies without police powers and with broader mandates than the investigation of crime. The Court has not defined national security. The Commission earlier took the view that "national security" cannot be defined exhaustively.[145] The Court however, has become increasingly skeptical to states' arguments that national security justifies a vaguer and more flexible approach to the requirements of foreseeability and accessibility. Certainly, preferential treatment for national security is becoming more difficult to justify the more the areas of policing and security overlap, as they do particularly in relation to terrorism.

In Amann v. Switzerland the applicant was a businessman engaged in the importation of depilatory equipment. In 1981 he had been telephoned by a woman from the Soviet embassy who wished to buy a depilatory apparatus. Soviet diplomats' conversations were routinely being intercepted by the Swiss security police and a file (albeit only a card index) was opened on the applicant as a "contact person". He complained inter alia of the lack of authority for the telephone tap. Under the applicable domestic law at the time (the Federal Council's Ordinance on Police Services of the Federal Attorney's Office 1958) the police were given competence to engage in the "surveillance and prevention of acts liable to endanger the internal or external security of the Confederation". A similarly worded provision can be found in Section 17 of the Federal Code of Criminal Procedure (FCCP). The Court, however, found that these provisions were not sufficiently foreseeable to serve as a basis for telephone tapping, even "passive tapping" which was the

[145] Mersch et al. v. Luxembourg Nos 10439-41/83, 10452/83 and 10512-3/83, 43 DR 78 (1985). See also M. v. France, No. 10078/82, 41 D.R. 103, 117 (1985). "As far as the legal definition of criminal offences against national security, territorial integrity and public safety are concerned, the authorities of the particular State are best placed to decide whether a restriction designed to prevent such offences is necessary."

case here. It stated that these provisions contain "no indication as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed. [These rules] cannot therefore be considered to be sufficiently clear and detailed to afford appropriate protection against interference by the authorities with the applicant's right to respect for his private life and correspondence."[146]

More generally, one can say that the Court is increasingly aware of the room for abuse of the national security concept.[147] In Iordachi, "national security" was one of the bases for surveillance. The Court criticized the lack of concretization of this and the other terms used in the applicable Moldovan law.[148] In Association for European Integration and Human Rights and Ekimdzhiev the Court referred to the need to take care "not to stretch the concept of "national security" beyond its natural meaning".[149] The Liberty and Weber and Saravia cases, discussed below, illustrate a tighter approach to national security. And there are several other cases involving security justifications in different contexts, e.g. security screening and security deportations, in which the Court has expressed the need for strong controls on the use of security powers to prevent abuse.[150]

In one aspect, the Court appears to accept that national security allows for greater latitude. A number of European legal systems, e.g. Germany and the UK,[151] do not appear to permit law enforcement surveillance of certain categories of people, but do appear to make an exception for national security surveillance. This prohibi-

[146] At para. 58.
[147] For an early warning in this regard, see Judge Pettiti's separate opinion in Kopp: "The legislation of numerous European states fails to comply with the Article 8 as far as telephone tapping is concerned. States use or abuse the concepts of official secrets and secrecy in the interests of national security. Where necessary they distort the meaning of that term. Some clarification of what these concepts mean is needed in order to refine and improve the system for the prevention of terrorism ... the Court's Klass, Malone, Huvig and Kruslin judgments have all remained largely ineffective. The people running the relevant State services remain deaf to these injunctions and to a certain extent act with impunity....".
[148] Op. cit at para. 46.
[149] Op. cit at para. 84.
[150] See e.g. Rotaru v. Romania, No. 28341/95, 4 May 2000, Al-Nashif v. Bulgaria, No. 50963/99, 20 June 2002, at para. 124 (security deportations), Turek v.Slovakia, No. 57986/00, 14 February 2006 (Alleged former collaborator with state security agency unable to challenge his registration in agency files in proceedings guaranteeing equal treatment of both parties), Gulijev v.Lithuania, No. 10425/03, 16 December 2008 (Expulsion on the basis of a "secret" report of the State Security Department which was not disclosed to the applicant), A. and Others v. UK, No. 3455/05, 19 February 2009 (security detentions), Nolan and K. v. Russia, No. 2512/04, 12 February 2009 (Exclusion of foreign Unification Church activist from country supposedly on national security grounds: violation of Article 9).
[151] See Council of Europe, 2005.

tion is naturally formulated in different ways. It can apply to all persons who are freed from the duty to give evidence under national law (doctors, priests, journalists etc.)[152] or it can apply only to more restricted categories, e.g. a defence attorney explicitly or implicitly engaged by a suspect.[153] Inter alia Klass v. FRG, Kopp v. Switzerland and a letter interception case, Erdem v. Germany,[154] indicate that the Convention does *not* require states to abstain totally from engaging in surveillance of "privileged communications", e.g. between lawyer and client.[155]

I will turn now to strategic surveillance. In Weber and Saravia, the applicants had argued that by intercepting private communications beginning and ending in another country the German authorities were violating international law. The Court considered that the term "law" refers back to national law, including rules of public international law applicable in the State concerned. However, the Court required proof in the form of "concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law" (para. 87). The Court considered that "Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany" (para. 88). The Court in these circumstances found that the applicants failed to prove their allegations.[156] It should be noted that the German Federal Constitutional Court (BVerfG) had previously scrutinized the changes made in the German legislation permitting strategic surveillance, and found

[152] E.g. Article 125h, as read together with Article 218, of the Dutch Code of Criminal Procedure.
[153] E.g. Swedish Code of Judicial Procedure Chapter 27, section 22. This definition entails that not all conversations between a lawyer and a suspect are protected. Cf. the wider category of persons in the Code of Judicial Procedure Chapter 36, section 5.
[154] No. 38321/97, 5 July 2001.
[155] See also Hewitt and Harman v. UK, No. 20317/92, where one of the applicants, a lawyer, alleged that files were held on inter alia her conversations with clients. The Commission accepted that that there was a reasonable likelihood of this, but did not find a violation of Article 8. Judge Pettitti expressed the separate opinion in Kopp that surveillance of partners should never be permitted, even in security cases. See further the recent UK case, In re McE (Appellant) (Northern Ireland), In re M (Appellant) (Northern Ireland), In re C (AP) and another (AP)(Appellants) (Northern Ireland) [2009] UKHL 15, in which the House of Lords held that it was, exceptionally, possible to subject lawyer-client contacts to secret surveillance.
[156] The capability to intercept telecommunications in other countries, without, obviously, applying for judicial authorisations, was the subject of much debate, and disagreement, in the EU Convention on Mutual Assistance in Criminal Matters, 12 July 2000, OJ C 197.

certain of these to be unconstitutional.[157] The law was therefore amended. In any event, as regards the quality of the law, the Court concluded that the challenged provisions of the amended G 10 Act contained the minimum safeguards against arbitrary interference as defined in the Court's case-law.[158]

The BVerfG's judgment thus has to be examined. As regards matters which fall broadly into the category of "accordance with the law", the BVerfG found that the inclusion of the offence of money laundering could not be justified. It also found the arrangements on transfer of information to the police to be unacceptable. The list of offences in section 3(3) of G10 includes certain minor offences. The BVerfG specified that the more minor the offence is, the more concrete the indications must be that a given person has committed it, before transfer of information is allowed. Even the arrangements for retention and use of information by the intelligence service (section 3(4)) and transfer of information to the government (section 3(3)) were found to be insufficiently specified. The German intelligence service naturally comes across all manner of interesting information in its trawl of telecommunications. The BVerfG stated that the G10 law should specifically state that only information falling within the functions of the intelligence service (i.e. relating to the defence of the state) may be retained and used by the intelligence service, and transferred to the government. The BVerfG stated more generally that section 3(7) of the G10 law is deficient as it does not provide for a clear duty to "mark" intelligence originating from strategic surveillance, so that it can later be identified (and its use controlled). Finally, where the information is used is some way, it should not be destroyed (a point related to notification). As the BVerfG had set high *Rechtsstaat* standards, there was no need for the Court to set higher standards.

By contrast, the Court found in the Liberty case that the UK system of strategic surveillance was not "in accordance with the law". The UK government argued in Liberty that the accessibility requirements should be lower. At issue were the so called section 6 arrangements – the technical search parameters designed to minimize the collection of surplus information together with the instructions to officials on how to produce intelligence assessments from

[157] BVerfG, 1 BvR 2226/94, 2420/95 and 2437/95, 14 July 1999, in NJW 2000, pp. 55-68. Thanks to Tobias Wagner for help in translation.
[158] See para. 98 of the Court's decision. The specific standards are set out below in my discussion of the Liberty case.

the raw intercept material and to whom these assessments could be disseminated. At the time these were not published. Even today, only parts of these are published, in the form of excerpts from the Code of Practice applicable to officials. To begin with, the government argued that disclosure of these arrangements would damage national security, as it would give information on search methods, allowing potential targets to modify their behaviour. It was also argued, which I would say tends to undermine the first argument, that the arrangements were anyway incomprehensible to anyone without a high degree of technical expertise in the area. The government furthermore argued that comparisons with the much more open German system were not fair. Besides, the UK faced a greater terrorist threat than other states, which should justify granting it a greater degree of leeway. The government argued that the UK system had quite different safeguards, in particular, the oversight of an IOC (now RIPA) Commissioner, a senior judge who operates a post-hoc supervision of the system, including looking at the working of the section 6 arrangements. In this respect, the government referred to the earlier case of Christie v. UK.[159] One of the issues before the Commission in this case was whether the authority given in the IOC Act to intercept communications on the broad ground of "national security" was sufficiently clear and foreseeable. The Commission considered in Christie v. UK that a vague term can be "explained by administrative or executive statements and instructions".[160] It referred to the requirement set out in the Act to minimize interference and destroy surplus material, the supervisory competence of the IOC Commissioner and the remarks made by the IOC Commissioner in two of his annual reports regarding the term "national security".[161] It concluded that, in the circumstances, the Act satisfied the requirements of "accordance with the law".

However, if one looks at these comments, one can see that the IOC Commissioner did not, in fact, further specify the term, but simply acknowledged the difficulty in doing so.[162] It can be said here

[159] Christie v. UK, No. 21482/93, 78A DR 119 (1994).
[160] At p. 135, referring to the judgment of the Court in Silver v. UK, 25 March 1983, A/61, paras 88–9.
[161] Reports of the Commissioner for 1986 and 1988, respectively Cm. 108 (1987) and Cm. 652 (1989).
[162] The IOC Commissioner also stressed in his comments that everyone involved was doing their job properly and that there was no cause for alarm. Such reassurances are a recurring feature of the UK system, see, e.g. the IOC Commissioner's explanation why there is no need to fear unauthorised tapping in Report of the Commissioner for 1997, Cm. 4001 para. 32.

that while the Convention organs have regarded executive regulations (ordinances etc.) as falling under the term "law", it is a significant expansion of the term to say that executive *statements* can do so. The Commission in effect said that the mere existence of the IOC Commissioner was enough to satisfy the quality of law requirements.

The Court, correctly in my view, rejected all of the government's arguments in Liberty. The Court stated that it "does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. The Court's approach to the foreseeability requirement in this field has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in … Christie v. the United Kingdom.[163]

It added that while the IOC (now RIPA) Commissioner was an "important safeguard" against abuse of power it did not "contribute towards the accessibility and clarity of the scheme".[164] The Court went on to list the issues which *should* be accessible in statute law, referring to its earlier decision in Weber and Saravia "In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order …Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act … The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions

[163] At para. 63.
[164] At para. 67. As already mentioned, I personally consider that while the Commissioner can be described as a "safeguard", I do not think it is "important" in the sense of being a robust and well-functioning safeguard.

governing the transmission, retention and use of data obtained through the interception of external communications."

The Court's emphasis of the accessibility requirements in this case are probably due to the wide, indeed "virtually unfettered" (para. 64) discretion the British legislation gave to the authorizing body.[165] In one sense, as the respondent government itself argued, the British system was foreseeable. Any and all communications between the UK and abroad could be, and were being, intercepted. However, in these circumstances, and as there was no, or no necessary, connection between the intelligence gathering and specific criminal offences, the consequence was that the Court considered it even more important that the legislation provided the public with reassurances that the data collected would only be used for limited purposes and subject to strict controls.

By contrast, in the Kennedy case, the "ordinary" British system of surveillance, even on national security grounds, was regarded as in "accordance with the law". Apart from the (supposed) specification of the term by the IOC Commissioner, the reason the Court gave for this was that the *form* requirements which exist for such an authorization means that the interference is much more narrow and specified than strategic surveillance authorized on national security grounds.[166] The Kennedy case is thus authority for not having to set out what "national security" means in any more detail, provided other form requirements exist which in practice narrow down or specify the individual targets.

Lastly I can note as regards the Liberty case that the British system for strategic surveillance, has, as authorizing body, a government minister who is – obviously – not independent from the executive. In the Iordachi and Association for European Integration and Human Rights and Ekimdzhiev cases the Court stressed that independent controls should exist at both the authorization stage and the follow-up stage. At the very least, where a system lacks

[165] Cf. Lagerwall, p. 64.

[166] Kennedy v. UK, op cit, para. 160 "the legislation must describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraph, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Finally, the Court notes that in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered (see paragraphs 40 to 41 above). Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant."

independent controls at the authorization stage, this should mean that very strong safeguards must exist at the follow-up stage.[167]

7 Concluding Remarks

There is no need to repeat the conclusions I have drawn earlier. It suffices to say that Court case law indicates plainly, or strongly, that certain methods not now explicitly regulated by statute require to be so regulated. Definite support in Court case law is lacking for requiring regulation of some other methods. However, the direction in the Court's case law – an expansive approach to what constitutes private life – is clear. In the circumstances, choosing not to regulate methods which are considered to be close to the boundary of private life is a risk strategy.

References

Asp, P. and Cameron, I., Terrorism and Legal Security – a Swedish and European perspective, in De Lege Årsbook 2009, Iustus (2010).

Breyer P., Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, 11 European Law Journal, 365–375 (2005).

Cameron, I. European Court of Human Rights – April 2006–March 2007, 13 European Public Law, 533–568 (2007)

Cameron, I. National Security and the European Convention on Human Rights (Iustus, Kluwer, 2000

Commission of Inquiry into certain activities of the Royal Canadian Mounted Police. 2nd Report, Freedom and Security under the Law (1981) ("McDonald Commission Report")

[167] Thus, notwithstanding the statement in Liberty that the RIPA Commissioner is an "important safeguard", and notwithstanding the finding in the Kennedy case regarding the adequacy of the Commissioner for ordinary interception of communications, I would say that its is doubtful if the British system of ministerial authorization of *strategic* surveillance with only a limited post hoc control mechanism will satisfy the Convention. But this is, fortunately, not a system which Sweden has chosen to emulate.

Council of Europe, Terrorism, Special Investigative Techniques, 2005.

Harris, D. J., O'Boyle M., Bates, E., and Buckley, C., Harris, O'Boyle and Warbrick: Law of the European Convention on Human Rights, Oxford UP, 2009

Helmius, I., Polisens rättsliga befogenheter vid spaning, Iustus, 2000.

Hert, de P., European Data Protection as a Potential Framework for Electronic Visual Surveillance, in Nijboer, J.F. and Riejntes, J.M. (eds), Proceedings of the First World Conference on New Trends in Criminal Investigation and Evidence, the Hague, 1997.

Ianni, F. and Reuss-Ianni, E., Network Analysis, in Andrews, P. P. and Peterson, M. B. (eds), Criminal Intelligence Analyses, Loomis, Cal., (1990).

Joubert, C. and Bevers, H., Schengen Investigated, Kluwer, 1996.

Krüpe-Gescher, C., Dorsch C., Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation und Anderer Verdeckter Ermittlungsmassnahmen, Max-Planck-Instituts für internationales Strafrecht, 2005,
http://www.mpg.de/bilderBerichteDokumente/dokumentation/jahrbuch/2005/strafrecht/forschungsSchwerpunkt/pdf.pdf

Lagerwall, A., Privacy and Secret Surveillance from a European Convention Perspective, Stockholm university, LLM thesis, 2008.

Loughlin, M., The Rule of Law In European Jurisprudence, European Commission For Democracy Through Law, Study 512/2009 CDL-DEM(2009)006

Lustgarten, L. and Leigh, I., In From the Cold: National Security and Parliamentary Democracy, Oxford UP, 1994.

Marx, G. T., Undercover, Berkley/Los Angeles/London, 1988.

Moreham, N. A., A Right to respect for private life in the European Convention on Human Rights – a reexamination, EHRLR, 44–79 (2008).

Nagel, T., Concealment and Exposure, 27 Philosophy and Public Affairs, 3–30 (1998)

Naismith, S. H., Photographs, Privacy and Freedom of Expression EHRLR 151–158 (1996).

Ovey C. and White R. A., Jacobs and White: European Convention on Human Rights, 4th ed., Oxford UP, 2006

Ruiz, B. R., Privacy in Telecommunications: A European and an American Approach, the Hague, 1997.

Venice Commission, Report on the democratic oversight of the security services, 71st Plenary Session (Venice, 1–2 June 2007) CDL-AD(2007)016

Valkaneer, C. de, La tromperie dans l'adminstration de la preuve, Larcier, 2000.

van Dijk P. and van Hoof G.J.H. van Rijn, A., Zwaak L. (eds), Theory and Practice of the ECHR, 4th ed., Intersentia, 2006

van Loenen, B., Groetelaers, D., Zevenbergen, J. and de Jong J., Privacy versus national security: The impact of privacy law on the use of location technology for national security purposes, 2007, http://www.springerlink.com/content/r124077351051308/fulltext.pdf

Expertrapport åt Polismetodutredningen

Av professor Iain Cameron

I svensk översättning
(översättningen utförd av Språkservice i Solna AB)

1 Inledning

Jag har ombetts skriva en rapport med en analys av den rättspraxis som tillämpas av Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) i samband med, för det första, tekniska spaningsmetoder och, för det andra, användning av infiltration. Fokus ligger i båda fallen på att undersöka vilka metoder för spaning och infiltration som kräver reglering i lag, samt graden av exakthet för denna reglering.[1] Rapporten är emellertid ingen systematisk jämförelse mellan de befintliga reglerna för spaning i Sverige och konventionens normer, även om jag i vissa fall tar upp sådana efterlevnadsfrågor.

Först vill jag ge några inledande kommentarer. Det är ingen lätt uppgift att utarbeta användbara och ”framsynta” regler utifrån domstolens ”bakåtblickande” rättspraxis. Domstolens rättspraxis borde betraktas som en samling av allmänna principer. Vagheten hos de aktuella principerna tenderar att minska deras värde i specifika, konkreta situationer. Domstolen avgör mål dels genom domar, dels genom beslut om att inte ta upp ett mål till sakprövning. Den motivering som redovisas i ett beslut är i allmänhet betydligt mer summarisk än i en dom och ger därför mindre vägledning (ett undantag kan nämnas här, nämligen målet Weber och Saravia, se nedan). I brist på domar i en viss fråga tvingas man bygga ett resonemang enbart på beslut att inte ta upp mål till sakprövning. Det kan alltså förekomma en del bristande överensstämmelse mellan tidigare och senare rättspraxis.[2]

De begrepp som används i konventionen är autonoma. Det innebär att det faktum att en viss åtgärd från det allmännas sida *inte* betraktas som intrång i privatlivet enligt en nationell konstitution och nationella lagar inte nödvändigtvis innebär att den inte heller betraktas så enligt konventionen. Även om begreppen i konventionen är autonoma så har domstolen sällan tagit vara på möjligheten att utveckla innebörden av ett specifikt begrepp, utan har till relativt nyligen försökt att tydligt begränsa diskussionen till det

[1] Jag vill tacka mina kolleger Torbjörn Andersson, Thomas Bull, Johan Boucht och Magnus Ulväng för deras användbara kommentarer till ett tidigare utkast till denna rapport. Eventuella återstående felaktigheter etc. är mitt ansvar. Rapporten skrevs i februari 2010 och tar därför upp rättspraxis fram tills detta datum. Vid tidpunkten för publicering, december 2010, har jag gjort vissa tillägg för att ta hänsyn till två viktiga domar som har avkunnats mellan februari och november 2010.

[2] Domslut har högre status än avgöranden om upptagande till sakprövning, men om ett domslut senare modifieras genom ett avgörande om upptagande till sakprövning blir rättsläget ovisst, i synnerhet om domstolens resonemang inte är tydligt hela vägen.

föreliggande målet. Den försiktighet som domstolen visat beror delvis på att domstolen inte är ämnad (och – än så länge – inte har behörighet) att agera som en fullfjädrad författningsdomstol. Dess ”konstitutionella” funktion ökar dock och domstolen blir alltmer ”pedagogisk” i sin uppläggning. Nu tenderar domstolen att inleda behandlingen av ett mål genom att ange tillämpliga allmänna principer, såsom de framgår ur rättspraxis, innan dessa sedan tillämpas på det aktuella fallet.

När domstolen drar slutsatsen att någonting efterlever eller inte efterlever konventionen tenderar den att beakta samtliga relevanta faktorer. En lag, eller rättslig funktion, som anses vara utformad på ett bristfälligt sätt (t.ex. för att den är otydlig) kan kompenseras genom en kontroll- eller skyddsmekanism som exempelvis minskar risken för missbruk till följd av bristen på tydlighet. Det är alltså väldigt viktigt att ta hänsyn till hela kontexten av ett domslut. Staterna A och B kanske utformar en viss statlig befogenhet på samma, eller i stort sett samma, sätt. Skydds- och kontrollmekanismer, eller de sätt som dessa tillämpas, kan emellertid variera mellan de båda staterna. Detta kan innebära att den skyddsmekanism X – som varit av avgörande betydelse för att kunna konstatera att stat A:s lagar varit godtagbara – saknas i stat B, eller existerar på papperet men tillämpas inte i praktiken, med följden att stat B inte anses efterleva konventionen.[3]

I detta avseende kan man notera att stater som är parter i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) är skyldiga att ta hänsyn till mål som rör andra stater. Inom ramen för artikel 46 EKMR ska staterna enbart förbinda sig att ”rätta sig efter domstolens slutgiltiga dom *i varje mål där de är parter*”. Det allmänna åtagandet i artikel 1 att ”*garantera* var och en, som befinner sig under deras jurisdiktion, *de fri- och rättigheter som anges i avdelning I av denna konvention*” innebär emellertid att den nationella lagstiftaren, och de nationella domstolarna, inte kan ignorera ärenden som rör andra stater. Samtidigt är det tolkningsutrymme som den nationella lagstiftaren och den nationella domstolen har vid tillämpning av rättspraxis som rör andra stater större, eftersom skillnaderna mellan de

[3] Det är naturligtvis mycket viktigt att domstolen förstått den svarande statens lagar och förfaranden till fullo. Om och när domstolen grundar sitt beslut på en missuppfattning av dessa undergrävs inte bara värdet av målet som en rättslig källa för den svarande staten, utan också för alla andra avtalsslutande parter.

två faktiska situationerna (den föreliggande situationen och den situation som Europadomstolen har hanterat) oftast är större.

En nationell lagstiftare kan i fråga om Europadomstolens rättspraxis beträffande andra stater förledas att betrakta frågan om huruvida dess lagstiftning efterlever konventionen som ”oklar”. Man kanske vill invänta ett domslut i ett mål mot det egna landet rörande liknande frågor, eller åtminstone ett tydligt avgörande från stora kammaren. (Ett av de huvudsakliga syftena med stora kammaren, som består av 17 domare, är att den ska se till att Europadomstolens rättspraxis är konsekvent.) Att ignorera rättspraxis från andra länder innebär dock att man åsidosätter skyldigheten i artikel 1 att garantera rättigheterna i konventionen.

Vi får inte glömma att EKMR är avsedd att vara en minimistandard.[4] I en situation där det är relativt tydligt att Europadomstolens rättspraxis starkt tyder på att en lag eller ett förfarande inte efterlever konventionen ska den nationella lagstiftaren inte ”balansera på gränsen” till vad som är tillåtet.[5] Detta gäller framför allt lagstiftare som verkligen vill undvika att tvinga landets domstolar att behöva ”skriva om” omfattande lagregler som visar sig bryta mot konventionen.[6] En stats strävan efter att se till att det inte råder någon tvekan om att man uppfyller sina skyldigheter inom ramen för konventionen bör också stärkas av att domstolen tillämpar en ”teleologisk” tolkningsmetod. Denna metod innebär att rättigheterna tolkas för att uppfylla de behov som finns i samhället i dag, vilket i sin tur innebär att de krav som ställs på staterna kan öka med tiden.

Som framgår nedan har kravet i domstolens rättspraxis på att åtgärder ska ha ”stöd av lag” utvecklats som ett skydd mot maktmissbruk. I detta sammanhang bör man vara medveten om att betydelsefulla skydd kan ”inbegripas” i ett lands rättskultur. Domstolen har emellertid dåliga förutsättningar för att kunna bedöma

[4] I detta avseende vill jag påpeka att en förstärkning av det konstitutionella skyddet av personlig integritet (regeringsformen 2:6) (prop. 2009/10:80) ska träda i kraft den 1 januari 2011: ”[…] var och en gentemot det allmänna [är] skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden”.

[5] Jfr SOU 2001:25, s. 331 ”balansera på gränsen till vad som kan tänkas strida mot grundläggande mänskliga rättigheter”.

[6] Detta klargjordes upprepade gånger i de förberedande rättsakterna för lagen om inkorporering, prop. 1993/94 117. De svenska domstolarna, för sin del, kräver ”klart stöd” i Europadomstolens rättspraxis innan man ”för att man med hänvisning till [EKMR] ska underkänna den ordning som gäller enligt intern svensk reglering”. Se NJA 2000 s. 622, NJA 2004 s. 840, och NJA 2010 s.268 I-II.

effektiviteten av skyddet som finns i rättskulturen.[7] Vilka de formella rättsliga skyddsmekanismerna än är så kan polis och åklagare genom professionalism, utbildning etc. i praktiken efterleva höga etiska normer när de utreder brott. Men domstolen har, enkelt uttryckt, haft svårt att säga öppet till stat A: ”Visserligen ansåg vi inte att stat B bröt mot konventionen i ett tidigare fall som liknar det föreliggande fallet, men vi kom till denna slutsats eftersom stat B:s polistjänstemän är bättre utbildade, har bättre resurser och uppför sig relativt väl, medan inget av detta stämmer in på era polistjänstemän.”

Ytterligare en utveckling som förstärker behovet av en mer formell reglering är att rättskulturella skyddsmekanismer kan bli föremål för påtryckningar och förändras med tiden. I detta avseende vill jag påpeka att kulturer inom polisväsenden och åklagarmyndigheter i allt högre grad kommer i kontakt med varandra över nationella gränser inom EU. Det finns ett uppenbart behov av ett ökat internationellt samarbete i hanteringen av gränsöverskridande brottslighet. Stöd inom EU baseras i allt högre grad på principen om ömsesidigt erkännande av domar i brottmål. Tanken är att polis och åklagare ska kunna erbjuda kolleger i andra EU-medlemsstater samma åtgärder som de själva använder för utredning och lagföring av brottslighet. Gemensamma utredningsgrupper blir allt vanligare, även om de fortfarande inte förekommer så ofta. Under dessa omständigheter räcker det inte att förlita sig på skyddet i den nationella rättskulturen. Det finns ett ökat behov av förtydliganden av tillämpliga lagtexter och av uttryckligt lagstadgade skyddsåtgärder mot missbruk.

I rapporten anger jag de uttryckliga normer som fastställts av domstolen. I de fall där dessa är otydliga har jag försökt extrapolera dem utifrån logiken i domstolens rättspraxis som helhet och min egen kunskap på området. Jag har försökt att göra en korrekt identifikation av vilka delar av rapporten som består av domstolens normer och vilka som består av min egen tolkning av dessa.

[7] Jfr Cameron, 2000, s. 258: ”I praktiken är mervärdet av extern kontroll huvudsakligen beroende av det politiska klimat i vilket övervakaren arbetar, tjänstemannens engagemang och kompetensen inom dennes personal. Dessa saker utgör en ganska abstrakt beslutsgrund långt borta i Strasbourg. Domstolen är, vilket redan nämnts, relativt dåligt utrustad för att bedöma huruvida *formella* skydd är *riktiga* skydd, och det är den medveten om.”

2 En typologi över spaning och något om infiltration

Spaning och tillgång till uppgifter blir alltmer nära förbundna till varandra. Vad gäller digitala uppgifter är det svårt att särskilja mellan ”lagrade” och ”överförda” uppgifter, eftersom formen på och innehållet i de uppgifter som lagrats i ett datorsystem kan ändras mycket snabbt, eller till och med uppdateras automatiskt genom kommunikation med en annan dator. Detta innebär i sin tur att det i praktiken kan vara svårt att särskilja en ”sökning” i en databas från ”avlyssning” av samtal. I konventionen fastställs dessutom krav när det gäller den rättsliga ramen för regleringen av dessa databaser, i den mån registrering av enskilda sker. Även dessa krav är relevanta för denna rapport. Jag har emellertid inte beskrivit dessa krav i detalj.

I samband med föreliggande rapport är det lämpligt att dela upp de tekniska spaningsmetoderna i åtta olika grupper. Den första är *buggning*, användning av dolda mikrofoner för att höra samtal som övervakaren inte är delaktig i. De andra och tredje är *dold* respektive *öppen visuell spaning*, vilket innebär att man använder utrustning för att övervaka *och göra bildupptagningar*. En undergrupp i detta sammanhang är användning av avancerad bildgenerering, som radarutrustning eller infraröda kameror, för att fånga upp aktivitet inne i byggnader eller i andra svåra spaningssituationer. Sådan utrustning kan manövreras manuellt eller fjärrstyras. Vid den fjärde spaningsmetoden används mikrofon och inspelningsutrustning för att ta upp ett samtal där övervakaren själv deltar. Samtalet kan föras och spelas in via telefon eller på en privat eller offentlig plats (”dold kroppsmikrofon” eller *ljudupptagning i samband med eget deltagande*). Delaktigheten i samtalet är öppen, men inte inspelningen. Spaningen är följaktligen fortfarande dold. Den femte metoden är videomotsvarigheten till den fjärde, nämligen användning av en dold kamerautrustning för att dokumentera en händelse som övervakaren är delaktig i (*bildupptagning i samband med eget deltagande*). De fjärde och femte spaningsmetoderna kan naturligtvis kombineras. Den sjätte typen är *teleavlyssning*, som innebär *avlyssning av telemeddelanden* som övervakaren själv inte sänder eller mottar. Detta brukade kallas för telefonavlyssning, men nuförtiden omfattar begreppet ”telemeddelanden” även radio-, mikrovågs- eller satellitkommunikation samt fax, e post och andra kommunikationsformer mellan eller via datorer. Vid den sjunde spaningsformen identifieras den grupp av personer eller teleadresser som den övervakade personen kommunicerar med (*teleövervakning*). Med den åttonde spaningsmetoden

inhämtar man vad som kan kallas *lokaliseringsuppgifter*, som visar ett föremåls eller en persons fysiska position. Man kan exempelvis fysiskt placera ut en dold sändare som avger en radiosignal som visar föremålets eller personens geografiska position. Användning av rörelsesensorer hör också hemma inom denna metod. Det kan emellertid ske en överlappning mellan den sjunde och den åttonde kategorin, i och med att pejling av en persons användning av en mobiltelefon eller bärbar dator uppkopplad mot Internet både ger information om position och om vem, eller vad, den övervakade personen kommunicerar med. En mobiltelefon som är påslagen eller en bärbar dator som är uppkopplad mot Internet sänder ut regelbundna signaler till de närmaste mottagarstationerna. På så sätt kan den övervakade personens position kartläggas med större eller mindre precision, beroende på signalens styrka i förhållande till de närmaste mottagarstationerna. Lokaliseringsinformation kan också inhämtas genom den övervakades användning av olika sorters plastkort som innehåller datachip eller elektromagnetiska band som sänder elektroniska signaler till offentliga eller privata databaser. Dessa signaler har sidoeffekten att de anger den övervakade personens position (t.ex. bankomatuttag, inträde i en zon som kräver nyckelkort, bibliotekslån). När jag hänvisar till både kategori sju och kategori åtta använder jag termen ”inhämtning av uppgift om elektronisk kommunikation”.

Det bör betonas att maktbefogenheter, precis som vatten, tenderar att söka sig till platsen för minst motstånd. Om ett spaningsområde har blivit föremål för hård kontroll, eller om detta område har förbjudits helt och hållet, finns risken att polis och säkerhetstjänster försöker få tag på samma information på andra sätt. Detta borde göra det ännu viktigare att reglera hela området för statlig övervakning.[8]

Även om jag har särskiljt dessa olika metoder bör de inte betraktas som vattentäta kategorier. Ovan angivna spaningskategorier kan, förutom att de kräver olika typer av utrustning, särskiljas utifrån huruvida de tillämpas efter en viss händelse eller samtidigt som den sker (i ”realtid”). Teleövervakning är ett exempel på spaning i efterhand. Att placera ut en dold sändare som anger geografisk position sker i realtid, medan de flesta andra former av lokaliseringsinformation (t.ex. uppgift om bankomatuttag), åtminstone som

[8] Jfr Lustgarten och Leigh 1994, s. 44.

tekniken ser ut i nuläget, kan inhämtas först en stund efter att händelsen ägt rum.

I fråga om infiltration kan följande sägas. Infiltration kan beskrivas som en ”särskild utredningsmetod”, där man använder informatörer/källor (privatpersoner) eller polisinfiltratörer (polis- och tulltjänstemän osv.) för att inhämta information från misstänkta och andra om lagöverträdelser som planeras, begåtts eller pågår. Gränslinjen mellan infiltration och ”vanligt” polisarbete, som också kan omfatta dold visuell observation eller avlyssning och användning av informatörer, är inte benhård.

Infiltration är en nödvändig del av polisens metoder när det gäller att hantera brottslighet, i synnerhet organiserad brottslighet. När en privatperson används för att nästla sig in i en förmodad kriminell verksamhet uppstår dock en rad problem när det gäller ansvar. Informatörens/källans verksamhet kan bli föremål för olika grader av (brist på) kontroll från ”hanterarens” sida inom polisen. Och problem kan uppstå ur rättsstatssynvinkel i anslutning till både polisinfiltratörer och informatörer/källor, om dessa deltar aktivt i kriminell verksamhet.

Den amerikanska sociologen Marx skiljer mellan fyra olika former av polisiärt arbete på grundval av två kriterier: åtgärdernas öppenhet och om de är av vilseledande eller icke vilseledande natur.[9] Det ger oss en fyrfaldig typologi: *öppen och icke vilseledande* (som omfattar stora delar av det traditionella polisarbetet), *öppen och vilseledande* (t.ex. om en misstänkt luras av polistjänstemän att avge en bekännelse), *dold och icke vilseledande* (t.ex. spaningsverksamhet) och *dold och vilseledande*. Den fjärde kategorin omfattar både ”infiltrerande” polisverksamhet med polistjänstemän som agerar under täckmantel och informatörer/källor som hanteras eller drivs av polistjänstemän.

Det finns också ett tredje kriterium: interagerande mellan å ena sidan utredande myndigheter och å andra sidan vittnen, misstänkta och tredje parter, vilket ger en sexfaldig typologi.[10] Enligt denna klassificering skulle användningen av informatörer falla inom ramen för ”hemlig utredning av interagerande men inte vilseledande art”, medan förhållandet mellan en polistjänsteman som döljer sin identitet och en misstänkt eller en potentiell gärningsman skulle betraktas som ”hemlig utredning av interagerande och vilseledande

[9] Marx, 1988, s. 11–13. Jfr Helmius 2000, s. 28, som i stället tillämpar en åtgärdsskala utifrån graden av intrång i den personliga integriteten.
[10] Se Europeiska rådet, 2005, med hänvisning till Valkaneer, 2000, s. 24.

art". Dessa klassificeringar kan till viss del användas för att fastställa om, och i så fall hur, olika former av infiltrationsoperationer kan göra intrång i den personliga integriteten. Man bör emellertid inte fästa alltför stort avseende vid dem. En medveten användning av informatörer/källor för infiltration av en kriminell organisation betraktas exempelvis så gott som alltid som en till viss del vilseledande åtgärd. Den misstänkta/potentiella gärningsmannen kanske känner till den sanna identiteten på den person han/hon talar med, men inte att denne verkar som informatör/källa åt, eller efter instruktioner från, polisen.

3 Europadomstolens syn på artikel 8

Europadomstolen hanterar i allmänhet mål som väcker frågor inom ramen för artikel 8 på följande sätt. Först överväger den huruvida den åtgärd som blivit föremål för klagomål faller inom ramen för den aktuella rättigheten och huruvida denna rättighet kränks. Om man konstaterar att rättigheten har kränkts går man vidare med att överväga huruvida den åtgärd som staten vidtagit faller inom ramen för en av undantagsklausulerna, dvs. om den har vidtagits för att främja ett legitimt syfte. Därefter prövar domstolen huruvida överträdelsen kan sägas ha skett "med stöd av lag". Det fjärde och sista steget för domstolen är att ta ställning till huruvida överträdelsen "varit nödvändig i ett demokratiskt samhälle". Konventionsorganen tenderar att behandla steg tre och fyra som successiva hinder. Det innebär att de, om de kommer fram till att en åtgärd som blivit föremål för klagomål inte har "stöd av lag", inte går vidare med att undersöka huruvida åtgärden uppfyller kraven på att "vara nödvändig i ett demokratiskt samhälle".[11]

[11] Se t.ex. målen Malone mot Förenade kungariket, Huvig mot Frankrike och Kruslin mot Frankrike, som diskuteras nedan. Se emellertid också Kennedy mot Förenade kungariket nedan.

4 Allmänt om lagbegreppet i Europadomstolens rättspraxis

Europadomstolen har angett att de två uttrycken ”med stöd av lag” (i artikel 8) och ”föreskrivna i lag” i artiklarna 9, 10 och 11 borde hanteras på samma sätt.[12] Domstolen höll i målet Sunday Times mot Förenade kungariket fast vid att ”lagen” omfattar både gemensamma allmänna bestämmelser, lagar och sekundärlagstiftning.[13] Domstolen har till och med accepterat att ett kollektivavtal kan utgöra ”lag” i samband med den nordiska traditionen att överlåta regleringen av arbetsmarknaden till anställda och arbetsgivarorganisationer.[14] Domstolen angav i målet Sunday Times att en norm måste vara tillräckligt lättillgänglig och tillräckligt exakt formulerad för att räknas som en ”lag”.[15] Detta är inte ett rent formellt krav. Det är också knutet till kvaliteten på lagen i fråga. I målet Silver m.fl. mot Förenade kungariket klargjorde domstolen att en lag som ger utrymme för en obegränsad diskretionär prövningsrätt i enskilda fall inte har den nivå av förutsebarhet som är nödvändigt och i det sammanhanget följaktligen inte är en ”lag”. Räckvidden för prövningsrätten måste anges med rimlig precision. Domstolen har också framhållit att det måste finnas tillräckliga *skydd* mot *missbru*k av den lagstadgade prövningsrätten.[16] Även om dessa inte måste tas in i själva lagtexten måste åtminstone villkoren och förfarandena för ingripandet uppställas i lagen.[17] Det råder alltså en överlappning mellan kravet på ”lag”, kravet på att ”vara nödvändig i ett demokratiskt samhälle” och kravet på ett effektivt rättsmedel i artikel 13.[18] Den grad av förutsebarhet som krävs för att en spaningsåtgärd som staten vidtar ska kunna sägas uppfylla kraven på lagstöd kan exempelvis också tjäna som skydd mot maktmissbruk (som relaterar till åtgärdens ”nödvändighet”). Ibland väljer domstolen att fokusera på

[12] Ett enda uttryck används i den franska texten (*prévue par la loi*). Silver m.fl. mot Förenade kungariket, 25 mars 1983, serie A/61, punkt 85. Se vidare van Dijk och van Hoof, 2006, s. 336. Även om frasen som sådan förekommer i artiklarna 8–11 anges också i andra artiklar i konventionen stöd enligt ”lag” underförstått eller uttryckligen som villkor för ett ingripande i en rättighet.
[13] Sunday Times mot Förenade kungariket, punkt 47.
[14] Wretlund mot Sverige, mål nr 46210/99, beslut av den 9 mars 2004 (åläggande av anställd vid kärnkraftverk att genomgå ett drogtest: otillåtet).
[15] Ibidem, punkt 49.
[16] Se t.ex. Silver m.fl. mot Förenade kungariket, punkterna 88–89.
[17] Klass mot Förbundsrepubliken Tyskland, mål nr 5029/71, rapport av den 9 mars 1977, punkt 63. Kruslin mot Frankrike, 24 april 1990, A/176 A, punkt 35, Huvig mot Frankrike, 24 april 1990, A/176 B, punkt 34.
[18] Se Ruiz, 1997, s. 183–184.

skyddsåtgärderna inom ramen för kravet på ”nödvändighet”.[19] Så kan vara fallet om det finns utrymme för tvekan om huruvida skyddsåtgärdernas funktion i praktiken överensstämmer med funktionen på papperet. I de flesta fall verkar domstolen emellertid tycka att det är lättare att fastställa att staten inte har uppfyllt kravet på lagstöd.

Kraven på förutsebarhet och tillgänglighet varierar beroende på lagens innehåll, vilket område den har utformats för och mottagarantalet ochstatus. I målet Groppera Radio mot Italien var exempelvis ”lagen” en föreskrift som riktades till radioföretag och som hänvisade till tekniska bestämmelser i vissa internationella fördrag på området för telekommunikation. Domstolen ansåg likväl att mottagarna hade, eller borde ha haft, tillgång till den experthjälp som krävdes för att förstå innehållet.[20] I målet Rekvenyi mot Ungern var en av frågorna huruvida en grundlagsfäst bestämmelse som innebar att polisen förbjöds att delta i politisk verksamhet var tillräckligt tydlig för att vara ”förutsebar” i avsaknad av normer för tillämpningen. Domstolen ansåg att så var fallet.[21] Inom området för straffrätt och brottmålsförfarande samt i andra mål där mottagarna är vanliga medborgare och intrånget i enskilda rättigheter är allvarligt, är risken för maktmissbruk större och konventionsorganen har i vissa fall varit mer krävande.[22]

Domstolen är dock medveten om svårigheten att utforma lagar. I målet Gorzelik m.fl. mot Polen[23] framhöll domstolen att ”det är en logisk följd av principen att lagar måste ha allmän giltighet att utformningen av lagar inte alltid är exakt. Behovet av att undvika överdriven rigiditet och att hålla jämna steg med ändrade förhållanden innebär att många lagar oundvikligen formuleras på ett mer eller mindre vagt sätt. Hur sådana rättsakter tolkas och tillämpas beror på praxis … Man får inte glömma att tillämpningen, hur tydligt utformad en lagbestämmelse än är, oundvikligen möjliggör en viss tolkning av domaren, eftersom tveksamma punkter alltid kommer att behöva utredas och bestämmelsen måste anpassas till särskilda omständigheter. Ett utrymme för osäkerhet i samband med tvek-

[19] Se S och Marper mot Förenade kungariket, mål nr 30562/04 och 30566/04, den 4 december 2008, och Bykovmålet, som tas upp nedan. Jag anser att detta sätt att gå till väga är bättre än det försök att tolka in skyddsåtgärder i begreppet ”med stöd av lag” som domstolen gjort tidigare i en rad mål, som Rotaru mot Rumänien, nr 28341/95, den 4 maj 2000.
[20] Punkt 68 i anförda arbete.
[21] Dom av den 20 maj 1999.
[22] Jfr Sunday Times mot Förenade kungariket, punkt 49, och Maestri mot Italien, mål nr 39748/98, beslut av den 17 februari 2004 med Cantoni mot Frankrike, av den 15 november 1996.
[23] Mål nr 44158/98, dom av den 17 februari 2004.

samma frågor gör inte i sig tillämpningen av en rättsbestämmelse oförutsebar. Inte heller innebär enbart det faktum att en sådan bestämmelse kan tolkas på mer än ett sätt att den inte uppfyller kravet på ”förutsebarhet” enligt konventionens syften. Det är i själva verket domstolarnas uppgift att just undanröja kvarstående tolkningsosäkerhet med beaktande av förändringar i den vardagliga praxisen.[24]

Utöver hänvisningarna till förutsebarhet och behovet av att utforma lagar och upprätta skydd för att undvika maktmissbruk har domstolen inte angett i detalj vilka underliggande värden som skyddas av kravet ”med stöd av lag”. Kravet betraktas ofta som ett uttryck för ”rättsstatsprincipen”. I den mån det sträcker sig bortom styrning genom lag är dock rättstatsprincipens innehåll föremål för diskussion. Det verkar i grund och botten bestå av det som författaren vill att det ska bestå av, och har därför ett begränsat teoretiskt värde.[25] Det finns enligt min uppfattning tre värderingar bakom tanken med lagstiftning: förutsebarhet/stabilitet, demokratisk legitimitet och institutionell kompetens. Vad gäller den första av dessa innebär principen om normhierarki, som i svensk lag uttrycks i regeringsformens 8 kap. 18 §, att lagstiftning enbart kan ändras genom lagstiftning. Reglering genom lagstiftning är följaktligen både stabilare och tydligare än reglering genom sekundärlagstiftning. Vad gäller den senare behöver man inte säga mycket. Demokrati har varit den styrande principen för den traditionella västerländska politiska organisationen i nästan 100 år (och har påverkat det västerländska politiska tänkandet i mycket hög grad långt dessförinnan).

Den tredje värderingen har samband med den tid och det kunnande som parlamentet har att tillgå för att utforma lämpliga allmänna regler, och med fullständighet av den debatten (med beaktande av alla relevanta faktorer) som följer, eller borde följa, diskussionen kring ett lagstiftningsförslag. Tidigare har domstolen inte uppmärksammat värdet av reglering genom lag stiftad av lagstiftaren i tillräcklig grad när den har beaktat rättsstatsprincipen. Det finns troligen två orsaker till detta. För det första accepterar domstolen, vilket har påpekats ovan, att allmänna regler alltid måste tolkas och utvecklas genom rättspraxis. Dessutom är Storbritannien och Irland *common law states*, som accepterar, och faktiskt välkomnar, att en förhållandevis stor del av rättsordningen består av regler som har kommit till genom rättspraxis. Man kan inte ”ogiltigförklara” stora delar av de rättsordningar som två av grundarna av

[24] Ibidem, punkterna 64–65 (hänvisningar saknas).
[25] Jfr Loughlin 2009.

Europarådet har. För det andra finns det i alla europeiska länder, oavsett om makten innehas av parlamentet eller av en president, en mycket stor andel icke-parlamentariskt producerad normgivning som antingen baseras på befogenheter som delegerats av parlamentet eller vilar på regeringens egen normgivningskompetens enligt grundlagen.[26] Efter att ha sagt detta har Europadomstolen nu, vilket framgår nedan, börjat insistera på *lagreglering* när det gäller hemlig övervakning.

5 Vad är ett ingrepp enligt artikel 8?

5.1 Innehållet i artikel 8

Genom artikel 8 garanteras fyra enskilda rättigheter, även om det förekommer en hög grad av överlappning mellan dem. Samma statliga åtgärd kan innebära intrång i t.ex. både rätten till ”familjeliv”, ”privatliv”, ”hem” och ”korrespondens”.[27] ”Familjeliv” är inte direkt relevant för den här undersökningen, men det är de andra tre rättigheterna. I artikel 8 hänvisas det till ”skydd” för de rättigheter som anges. Det innebär att det inte är alla åtgärder som *påverkar* en angiven rättighet som utgör ett *intrång* i nämnda rättighet.[28] Jag bör också betona att det faktum att något anses göra intrång i (eller ”interferera med”) en av de rättigheter som nämns i artikel 8 inte innebär att det är en *överträdelse* av artikeln, utan enbart att intrånget måste motiveras.

[26] Jfr RF 8:7 (lydelse efter 1 januari 2011).
[27] Man kan hävda att en åtgärd som interfererar med både rätten till privatliv och hem borde granskas ännu noggrannare. Jfr Ovey och White, 2006, s. 218 ”det faktum att rättigheterna grupperas samman i samma artikel stärker det skydd som artikeln ger, eftersom varje enskild rättighet förstärks i sammanhanget”.
[28] Harris, et al. 2009, s. 381.

5.2 Hem och korrespondens

5.2.1 Allmänt

Begreppet ”hem” kan under vissa omständigheter utvidgas till att omfatta affärslokaler.[29] Att placera en avlyssningsutrustning i ett hem[30] eller använda ett ombud eller en informatör som bär en avlyssningsutrustning på sig (”*ljudupptagning i samband med eget deltagande*” eller ”dold kroppsmikrofon”)[31] i hemmet är en åtgärd som tydligt inskränker rättigheten i artikel 8.1. Begreppet ”hem” har ansetts omfatta ett garage som ägs av den övervakade men finns på en annan plats än hemmet, samt en annan persons hem som den övervakade besökt.[32] Utifrån denna rättspraxis verkar det framgå ganska tydligt att också andra typer av avlyssningsutrustning, som kan fånga ljud på avstånd och som inte fysiskt *placeras* i hemmet utan *riktas* mot det, innebär ett intrång i hemmet.[33] Det kan också

[29] Niemietz mot Tyskland, den 16 december 1992, A/251 B, punkterna 27–33. Domstolen framhöll också i detta mål (som rörde husrannsakan av en jurists kontor och beslagtagande av dokument) att ”privatliv” på samma sätt kan omfatta affärsverksamhet. Detta synsätt är utan tvekan förnuftigt. Internet och utvecklingen inom kommunikationsteknik innebär att många människor lätt kan arbeta från sin bostad. Domstolen har bekräftat detta synsätt i en rad senare mål, t.ex. i Buck mot Tyskland, mål nr 41604/98, den 28 april 2005. I målet Stés Est m.fl. mot Frankrike, nr 37971/97, den 16 april 2002, gick domstolen så långt som att tillämpa skydd för ”bostaden” på juridiska personers lokaler: ”Domstolen konstaterar, utifrån sin dynamiska tolkning av konventionen, att man i detta läge anser att de rättigheter som garanteras genom artikel 8 i konventionen under vissa omständigheter kan tolkas så att de omfattar en rätt till respekt för ett företags säte, filialer eller andra affärslokaler” (se punkt 41).

[30] Se de tidigare kommissionsmålen Redgrave mot Förenade kungariket, mål nr 20271/92, beslut av den 1 september 1993: otillåtet, och Govell mot Förenade kungariket, mål nr 27237/95, rapport av den 14 januari 1998, Khan mot Förenade kungariket, mål nr 35394/97, ECHR 2000 V, punkterna 26–28, Chalkley mot Förenade kungariket, mål nr 63831/00, dom av den 2 juni 2003.

[31] Heglas mot Republiken Tjeckien, mål nr 5935/02, dom av den 1 mars 2007 (bristande rättslig ram vid den tidpunkten för reglering av kroppsmonterad avlyssningsutrustning och mätarinformation), Bykov mot Ryssland, mål nr 4378/02, dom av den 21 januari 2009.

[32] Se Hewitson mot Förenade kungariket, mål nr 50015/99, dom av den 27 maj 2003 respektive Armstrong mot Förenade kungariket, mål nr 48521/99, dom av den 16 juli 2002. Se också Vetter mot Frankrike, mål nr 59842/00, dom av den 31 maj 2005 (utplacering av mikrofoner av polisen i en bostad tillhörande en person som den övervakade besökte). Å andra sidan betraktades en skådespelares loge inte som en del av dennes ”hem” i målet Hartung mot Frankrike, nr 10231/07, dom av den 3 november 2009. I Bykovmålet hävdade regeringen att det pensionat där avlyssningen med delaktighet ägde rum (se nedan) inte utgjorde en del av sökandens ”hem”. Domstolen framhöll helt enkelt att det hade gjorts intrång i sökandens rätt till privatliv.

[33] Jfr de amerikanska rättsfallen beträffande avsökning av bostäder utifrån med värmekameror för att fånga onaturligt höga värmeutsläpp, som skulle kunna visa på förekomsten av natriumlampor, som används vid odling av marijuanaväxter, USA mot Robinson, 62 F. 3rd 1325 (*Circuit Court* [motsv. domkrets] nr 11 1994) och USA mot Kyllo, 9630333v2 (*Circuit Court* nr 9 1998). Det fjärde tillägget till Förenta staternas konstitution föreskriver huvudsakligen rätt till skydd mot ”husrannsakan utan tillstånd”, och detta förfaringssätt ansågs inte utgöra en sådan husrannsakan i något av dessa två fall.

”med säkerhet sägas” att det skulle vara i strid mot artikel 8.1 att rikta visuell spaning mot en person som befinner sig i sin bostad.[34] Sådana åtgärder innebär dock också i de flesta situationer, vilket diskuteras nedan, ett intrång i privatlivet.

”Korrespondens” omfattar inte bara användning av post- och telefonitjänster[35], utan också telegram, faxmeddelanden, e-post och Internetanvändning.[36] Korrespondens behöver inte var hänförlig till ens ”privatliv” utan omfattar alla möjliga sorters korrespondens, inklusive sådan som skickas till och från arbetsplatsen.[37] I målet Halford mot Förenade kungariket drog domstolen slutsatsen att telefonsamtal som gjorts i affärslokaler på ett slutet telenät föll under begreppet privatliv (och korrespondens) och på så sätt kunde skyddas mot avlyssning genom artikel 8.[38] Ärendet rörde en överordnad polistjänsteman som hade förbigåtts när det gäller befordran vid ett antal tillfällen och som hade väckt talan vid en arbetsdomstol under åberopande av diskriminering på grund av kön. Senare misstänkte hon att både hennes hemtelefon och arbetstelefon hade avlyssnats i ett försök att inhämta användbar information mot henne under det rättsliga förfarandet. Den svarande staten medgav att telefonen på hennes arbetsplats hade avlyssnats. Domstolen noterade att Halford inte hade fått någon varning om att hennes kontorstelefon skulle avlyssnas och att hennes ”rimliga förväntningar på skydd av privatlivet” förstärktes av att hon inte delade kontor med någon, att hon hade två telefoner, varav en var särskilt avsedd för privat bruk, och att hennes chef i ett meddelande hade försäkrat henne om att hon kunde använda telefonerna på sitt kontor för att förbereda könsdiskrimineringsmålet.

Ett liknande tillvägagångssätt tillämpades i målet Amann mot Schweiz, där sökandens, en affärsman, telefonsamtal till och från kontoret registrerades[39], och i målet Copland mot Förenade kungariket,

[34] Naismith, 1996, s. 152. Se också domstolens rättspraxis nedan beträffande fotografering av en person utanför hemmet.
[35] Konventionsorganen accepterade också i ett tidigt skede att *teleavlyssning* innebär ett intrång i rätten till skydd av ”korrespondens”. Se Klass mot Förbundsrepubliken Tyskland, dom av den 6 september 1978, A/28, punkt 40.
[36] Se PG och JH mot Förenade kungariket, mål nr 44787/98, dom av den 25 september 2001, punkt 42, Copeland mot Förenade kungariket, mål nr 62617/00, dom av den 3 april 2007 och Liberty mot Förenade kungariket, mål nr 58243/00, dom av den 1 juli 2008, nedan. Se nedan beträffande frågan om dold tillgång till uppgifter som finns på en persons dator eller på en server och som inte överförs.
[37] PG och JH, ibidem och Niemietz, punkt 32.
[38] Halford mot Förenade kungariket, dom av den 25 juli 1997, punkterna 42–46.
[39] Dom av den 16 februari 2000, diskuteras vidare nedan.

som omfattade övervakning av en offentliganställds telefoner och tillgång till Internet på kontoret.[40] I Coplandmålet lade domstolen, liksom i fråga om situationen i Halford-målet, betoningen på sökandens rimliga förväntningar på skydd av privatlivet. Hon hade inte informerats om att bl.a. hennes Internetanvändning skulle kunna komma att övervakas.

Det framgår tydligt att domstolen anser att ”korrespondens” kan genomföras utanför hemmet och att den också måste skyddas utanför hemmet.[41] Jag vill dessutom påpeka att skyddet för korrespondens har konsekvenser för föreningar. Även om en förening som sådan (till skillnad från medlemmarna) kanske inte har rätt till skydd för något privatliv så har den rätt till skydd för korrespondens.[42]

Vad gäller att inskaffa information om de teleadresser som en person eller en grupp människor använder när de kommunicerar (s.k. hemlig teleövervakning) fastslog domstolen så långt tillbaka som 1986 i målet Malone mot Förenade kungariket att detta utgör ett intrång i privatlivet.[43] Det bör påpekas att den typ av uppgifter som tillhandahålls med hemlig teleövervakning har förändrats betydligt med uppkomsten av mobiltelefoner och Internet. Nu får man genom mobiltelefoner uppgifter om lokalisering (beaktas nedan) och genom kontroll av surfande på Internet uppgifter om vilka webbplatser som besökts. Senare kommer jag att ta upp vilken sorts reglering, och vilken nivå på regleringen, som krävs för att man ska få tillgång till sådana uppgifter.

Domstolen har vidare framhållit att *teleavlyssning i sig självt* utgör ett intrång i privatlivet.[44] Det har ingen betydelse om man sedan inte *använder* inspelningarna. Domstolen har i samband med strategisk övervakning (se nedan) också framhållit att själva förekomsten av detta är ett intrång i de berörda personernas (som skulle kunna

[40] Anfört arbete.
[41] Förekomsten av mobiltelefoner och bärbara datorer innebär ändå att det vore orealistiskt att dra en gräns mellan teleavlyssning och bevakning av e postmeddelanden ”inom” och ”utanför” hemmet.
[42] *Association for European Integration and Human Rights* [förening för europeisk integration och mänskliga rättigheter] och Ekimdzhiev mot Bulgarien, mål nr 62540/00, dom av den 28 juni 2007 (föreningen kunde hävda att den var ”offer” för en lag som ger tillstånd till hemliga övervakningsåtgärder).
[43] Malone mot Förenade kungariket, punkterna 83–88. Ministerkommittén intog också den ståndpunkten att sådan information bör vara konfidentiell, utom när den måste avslöjas av skäl som rör den nationella säkerheten, brottsbekämpning etc. Skydd för personuppgifter på området för telekomtjänster, med särskild hänvisning till telefontjänster, rekommendation nr R(95)4, punkt 4.
[44] Kopp mot Schweiz, dom av den 25 mars 1998, punkt 37, se nedan.

vara en stor del av befolkningen) privatliv eller korrespondens. Man kan på samma sätt hävda att den skyldighet till lagring av uppgifter inom teletrafik som infördes genom ett EU-direktiv i sig självt utgör ett intrång i privatlivet.[45] Det faktum att en person vet att uppgifter om dennes Internetanvändning nu kommer att finnas tillgängliga för polisen och inte bara bevaras av tjänsteleverantören i faktureringssyfte kan mycket väl påverka vilka webbplatser som personen besöker.

Det är tre frågor beträffande ”hem” och ”korrespondens” som måste behandlas mer ingående. Den första är när det allmänna underlättar eller möjliggör för en enskild att utföra ljudupptagning i samband med eget deltagande, riktad mot en annan enskild.

5.2.2 Medverkan i enskilds ljudupptagning i samband med eget deltagande, riktad mot annan enskild

Bestämmelserna på detta område har varierat från stat till stat beroende på bland annat om medgivande krävs från alla samtalsparter för att en skadeståndsgrundande kränkning eller ett brott ska ha begåtts genom att ett förtroende har röjts, eller om det räcker att en enda samtalspart gör ett medgivande.[46] Före Bykovmålet (behandlas i avsnitt 5.2.3) var det ledande konventionsmålet på detta område A. mot Frankrike. I det fallet hade en informatör underrättat en högt uppsatt polistjänsteman om att han hade lejts av sökanden, A., för att döda en person. Han erbjöd sig att kontakta sökanden per telefon och att spela in samtalet. Polistjänstemannen gick med på detta. Telefonsamtalet genomfördes från polistjänstemannens kontor och spelades in med polisens inspelningsutrustning. År 1989 hade kassationsdomstolen i ett liknande mål fastställt att enbart en domare får godkänna inspelningen av ett telefonsamtal. Polisen fick inte göra detta själv under en förundersökning. Den franska regeringen medgav följaktligen att det inte fanns någon rättslig grund för inspelningen inom ramen för fransk lag. Domstolen fastställde därför som väntat att inspelningen inte skedde ”med stöd av lag”. Det intressanta här är emellertid att domstolen

[45] Se Breyer, 2005. Se vidare diskussionen om varför privatpersoners tillgång till telekommunikationsuppgifter inte leder till samma typ av frågor beträffande privatlivet i avsnitt 5.3 nedan.

[46] Se Joubert och Bevers, 1996, s. 157–170 för en kortfattad jämförelse mellan lagarna i fem stater i detta sammanhang. I Sverige kan olovlig avlyssning enbart begås av en person som själv inte är part i samtalet (brottsbalken, 4 kap., § 9 a).

ansåg att en privatpersons inspelning av ett samtal utgjorde ett intrång i en annan persons rätt till korrespondens när staten underlättade det. Detta synsätt bekräftades med domen i det senare målet M.M. mot Nederländerna.[47] Detta mål rörde inspelning av en persons inkommande, i stället för utgående, samtal. Man kan skilja mellan att helt enkelt underlätta inspelning av inkommande samtal och en situation av brottsprovokation där det allmänna kan sägas ha uppmuntrat en samtalspart (A) att ringa upp den andre (B) och att ha tillhandahållit A utrustning för att kunna spela in sådana kompromitterande uppgifter som B skulle kunna tänkas framföra.[48] Majoriteten i domstolen verkade emellertid inte göra någon sådan åtskillnad. Man får därför anta att majoriteten inte betraktar det som en motiveringsgrund för att inte reglera underlättande av inspelning av inkommande samtal. Jag vill tillägga att polisen, med tanke på hur lätt det är att få tag på utrustning för inspelning av hög kvalitet av telefonsamtal nu för tiden, inte borde behöva blandas in överhuvudtaget, utöver att helt enkelt råda en person att spela in hotsamtal etc. Men i den mån polisen anser att det skulle vara till nytta att underlätta inspelning av samtal verkar det stå klart att detta enligt konventionen kräver rättsligt stöd.

En fråga som hör hemma under denna rubrik är om det krävs ett lagstadgat bemyndigande för att polisen ska få tillgång till ett inspelat telefonsamtal mellan en privatperson och en larmcentral (SOS Alarm). Å ena sidan är personen, eller i alla fall borde vara, medveten om att en sådan konversation spelas in. Å andra sidan görs inspelningen i ett särskilt syfte (för att göra det lättare att snabbt fastställa vilket slags nödsituation det rör sig om och var den sker). I detta avseende liknar situationen den där information om lokalisering eller uppgift om elektronisk kommunikation inhämtas från en telefonioperatör (beaktas nedan i avsnitt 5.3.4).

5.2.3 Infiltration av hemmet

Den andra frågan rör om man gör intrång i en persons rätt till skydd för sitt hem om man skickar en informatör/källa eller infiltratör till

[47] Mål nr 39339/98, dom av den 8 april 2003. Se också Bykov- och Heglasmålen, anfört arbete.
[48] Se Palms skiljaktiga mening i detta mål och Mejyers särskilt yttrande i det senare målet Van Vondel mot Nederländerna, mål nummer 38258/03, dom av den 25 oktober 2007. Se också två beslut av justitieombudsmannen (JO 1996 dnr 1953 1995 och JO 1997/98:118) i vilka statstjänstemän kritiseras för att ha spelat in sina samtal med (oförskämda) privatpersoner utan att ha informerat dem om det. JO ansåg att detta var ett brott mot kravet ”med stöd av lag” som föreskrivs i artikel 8.

nämnda hem, även om denne inte bär dold inspelningsutrustning för ljud- eller bildupptagning. Privatlivet sträcker sig, vilket framgår nedan, utanför hemmet. Följaktligen kan också infiltration utanför hemmet väcka frågor rörande konventionen. Argumenten för att det enligt konventionen krävs lagstiftning för infiltration är dock starkast i samband med vistelse i en misstänkt persons, eller en tredje parts, hem.

En fråga i detta sammanhang är huruvida domstolens domslut i Bykovmålet visar på ett nytt synsätt. Tidigare, i målet Lüdi mot Schweiz[49], ansåg inte domstolen att användningen av en infiltratör, som skulle köpa narkotika av sökanden, utgjorde ett intrång i sökandens privatliv. Domstolen verkade inta en ståndpunkt liknande den som intogs av USA:s högsta domstol[50], nämligen att en person som deltar i kriminell verksamhet (X) underförstått gör avkall på rätten till privatliv när han eller hon talar med en annan person (Y), eftersom X borde vara medveten om att Y skulle kunna vara informatör eller polistjänsteman.[51] Sedan Lüdi-målet har Europadomstolen några gånger meddelat domar i mål rörande personer som har varit föremål för hemliga operationer som ingriper användning av informatörer/källor eller infiltratörer. Emellertid har frågan alltid, såvitt jag vet, snarare rört artikel 6 (rättvis rättegång) än frågan om huruvida själva aktiviteten utgör ett intrång i rätten i artikel 8 till skydd för hem och privatliv. I målet Ramanauskas mot Litauen,[52] ett mål om brottsprovokation avgjort på stor kammare, togs exempelvis inte artikel 8 upp. Det förelåg en uttrycklig lagstadgad grund för användningen av ”modeller för operativ simulering”, och förfarandet krävde tillstånd från riksåklagaren eller dennes ställföreträdare.

Enligt min uppfattning bör följande saker klargöras. Jag anser att man inte bör fästa alltför stor vikt vid Lüdimålet. Det utspelade sig år 1992, och domstolen behandlade frågan ytligt. Den organiserade brottsligheten har uppenbarligen ökat i Europa sedan dess och det är rimligt att anta att det har blivit vanligare att använda informatörer och infiltratörer för att infiltrera den organiserade

[49] Mål nr 12433/86, dom av den 15 juni 1992.
[50] Se Hoffa mot Förenta staterna, 385 US 293, 302 (1966) och Illinois mot Perkins, 496 US 292, 300 (1990). Se också Ross, 2007, s. 505.
[51] ”Därför måste Lüdi från och med då ha varit medveten om att han deltog i en brottslig gärning som är straffbar inom ramen för artikel 19 i narkotikalagstiftningen och att han följaktligen riskerade att komma i kontakt med en infiltratör inom polisen vars uppgift i själva verket skulle vara att avslöja honom” i punkt 40.
[52] Mål nr 74420/01, dom av den 5 februari 2008. Se Sallinen m.fl. mot Finland, mål nr 50882/99, dom av den 27 september 2005 och Taxquet mot Belgien, mål nr 926/05, dom av den 13 januari 2009.

brottsligheten. Man känner också bättre till de problem som följer av användningen av informatörer och infiltratörer. Kriminella personer kan t.ex. ge en infiltratör tillträde till lokaler utan att vara medvetna om att denne arbetar för polisen. I obevakade ögonblick kan han eller hon säkra samma mål som en operation som omfattar användning av traditionella öppna eller dolda tvångsmedel (husrannsakan eller beslag). Domstolen har många gånger betonat att sådana åtgärder måste ske inom ramen förjudiciell kontroll. Men om man ”lägger ut” dessa åtgärder på en infiltratör eller polistjänsteman som arbetar under täckmantel öppnas möjligheterna för att undvika befintligt rättsskydd.

Vad gäller länken mellan spaning och infiltration, en länk som fanns i Bykovmålet, går det att göra en åtskillnad mellan en situation där ett samtal med en informatör eller infiltratör spelas in och en situation där det inte spelas in. I det förstnämnda fallet har en inspelning vanligtvis ett större eller mycket större bevisvärde vid en efterföljande rättegång (inom vissa system tillåts man kanske inte ens presentera vittnesmål av en infiltratör eller informatör som rör innehållet i ett samtal med den åtalade). Frågan är samtidigt om skillnaden är relevant för frågan om det skett ett intrång i rätten till skydd för hemmet. I båda fallen har personen fått tillträde till hemmet och möjlighet att tala med den övervakade genom en (aktiv eller passiv) vilseledande åtgärd.

Olika typer av system för brottsutredning och lagföring används i olika europeiska länder. I vissa system, t.ex. inom ramen för den brittiska lagen om undersökningsbefogenheter från 2000, beslutar polistjänstemännen själva om användning av informatörer och infiltratörer, även om det skulle omfatta infiltration av hemmet. Det finns också länder där åklagaren beslutar om infiltration. Åklagaren kan, beroende på konstitutionellt system, tillhöra antingen den verkställande eller den dömande makten. En tredje metod för kontroll av infiltrationsåtgärder är att kräva godkännande från en undersökningsdomare. Domstolen betraktar förmodligen denna tredje metod som den starkaste formen av kontroll. I Lüdi-målet fäste domstolen verkligen vikt vid att operationen hade kontrollerats av en undersökningsdomare. Domstolen kan möjligen vara mindre krävande i fråga om tydligheten i ett lagstadgat bemyndigande för infiltration om en domstol är delaktig i godkännandet av infiltration som omfattar besök i hemmet (även om värdet av denna kontroll i praktiken kan skilja sig mellan olika länder, beroende på domares grad av oberoende från den verkställande makten).

Man kan hävda att åklagare i Sverige har en stark skyldighet att vara objektiva och tillhandahåller i många hänseenden en skyddsnivå motsvarande en undersökningsdomare. Samtidigt utgör de ur ett konstitutionellt perspektiv en del av den verkställande makten. Dessutom är riksåklagaren tillsatt av regeringen. Riksåklagaren (och överåklagare) har inte befogenhet att beordra underordnad åklagare att fatta ett visst beslut (jfr 20 kap. RB) men har befogenhet att överpröva eller ta bort mål från en underordnad åklagare.

I verkligheten har en svensk åklagare betydelsefulla konstitutionella garantier för oberoende av direkt statlig kontroll i enskilda ärenden (regeringsformens 11 kap. 7 § och efter den 1 januari 2011 regeringsformens 12 kap. 2 §). Dessutom skyddar den svenska rättskulturen (tillsammans med ett starkt konstitutionellt skydd för informationsfrihet och yttrandefrihet) åklagare från oegentliga avstängningar från enskilda ärenden av riksåklagaren. Det ska dock medges att det strukturella skyddet i Sverige är relativt svagt på papperet.

I vilket fall som helst kontrolleras inte alla brottsutredningar i Sverige av åklagare, eller ens majoriteten av dessa. Också vid utredning av allvarligare brott, där åklagaren undantagslöst involveras, kan denne mycket väl involveras i ett senare skede, efter att polisen har genomfört en infiltrationsoperation.

I Storbritannien fattades 2000, vilket redan har nämnts, beslutet att införa en uttrycklig lagstadgad grund för all användning av personer som dolda underrättelsekällor samt administrativa riktlinjer och ett system för hierarkiskt bemyndigande och kontroll inom polisen, just för att polisen själv fattar beslut om infiltration.[53] I det

[53] I brittiska *Covert Human Intelligence Sources Code of Practice* [riktlinjer reglerande användning av personer som dolda underrättelsekällor] anges följande:
4.1 Enligt avsnitt 26.8 i lagen från 2000 är en person en källa om han eller hon a) upprättar eller upprätthåller en personlig eller annan relation till en person med som dolt syfte att underlätta utförande av allt som faller inom ramen för punkt b) eller c), b) i hemlighet utnyttjar en sådan relation för att inhämta information eller skaffa information för någon annans räkning, eller c) i hemlighet avslöjar information som inhämtats genom en sådan relation eller som en följd av en sådan relation.
4.2 En källa kan utgöras av infiltratörer, informatörer eller polistjänstemän som arbetar under täckmantel.
4.3 Ett syfte är enligt avsnitt 26.9 b i lagen från 2000 dolt i relation till upprättandet eller upprätthållandet av en personlig eller annan relation om, och enbart om, relationen sköts på ett sätt som är avsedd att se till att en av parterna i relationen inte känner till syftet.
4.4 Enligt avsnitt 26.9 c i lagen från 2000 används en relation i hemligt syfte, och avslöjas information som inhämtats enligt beskrivningen i punkt 4.1 c ovan i hemlighet om, och endast om, den används eller, i vederbörande fall, avslöjas på ett sätt som är avsedd att se till att en av parterna i relationen inte känner till den aktuella användningen eller avslöjandet.
4.5 Användning av en källa innebär t.ex. att förmå, be eller hjälpa en person att ta del av en källas agerande eller att skaffa information med hjälp av en sådan källas agerande.
(s. 20, http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/human-cop2835.pdf?view=Binary)

brittiska systemet hanteras också problemet med att upprätta en tröskel för ”infiltration”, med andra ord att skilja detta från den ”traditionella” användningen av informatörer eller civilklädda poliser som bara iakttar personer eller brottsplatser. Britterna använder sig av kriterierna riktning och kontroll. Man behöver naturligtvis inte välja den brittiska modellen. Även andra modeller kan konstrueras.

En annan relevant fråga som bör beaktas är landets regler för att utesluta bevismedel i syfte att garantera en rättvis rättegång. Även om frågan om reglering genom lagstiftning skiljer sig från frågan om en rättvis rättegång finns det ett tydligt samband mellan dessa två frågor i och med att det är slutresultatet som domstolen intresserar sig för. Något måste följaktligen sägas om detta, även om jag inte behöver gå in på detaljer om denna fråga i den här rapporten. I målet Teixeira de Castro mot Portugal[54], och senare i en rad andra domar och beslut[55], ansåg Europadomstolen att en nationell domstol måste överväga huruvida en infiltrationsoperation, när sådan har använts, undergräver rätten till en rättvis rättegång. Om infiltratörer eller informatörer/källor har gått så långt att de agerat som provokatörer måste bevisningen uteslutas. Vad gäller frågan om att presentera bevis som har införskaffats i strid med en materiell rättighet inom ramen för konventionen verkar det hittills som att det endast vid bevisning som införskaffats genom tortyr *automatiskt* innebär att rättegången strider mot artikel 6.[56]

Domstolen har alltså – hittills – uteslutit doktrinen om ”frukten från det förgiftade trädet” som ett sätt att förmå polisen att efterleva konventionens materiella rättigheter. Domstolen är medveten om att bevissystem, liksom förfaranden för godkännande av infiltration, varierar i betydande grad mellan olika länder. Domstolen vet också att effektiviteten hos de olika mekanismer som länder använder för att garantera att polisen följer reglerna varierar stort, liksom sanktionerna mot polistjänstemän som inte följer reglerna. Men det faktum att ”frukten från det förgiftade trädet” doktrinen har uteslutits talar för att domstolen i framtiden kommer att ställa

[54] Dom av den 9 juni 1998.
[55] Se framför allt Sequeira mot Portugal, mål nr 73557/01, ECHR 2003 VI, Taal mot Estland, mål nr 13249/02, dom av den 22 november 2005, Vanyan mot Ryssland, mål nr 53203/99, dom av den 15 december 2005, Eurofinacom mot Frankrike (dec.), mål nr 58753/00, ECHR 2004 VII, Khudobin mot Ryssland, mål nr 59696/00, dom av den 26 oktober 2006.
[56] Se Jalloh mot Förbundsrepubliken Tyskland, mål nr 54810/00, dom (GC) av den 11 juli 2006 och Gäfgen mot Förbundsrepubliken Tyskland, mål nr 22978/05, dom (GC) av den 1 juni 2010. Det sistnämnda målet rörde hantering av tillåtligheten av bevis på hot om fysiska skador från förhörsledare inom polisen.

hårdare krav så vitt gäller reglering av infiltration, som faller inom tillämpningsområdet för artikel 8.

Eftersom det är slutresultatet som är viktigt kan domstolen vara beredd att ge ”friare tyglar” till ett system som ger den tilltalade ett starkt skydd vid själva rättegången (dvs. utesluter bevis som bedöms ha införskaffats på ett illegitimt sätt). Detta stöds av målet Uzun mot Förbundsrepubliken Tyskland[57] som avgjordes nyligen. Det avsåg användning av en GPS-mottagare som i hemlighet placerats i en bil. Europadomstolen vägde in den tyska domstolens rätt att skönsmässigt utesluta bevis under rättegångsskedet, i analysen av huruvida de tyska föreskrifterna om GPS som lokaliseringsutrustning hade ”stöd av lag”.[58]

I detta sammanhang kan man notera att grundprincipen i fråga om bevisföring i Sverige är fri bevisprövning, även om de svenska domstolarna ibland har ingripit för att upprätthålla parternas likställdhet samt uteslutit eller gett ett lågt bevisvärde till olovligt åtkomna bevis.[59] Även om EKMR kan sägas undantagsvis kräva att en domstol måste utesluta bevisning skulle jag säga att det inte är önskvärt att göra detta till en ”standard regel” i Sverige.

Det finns andra skäl till varför lagreglering av infiltration är önskvärt. Den legalitetsprincip som gäller för åtal borde också leda till någon form av reglering av en situation där en informatör/källa eller infiltratör som ett led i en infiltrationsoperation bryter mot lagen. Och utifrån ett rättssäkerhetsperspektiv finns det naturligtvis nackdelar med att fokusera på skydd på rättegångsstadiet, eftersom flera, eller t.o.m. många, infiltrationsoperationer inte leder till åtal och rättegång. Det ökade internationella samarbetet (framför allt stöd som baseras på principen om ömsesidigt erkännande) innebär slutligen, vilket redan har nämnts, att behovet av ett förtydligande av lagen och av uttryckliga skyddsåtgärder mot missbruk har ökat.

---

[57] Mål nr 35623/05, dom av den 2 september 2010.

[58] Punkt 71. Se även Khudobin mot Ryssland, anfört arbete, ”domstolen påminner om att ett tydligt och förutsebart förfarande för godkännande av undersökningsåtgärder samt en ordentlig kontroll av dessa bör upprättas för att garantera myndigheternas goda tro och efterlevnad av lämpliga brottsbekämpningsmål. […] I detta fall hade polisens arbetssätt godkänts genom ett enkelt administrativt beslut av det organ som senare genomförde operationen. Det framgår av materialet om målet att beslutstexten innehöll väldigt lite information om anledningarna till och syftet med det planerade ”testköpet”. Det hade inte heller gjorts någon rättslig granskning av operationen, eller någon annan oberoende kontroll. I avsaknad av ett komplett kontrollsystem i samband med operationen […] fick den efterföljande kontroll som genomfördes av rättegångsdomstolen avgörande betydelse.”

[59] Se t.ex. RH 1995:32, NJA 1996 s. 649, RH 1997:95, NJA 1998 s. 204, NJA 2003 s. 323, NJA 2007 s. 1037, NJA 2007 s. 547, NJA 2009 s. 475.

Även om man inte kan säga att rättspraxisen inom konventionen i detta skede definitivt kräver en lagstadgad grund för infiltrationsoperationer som påverkar (för att inte säga faktiskt utgör intrång i) hemmet, så talar de faktorer som beskrivs ovan alltså för att detta bör införas i svensk lag. Det förnuftiga skulle vara att skapa ett ”skiktat” system för bemyndigande, där infiltrationsoperationer som påverkar hemmet (eller privatlivet utanför hemmet, se nedan) på ett mindre ingripande sätt skulle kräva endast beslut av ett högre polisbefäl. Åtgärder som påverkar hemmet eller privatlivet utanför hemmet på ett mer betydande sätt skulle kräva bemyndigande från åklagare och möjligen även från domstol.

Vad gäller att frågan om att involvera åklagaren i processen, kan man givetvis hävda att insamling av information är en uppgift för polisen och att det först är när informationen blir ”bevismaterial” som åklagaren bör involveras. Denna skiljelinje tillämpas emellertid inte alltid tydligt i praktiken. Enligt min uppfattning ligger det definitivt ett värde i att kräva bemyndigande från åklagare i fråga om infiltration som på ett mer betydande sätt påverkar hemmet eller privatliv utanför hemmet. Det ligger ett värde i att tvinga polisen att ”gå utanför huset” för att övertyga en person som ”befinner sig ett steg längre bort” från utredningen om behovet av att vidta en viss åtgärd. Samtidigt som polisen förväntas följa lagen kan man med rätta säga att åklagaren, på grund av sin utbildning, grupptryck och organisatorisk press, är under ännu starkare press att följa lagens bokstav och anda.[60] Dessutom är åklagare vana vid att balansera restriktioner av rättigheter mot behovet av effektivitet inom brottsutredning och lagföring. Jag behöver inte gå närmare in på dessa frågor. Det räcker att säga att det finns ett antal olika sätt att konstruera ett tillfredställande kontrollsystem. Ett skiktat bemyndigandesystem behöver inte vara oflexibelt. Det kan naturligtvis uppstå brådskande situationer även för infiltrationsoperationer i den ”allvarliga” änden av skalan (plötsliga infiltrationsmöjligheter osv.). Dessa situationer är dock knappast det vanliga och de skulle kunna hanteras med ett system för bemyndigande i efterhand.

Vad gäller huruvida det räcker att involvera åklagaren om Europadomstolen senare skulle klargöra att infiltrationen kan vara ett intrång i skyddet för hem/privatliv kan jag notera att en svensk åklagare, enligt domstolens rättspraxis, inte betraktas som ett tillräckligt oberoende kontrollinstrument i fråga om gripande och kvar-

[60] Se också avsnitt 6.4 nedan om värdet av preciserade regler.

hållande.[61] Det stämmer visserligen att det finns svagheter på papperet när det gäller svenska åklagares oberoende från verkställande kontroll. Det råder emellertid ingen tvekan om att åklagaren är oberoende av *polisen*. Inte heller finns det tvivel om att åklagaren i slutändan kan kontrollera polisen i samband med en förundersökning om och när denne så skulle vilja. Slutligen är de normer som finns i artikel 8 mer flexibla än vad gäller artikel 5. När det gäller infiltration av hemmet som inte omfattar inspelning (som diskuteras vidare nedan) *skulle* det kunna räcka med att ge infiltrationen en lagstadgad grund och upprätta de två första lagren av bemyndiganden och kontroll, nämligen bemyndigande från en överordnad polistjänsteman och bemyndigande från en åklagare – så länge som den svenska domstolen, med tillämpning av proportionalitetsprincipen, i rättegångsstadiet prövar frågan om bevis som har inhämtats på ett ”illegitimt sätt” bör uteslutas.

Efter att ha sagt detta måste det medges att Europadomstolen i Uzun-målet uttryckligen betonade att man var beredd att godkänna ett sådant system som beskrivs ovan (dvs. inget bemyndigande från domstol) enbart för att åtgärden att i hemlighet placera en GPS-mottagare i en bil innebar en *lägre* grad av intrång i privatlivet (diskuteras vidare i avsnitt 5.3.4). Följden av detta synsätt verkar bli att bemyndiganden för *betydande* intrång i privatlivet skulle kräva strängare kontroller, dvs. förhandskontroll av domstol.

5.2.4 Strategisk avlyssning av radioburen kommunikation

Den tredje frågan handlar om avlyssning av innehållet i telekommunikationer eller upptagning av uppgift om elektronisk kommunikation som framförs av radiovågor. Det kan antingen röra sig om specifika meddelanden eller om en allmän ”strategisk” bred övervakning. Man kan hävda att man inte kan förvänta sig att ens personliga integritet skyddas när radiovågor används, eftersom ”etern är fri”. All avlyssning av teletrafik som bärs av radiovågor kan alltså inte innebära ett överskridande av artikel 8.1. Vad gäller en bred kartläggning av uppgifter om elektronisk kommunikation eller en strategisk övervakning av samtalsinnehåll kan man dessutom hävda att man inte kan fastställa, åtminstone inte omedelbart, identiteten

[61] McGoff mot Sverige, den 26 oktober 1984, A/83. Se även Popescu mot Rumänien, nedan avsnitt 6.3.

på de personer som kommunicerar, vilket innebär att det inte sker något intrång i rätten till privatliv eller korrespondens.

Det finns ett visst stöd för detta påstående i äldre rättspraxis. I målet B.C. mot Schweiz hade sökanden använt en sladdlös telefon som sände på en radiofrekvens som var reserverad för civil och militär luftfartstrafik. Detta var ett brott enligt schweizisk lag. Den schweiziska telekommunikationsmyndigheten spelade in hans samtal och använde en radiopejlapparat för att lokalisera hans telefon. Eftersom sökanden valt att använda en apparat som använde en våglängd reserverad för andra syften än privata telefonsamtal ansåg kommissionen att sökandens samtal var tillgängliga för andra telekomanvändare och därför knappast kunde klassificeras som privata.[62]

Detta mål utgör emellertid inte längre (om det någonsin har varit det) något stöd för att anse att avlyssning av normala mobiltelefoner på lagliga frekvenser inte kommer i konflikt med artikel 8.[63] Det är en enorm skillnad mellan det stora antalet personer som kommunicerar via ”radio” i dag och det mycket begränsade antal personer som kommunicerade via kortvågsförbindelse på 1980-talet. Alla som har en mobiltelefon eller som använder trådlös Internetuppkoppling kommunicerar via ”radio”. Dessutom kan till och med telekommunikationsmeddelanden som går via kabel ledas via mikrovågor. Man kan emellertid inte hävda, som i fallet med kommunikation via kortvågsförbindelse, att en person som använder en bärbar dator eller mobiltelefon ”vet” att han eller hon kan avlyssnas. Trafik via mikrovågsradio i digital form kan inte avlyssnas och uppfattas av någon med en radiomottagare. Dessutom kan man argumentera att om ett system för sträng reglering av övervakning av kommunikation via kabel skulle kunna kringgås genom upptagande av kommunikationsinnehåll i det ögonblick då detta omvandlas till mikrovågor skulle systemet göras till åtlöje.[64] Europadomstolen

[62] Mål nr 21353/93, 80 DR 101 (1995) s. 105. Kommissionen tillade också att innehållet i de avlyssnade samtalen inte hade avslöjats. Den sista punkten kan vara missledande, med tanke på domstolens ståndpunkt i Malonemålet, att en stat gör sig skyldig till överträdelse av artikel 8 bara genom att tillåta polisen tillgång till uppgift om elektronisk kommunikation i avsaknad av lagstadgat bemyndigande. Domstolen tillkännagav också ett domslut i ett annat mål beträffande olagliga mobiltelefoner, men i det fallet var problemet bara lagenligheten när det gäller genomsökandet av sökandens hem (Caminzind mot Schweiz, av den 19 december 1997).

[63] Det finns annan rättspraxis nämligen X. and Y. v Belgium, No. 8962/80, decision of 13 May 1982, var kommissionen lämnade det öppet om radiokommunikationer mellan två personer föll in under artikel 8.

[64] Man kan till och med föreställa sig ett upprättande av kommunikationssystem med en sådan mikrovågskomponent inbyggd för just detta syfte, även om detta förmodligen skulle vara tekniskt och ekonomiskt ogenomförbart.

betraktar inte heller, vilket framgår nedan, frågan huruvida det finns ”rimliga förväntningar” som avgörande för om en åtgärd utgör ett intrång i privatlivet eller inte.

Även om domslutet var det rätta vid den aktuella tidpunkten är BC-målet inte gällande i dag. I de två senaste målen rörande denna fråga, Liberty mot Förenade kungariket och Weber och Saravia mot Tyskland, gjorde domstolen ingen åtskillnad mellan å ena sidan upptagning av uppgift om elektronisk kommunikation eller innehåll i meddelanden som skickas via kabel och å andra sidan samma typ av upptagning av kommunikation via mikrovågor. I båda fallen hade upptagning ägt rum av både meddelanden via kabel och meddelanden via mikrovågor. Domstolen ansåg i båda fallen att upptagningen utgjorde ett intrång i rätten till skydd för korrespondens/privatliv. Det bör också noteras att domstolen i målet Weber och Saravia även ansåg att överföringen av uppgifter till andra myndigheter, och deras användning av dessa, utgjorde *separata* intrång i sökandenas rättigheter enligt artikel 8, liksom förstörelsen av uppgifterna och vägran att underrätta sökandena.[65]

5.3 Privatliv

5.3.1 Allmänt

Medan rätten till skydd för korrespondens och hem är relativt lättbegripliga är det svårt att definiera ”rätten till skydd för privatliv”. Domstolen anser i själva verket att det är en ”generell term som inte går att ge en fullständig definition”.[66] Man har hittills nöjt sig med att ange vad den omfattar, nämligen ”yrkes- eller affärsverksamhet”, ”rätten att inleda och utveckla relationer med andra, också i offentliga sammanhang”, ”en persons fysiska och psykiska integritet”, ”rätten till […] personlig utveckling och till att fastställa detaljer för sin identitet som individ”.[67] Ett brett synsätt i fråga om begreppet privatliv är inte nödvändigtvis problematiskt för offentliga myndigheter, vilket kommer att framgå nedan, eftersom domstolen kan balansera detta med en flexibel strategi när det gäller

[65] Anfört arbete, punkt 79. I målet Liberty m.fl. nöjde sig domstolen med att förklara att den anser att förekomsten av dessa befogenheter, i synnerhet befogenheter som tillåter granskning, användning och lagring av upptagen kommunikation, utgör ett intrång i de rättigheter som sökandena har enligt artikel 8, eftersom de är personer som dessa befogenheter kan tillämpas på (punkt 57).
[66] Peck mot Förenade kungariket, mål nr 44647/98, dom av den 28 januari 2003, punkt 57.
[67] Moreham, 2008, s. 45 och hänvisningar där.

kraven ”stöd av lag” och ”nödvändighet i ett demokratiskt samhälle”. I spaningssammanhang innebär ett brett synsätt i fråga om privatliv absolut inte att spaning inte får förekomma. Domstolen klargjorde så tidigt som i målet Lüdi mot Schweiz att en misstänkt brottsling inte kan hävda att hans eller hennes samtal ska vara fullständigt skyddade mot inspelning.[68]

Den bakomliggande orsaken till att privatlivet skyddas i konventionen är att detta krävs för att en individs personlighet ska kunna utvecklas och bibehållas.[69] Men samhällets välbefinnande står också på spel. Vilken sorts samhälle främjar man till exempel om man förväntar sig att människor ska ”vara försiktiga med vad de säger” varje gång de svarar i mobiltelefonen?

Ett annat argument är knutet till graden av intrång. Medan hemlig elektronisk övervakning i en mening är mindre direkt och förödmjukande än ett sådant mer traditionellt intrång i privatlivet som en öppen, omstörtande husrannsakan, är den ett större intrång än en husrannsakan i den meningen att den oftast pågår längre, är mer urskillningslös, förutsättningslös och påverkar fler personer.[70] När resultatet av den hemliga elektroniska övervakningen *används*, t.ex. vid säkerhetskontroller eller för att rättfärdiga synliga och mer ingripande åtgärder (t.ex. gripande eller husrannsakan) kommer det naturligtvis att påverka den person som övervakats. Resultatet kan ge antingen en korrekt bild av situationen – att den övervakade personen är delaktig i kriminell verksamhet – eller en felaktig bild. Under alla förhållanden finns potential att i mycket hög grad påverka en människas liv, vilket innebär att det måste vara föremål för kontroll.

Medan vissa saker framgår tydligt av domstolens rättspraxis är det fyra frågor som kräver en mer detaljerad behandling. De första tre rör *när* och *under vilka förutsättningar* som övervakning av en person på offentlig plats, eller på en privat plats som inte utgör en del av ”hemmet”, genom avlyssning, visuell observation eller lokaliseringsinformation omfattas av privatliv. Den fjärde frågan rör huruvida tillgång till personuppgifter om en person som lagras på en dator som inte tillhör densamme innebär ett intrång i denna per-

[68] Lüdi mot Schweiz, anfört arbete.
[69] Som det uttrycks i *de Hert*: ”Den grundläggande rätten att få vara människa skulle rubbas och hotas om alla våra åtgärder skulle granskas, av det enkla faktum att vi agerar annorlunda när vi iakttas”, *de Hert*, 1997, s. 560, fotnoter utelämnade. EU-domstolens rättspraxis på detta område inleddes med det berömda målet ”Icelandic Dogs”, X mot Island, nr 6825/74, 5 DR 86 (1976).
[70] Lustgarten och Leigh 1994, s. 51.

sons privatliv. I de följande avsnitten diskuteras dessa frågor. Jag anser, vilket framgår av förklaringen nedan, att det går att göra åtskillnad mellan fotografering/hemlig visuell övervakning å ena sidan och dold ljudupptagning å den andra. Jag inleder därför med visuell övervakning, vilket också är det ämne som kräver den mest detaljerade genomgången.

5.3.2 Privatliv i icke-privata zoner: bildupptagning

Domstolen har i ett flertal fall ansett att visuell övervakning på offentliga plaster – genom fotografering eller videoinspelning – kan utgöra intrång i rätten till skydd för privatliv. Domstolen har framhållit att det, också i ett offentligt sammanhang, finns ”en zon för interaktion mellan en person och dennes omgivning som kan falla inom ramen för ’privatliv’”.[71] Det initiala sättet att gå till väga från konventionsorganens sida när det gäller frågan om bildupptagningar på offentliga platser framgår av målet Friedl mot Österrike.[72] Detta mål rörde polisövervakning av demonstranter. Kommissionen ansåg att det inte var ett intrång i privatlivet att bara *fotografera* en person på offentlig plats.[73] Kommissionen framhöll att tre faktorer var relevanta för frågan om huruvida det gjorts intrång i privatlivet: för det första ”om fotograferingen innebar ett inkräktande på individens privatliv, om den var knuten till privata angelägenheter eller offentliga händelser och om fotografierna varit tänkta att användas för ett begränsat syfte eller sannolikt skulle ha gjorts tillgängliga för allmänheten”.[74] Den första faktorn är knappast till någon hjälp, men kan antagligen knytas till tanken om ”en legitim förväntan av skydd för privatlivet”. Om man träffas på en offentlig plats kan man försöka dölja att man träffas genom att välja en avlägsen, lugn, mörk eller övergiven plats. Men det finns nästan undantagslöst en risk för att någon kan få syn på en. Förekomsten av

[71] Perry mot Förenade kungariket, mål nr 63737/00, dom av den 17 juli 2003, punkt 37.
[72] Friedl mot Österrike, mål nr 15225/89. Rapporten antagen den 19 maj 1994. Målet avgjordes efter förlikning. Regeringen betalade skadestånd till sökanden och gick med på att förstöra de fotografier som tagits.
[73] Man kan hävda att den yttrandefrihet och mötesfrihet som fastställs i artiklarna 10–11 borde utgöra en del av tolkningssammanhanget här. Yttrande- förenings- och demonstrationsfriheterna är av särskilt betydelse för det öppna samhället (jfr RF 1:1 st. 2). Fotografering av polisen kan onekligen *påverka* en persons benägenhet att delta i protester, även om denna åtgärd kanske inte går så långt som att *inskränka* yttrandefriheten. Detta i sig stärker argumenten att polisens möjligheter att fotografera eller filma demonstranter bör lagregleras. Vidare diskussion av denna fråga faller utanför ramen för denna rapport.
[74] Ibidem, punkt 48.

teleobjektiv innebär att till och med avlägsna mötesplatser kan observeras. Man kan hävda att det mycket sällan föreligger en ”rätt till legitimt skydd” mot att bli sedd. Men rätten till ett ”legitimt skydd” för privatliv är naturligtvis varierande till sin natur. Den ständiga utvecklingen av spaningsteknologin skulle innebära att en person snart, objektivt sett, inte längre kan ha en legitim förväntning av något skydd för privatlivet. Det bör enligt min uppfattning följaktligen inte fästas alltför stor vikt vid denna faktor. Och det anser inte domstolen heller nuförtiden, vilket framgår nedan.

Det framgick hursomhelst i målet Friedl mot Österrike att fotografierna hade tagits öppet, inte i hemlighet, och att aktiviteten – demonstrationen – var *avsedd* att synas. Dessutom användes inte de fotografier som tagits till att identifiera enskilda individer. Därför ansåg kommissionen att det inte hade förelegat något intrång i privatlivet. Liknande fall har emellertid lett till skärpta krav på det allmänna, vilket redovisas nedan.

I målet Murray mot Förenade kungariket greps sökanden i sitt hem av soldater, som misstänkte henne för delaktighet i terrorism.[75] Senare fotograferades hon i häktet, utan att hon visste om det eller hade gett sitt medgivande. Domstolen framhöll att denna fotografering var ett intrång i sökandens privatliv. Det faktum att sökanden hade förts från sitt hem hade förmodligen betydelse för detta utslag, men det hade också det faktum att fotograferingen hade skett utan hennes vetskap. En annan betydelsefull faktor var emellertid att fotografiet användes för att upprätta en personakt. Sökanden i målet Tsavachidis mot Grekland hade ”skuggats” och observerats systematiskt av statstjänstemän, och man hade samlat in utförlig information om hans aktiviteter. Kommissionen ansåg att detta var ett intrång i hans privatliv.[76]

I målet P.G. och J.H. mot Förenade kungariket bekräftade domstolen ståndpunkten i Tsavachidismålet och fastslog följande. ”Vid beslut om huruvida en persons privatliv berörts vid åtgärder som vidtagits utanför en persons hem eller privata fastighet måste många olika faktorer beaktas. Eftersom det finns tillfällen då människor medvetet eller frivilligt deltar i aktiviteter som spelas in eller kan spelas in eller rapporteras offentligt så kan en persons rimliga förväntning om skydd av privatlivet vara en betydelsefull, om än inte

[75] Dom av den 28 oktober 1994, A/300 A.
[76] Mål nr 28802/95, dom av den 28 oktober 1997. Detta mål har naturligtvis implikationer för alla typer av systematisk och hemlig insamling från statens sida av allmänt tillgänglig information om privatpersoner. Se nedan.

nödvändigtvis avgörande, faktor. En person som promenerar på gatan är naturligtvis synlig för alla andra som är i närheten. Det är ingen större skillnad att med tekniska medel övervaka samma offentliga plats (t.ex. genom en säkerhetsvakt som bevakar platsen med tv-övervakning). Om systematiska eller permanenta inspelningar av sådant material från offentlig plats framställs kan dock frågeställningar som avser rätten till skydd för privatlivet uppstå."[77]

I målet Allan mot Förenade kungariket[78] filmades och spelades in en person, som var misstänkt för ett brott och som hade vägrat att svara på frågor, i hemlighet i sin cell och på fängelsets besöksområde. Detta betraktades som ett intrång i hans privatliv.[79]

I andra mål har domstolen fäst vikt vid *oväntad* eller *orimlig* användning av filmande som gjorts och fotografier som tagits av aktiviteter som förekommit offentligt. Målet Perry mot Förenade kungariket rörde en person som hade filmats med övervakningskameror i häktet, för att man ville skaffa fram bilder att använda vid en konfrontation. Den övervakade kände till, eller kan åtminstone förväntas ha känt till, övervakningskamerorna, men domstolen ansåg att det inte fanns någonting som "tydde på att sökanden väntade sig att bli filmad på polisstationen för att filmen sedan skulle användas vid en videokonfrontation och, potentiellt, som bevismaterial till dennes nackdel vid en rättegång"[80]. Det var följaktligen ett intrång i privatlivet. Polisens användning av film vid konfrontation reglerades inte genom lagstiftning utan genom riktlinjer. Den nationella domstolen (vid Pecks rättegång) ansåg emellertid att polisen inte hade efterlevt dessa riktlinjer. Europadomstolen fastställde därför att åtgärden inte skedde "med stöd av lag".

---

[77] Punkt 57.

[78] Mål nr 48539/99, dom av den 5 november 2002.

[79] Se också van der Graaf mot Nederländerna, mål nr 8704/03, domslut av den 1 juni 2004. Permanent kameraövervakning av internerad under en tidsperiod på två veckor utgjorde ett intrång i privatlivet, men försvarades i sammanhanget som berättigat med stöd av lag och nödvändigt i ett demokratiskt samhälle: otillåtet.

[80] Punkt 41 i anförda arbete. Domstolen tillade: "En traditionell användning av övervakningskameror väcker i sig självt inga frågor inom ramen för artikel 8.1, när de används i legitimt och uppenbart syfte på offentliga gator eller i utrymmen som köpcentrum eller polisstationer […] I detta fall ställde polisen dock in övervakningskameran så att den skulle ta närbilder av sökanden i häktet och lade sedan in dem i ett filmmontage med andra personer för att visa för vittnen i syfte att se om de skulle identifiera sökanden som gärningsman i de rån som utreddes. Videon visades också i en offentlig rättssal under rättegången mot sökanden […] Detta trick från polisens sida gick bortom traditionell och förväntad användning av denna typ av kamera, vilket framgår tydligt av att polisen var tvungen att inhämta tillstånd och att en tekniker måste justera kameran. Den varaktiga bildupptagningen och det faktum att bilderna användes i ett montage för vidare bruk kan därför betraktas som behandling eller insamling av personuppgifter om sökanden."

Målet Peck mot Förenade kungariket rörde en person som hade filmats med övervakningskameror på en gata och vars beteende antydde att han skulle begå självmord. Tack vare bilderna kunde de som skötte kamerorna kontakta polisen i tid, som sedan räddade hans liv. Bilderna distribuerades senare till pressen av den lokala myndighet där bildupptagningen gjorts, som en del av en kampanj som utformats för att visa på fördelarna med övervakningskameror, något som verkligen upprörde sökanden. Domstolen fastslog följande: ”Övervakning av en privatpersons agerande på offentlig plats med hjälp av inspelningsutrustning som inte lagrar visuell data är inte i sig självt ett intrång i en persons privatliv.”[81] Domstolen tillade dock: ”Å andra sidan kan inspelningen av uppgifterna och inspelningens systematiska eller permanenta natur leda till slutsatsen att intrång föreligger.”[82] Man ansåg vidare att arkiveringen av uppgifterna innebar intrång i den personliga integriteten. Den lokala myndigheten hade en tydlig rättslig befogenhet att använda övervakningskameror. Men domstolen ansåg att man kränkt artikel 13 (om effektivt rättsmedel) eftersom sökanden inte på ett effektivt sätt kunde bestrida lagringen och spridningen av de bilder som upptagits.

Ett annat mål där man ansåg att en överträdelse förelegat var Sciacca mot Italien.[83] Det berodde på att polisen inte hade haft någon rättslig grund för att överlämna ett fotografi på en person som satt i husarrest till pressen.

Här kan också nämnas målet von Hannover mot Tyskland[84]. Det rörde en positiv skyldighet för staten att förhindra publicering av fotografier som tagits av paparazzifotografer och kan som sådana inte direkt jämställas med öppen eller dold fotografering från polisens sida. Detta mål ger dock ytterligare stöd för uppfattningen att man uppenbarligen kan ha rätt till skydd för privatlivet i offentliga sammanhang. Domstolen hänvisade till fotografering av sökanden medan hon ägnade sig åt aktiviteter av ”rent privat natur”. Den tyska författningsdomstolen hade konstaterat att sökanden, om hon objektivt sett hade uppsökt en avskild plats, hade rätt till skydd för sitt privatliv, och följaktligen att det var tillåtet att publicera fotografier av henne på en sådan plats. Andra fotografier fick emellertid publiceras. Europadomstolen framhöll dock att allmänheten inte ”har ett

[81] Punkt 59. Domstolen hänvisade till Herbecq mot Belgien, mål nr 32200/96 och 32201/96, kommissionens beslut av den 14 januari 1998, DR 92 A, s. 92.
[82] Ibidem.
[83] Mål nr 50774/99, dom av den 11 januari 2005.
[84] Nr 59320/00, dom av den 24 juni 2004.

legitimt intresse att veta var sökanden befinner sig och hur hon beter sig generellt i sitt privatliv, inte heller när hon befinner sig på platser som inte alltid kan beskrivas som avskilda och trots att hon är välkänd hos allmänheten”[85].

Målet Reklos och Davourlis mot Grekland[86] rörde fotografering av en nyfödd baby utan att hans föräldrar gett ett förhandsgodkännande, och bevarande av negativen. Domstolen ansåg att detta var en överträdelse av artikel 8. Den framhöll (i punkt 40) att ”en bild av en person är något av det mest utmärkande som finns för dennes personlighet eftersom den visar personens unika särdrag och skiljer personen från dennes likar. Rätten till skydd för bilder av ens person är följaktligen en av de avgörande komponenterna för den personliga utvecklingen och förutsätter rätten att kontrollera användningen av sådana bilder. Medan rätten till kontroll av sådan användning i de flesta fall omfattar möjligheten för en enskild person att vägra publicering av en bild av henne eller honom, inbegriper den också den enskilda personens rätt att motsätta sig en annan persons upptagning, bevarande och återgivande av sådana bilder. Eftersom en bild av en person är ett av särdragen hos hans eller hennes personlighet kräver ett effektivt skydd i princip, och i en sådan situation som i det aktuella fallet, […] inhämta samtycke från den berörda personen när bilden tas och inte bara om eller när den publiceras. Annars skulle ett utmärkande personlighetsdrag vara i händerna på en tredje part, och den berörda personen skulle inte ha någon kontroll över hur bilden används.”[87]

Slutligen kan ett annat mål nämnas: Wood mot poliskommissarien i Metropolis.[88] Detta är inte ett fall från Europadomstolen. Däremot har den en viss relevans eftersom den brittiska appellationsdomstolen tillämpade artikel 8 i konventionen (som, liksom i Sverige, har införlivats i lagen). Ärendet rörde polisens fotograferande av en ledande aktivist vid en demonstration mot vapenhandel. Polisen hade oroat sig för att det skulle kunna uppstå våld under demon-

[85] Punkt 76. Se nu RF 2:6 st. 2 (lydelse efter 1 januari 2011). Se också Verliere mot Schweiz, dom av den 28 juni 2001.
[86] Mål nr 1234/05, dom av den 15 januari 2009.
[87] Där det råder motstridiga intressen, i synnerhet gällande yttrandefrihet, så måste de två intressena balanseras. Domstolen har vid upprepade tillfällen vederlagt beslut av österrikiska domstolar som syftat till att begränsa journalisters publicering av fotografier på politiker på grundval av att politikerna har immateriella rättigheter till bilder av sig själva. Se t.ex. News Verlags GmbH & CoKG mot Österrike, mål nr 31457/96, dom från 2000, Krone Verlags GmbH & Co KG mot Österrike, mål nr 34315/96, dom av den 26 februari 2002, Osterreichischer Rundfunk mot Österrike, mål nr 35841/02, dom av den 7 december 2006.
[88] [2009] EWCA Civ 414 (den 21 maj 2009),
http://www.bailii.org/ew/cases/EWCA/Civ/2009/414.html.

strationen, vilket dock inte skedde. Polisen motiverade fotograferingen med att den gjordes inom ramen för den sedvanerättsliga (dvs. inte lagstiftade) befogenheten att upprätthålla allmän ordning. Sökanden i ärendet var medveten om att han hade fotograferats och krävde att fotot skulle förstöras, men polisen vägrade. Appellationsdomstolen ansåg inte att själva fotograferingen var en överträdelse av artikel 8. Omständigheterna indikerade dock att det varken förelåg någon anledning att åtala sökanden för hans agerande vid tidpunkten eller för hans agerande under en påföljande demonstration kort därefter. Det framstod som om fotografiet bevarades i allmänt underrättelsesyfte, eftersom det visade sökanden och andra personer i hans bekantskapskrets. Appellationsdomstolen ansåg att fotografierna tillsammans med det faktum att de hade bevarats utan förklaring innebar ett intrång i sökandens privatliv.

Domstolen ansåg att den sedvanerättsliga befogenheten att upprätthålla allmän ordning var en tillräcklig grund för att ta fotografierna och att detta följaktligen skedde ”med stöd av lag”. Majoriteten i domstolen ansåg emellertid att det förelåg en proportionalitetsbrist beträffande lagringen av fotografierna. En domare, Dyson, ansåg att det måste krävas en mer övertygande motivering, om syftet med att bevara fotografierna är att skydda samhället från störning av den allmänna ordningen eller kriminalitet på låg nivå, än vad som skulle krävas för att bevara ett fotografi för att skydda samhället mot terrorism eller mycket allvarlig kriminalitet.[89]

Enligt min uppfattning kan dessa mål sammanfattas på följande sätt.[90] Med viss reservation för målet Reklos och Davourlis, som kan tolkas som ett upprättande av en ny standard för fotografering i sig själv, verkar det som att det, i fråga om både dold och öppen fotografering eller filmupptagning från polisens sida, inte är aktiviteten i sig utan bevarandet av resultatet, eller lagringen av det i en fil, eller spridningen av det till andra offentliga myndigheter eller privata organ, som utgör intrång i privatlivet. Hur fotografiet, filmen el. dyl. kom till är inte viktigt. Det spelar alltså ingen roll vem som faktiskt utför bildupptagningen (fotograferingen, filmupptagningen etc.).[91]

[89] Punkt 86.
[90] Jag kommer inte att gå in på frågan om att väga integritetsskydd mot den i svensk grundlag fastställda informationsfriheten och yttrandefriheten vad gäller bildupptagning av privatpersoner för privat syfte.
[91] I t.ex. Woods-målet togs fotografierna av en privatfotograf som anlitats av polisen. Att använda privata organ för att inhämta bild- eller ljudupptagningar kan leda till särskilda problem i fråga om rättslig kontroll, t.ex. om ett privat företag anlitas för att filma misstänkta brotts-

För att få filma eller fotografera öppet måste polisen följaktligen kunna rättfärdiga lagringen av fotografierna eller filmerna när och om berörda personer inkommer med klagomål om detta. Detta innebär att det måste upprättas lagstöd för lagring av visuella inspelningar som gjorts med tekniska medel tillsammans med kontrollmekanismer (som beaktas i nästa avsnitt). När det gäller filmupptagning eller fotografering som görs i hemlighet är den berörda personen, och eventuella andra personer som också hamnar i bildfånget, förmodligen omedvetna om detta. Även i sådana fall är det emellertid fråga om ett intrång i privatlivet om fotografierna lagras, även om ”offret” inte inkommer med klagomål. Eftersom människor inte kan klaga på dessa intrång måste det finnas någon alternativ form av tillsynsmekanism. Det måste också finnas någon form av rättsligt stöd för alla typer av spridning av upptagningar som gjorts med tekniska medel, både öppna och dolda.

Det finns inget som visar att domstolen anser att det råder en skillnad mellan digital lagring av uppgifter och lagring i form av tryckta bilder. En sådan skillnad skulle förmodligen uppmuntra till att kringgå bestämmelserna. Samtidigt har en digital lagring av bilder naturligtvis potential att i hög grad öka tillgången till bilderna, vilket innebär en större potential för obehörig tillgång och spridning, med medföljande risk för intrång i den personliga integriteten.

En fråga som ännu inte besvarats helt är om domstolen fastställer en tröskel för ”hantering” av uppgifterna på individuell nivå i fall av dold fotografering. Är det med andra ord först när fotografiet/filmen har införts i en akt som öppnats om en individ som intrång faktiskt sker i privatlivet? Problemet med en sådan sätt att se på saken är också att regeln går att kringgå, t.ex. genom att ”arbetsfiler”, ”ortsfiler” eller ”ämnesfiler” kan skapas utan att uttrycklig identifiering görs av enskilda individer.

Domstolen hänvisade till ”permanenta *eller* systematiska” upptagningar i Peckmålet (min kursivering). Digital film och fotografier är ”permanenta” i jämförelse med övervakningskameror, som inte spelar in något eller där inspelningarna automatiskt försvinner i och med att de spelas över efter några dagar. En sådan tolkning skulle innebära att alla digitala bilder som tagits öppet eller dolt, till och med av oidentifierade personer, och som överförs till

lingar. Sådana problem kan väcka frågor både vad gäller kvaliteten på lagen (precision etc.) och utarbetande av kontrollmekanismer.

en dator eller skrivits ut skulle kunna betraktas som ett intrång i dessa personers privatliv.

Detta framstår som orimligt i ett avseende. Det kommer att finnas många situationer där polisen har filmat eller fotograferat stora grupper av människor, t.ex. utpekade fotbollshuliganer eller demonstranter som begår våldsgärningar, där ingen identifiering är möjlig förrän i ett senare – eller mycket senare – skede. Polisen kan ha ett ganska bra grepp om vem en viss demonstrant är, utan att kunna identifiera honom eller henne slutgiltigt. Polisen kan ha goda skäl att lagra sådana upptagningar en viss tid, i väntan på en slutgiltig identifiering av den utpekade gärningsmannen.[92] Under sådana omständigheter kan det tyckas oskäligt att anse att det föreligger ett fortgående intrång i denna persons privatliv om bilderna inte är individualiserade. Å andra sidan kräver befintliga bestämmelser om dataskydd ändå att det ska göras en bedömning av nödvändigheten att lagra uppgifter om en person, innan en sådan lagring tillåts.

Vilken ståndpunkt man än intar i denna fråga ser man snabbt att intrång görs i en persons privat- och yrkesliv om denna bildupptagning av en hittills oidentifierad person sprids på något sätt – definitivt till pressen (se t.ex. Sciacca-målet ovan) men möjligen också till andra myndigheter (t.ex. socialarbetare, när det gäller ungdomar) och till och med privatpersoner som fotbollssupporterklubbar (t.ex. för att be om hjälp med att identifiera personen i fråga) eller till personer som organiserar demonstrationer (t.ex. för att uppmana dem att hålla uppsikt efter denna person, som kanske är ute efter att ställa till problem). Detta innebär inte att polisen inte kan ha goda skäl att sprida en bildupptagning eller att detta är ett brott mot konventionen. Dessa exempel klargör helt enkelt att till och med en bildupptagning av en oidentifierad person potentiellt kan innebära ett intrång i dennes privatliv.

Jag skulle säga att en sund strategi skulle vara att acceptera att polisen måste ges rätt att göra en bedömning av när en bildupptagning är tillräckligt ”individualiserad” för att den ska anses utgöra ett intrång i privatlivet. Men detta måste balanseras av någon form av extern tillsyn och kontroll av denna, av nödvändighet ganska vitt formulerade, bedömningsrätt.

Det praktiska resultatet av detta kan bli att trots att den faktiska bildupptagningen – att trycka på knappen – inte anses utgöra ett intrång i rätten till privatliv, det lik väl skulle kunna utgöra ett intrång

[92] När det handlar om långsiktiga sammansvärjningar, t.ex. organiserad brottslighet eller säkerhetsbrott, kan denna tidsperiod naturligtvis vara längre.

i privatlivet. Detta är fallet på grund av att polisen, så snart som knappen har tryckts ned, måste kunna hänvisa till lagstöd för lagring av upptagningen vid tillsyn av ett externt tillsynsorgan.

Jag bör påpeka att detta inte innebär att det nu finns en skillnad mellan ”gammaldags” polisarbete – att skugga personer och notera deras förehavanden och umgängeskretsar osv. – och samma sorts arbete utfört med tekniska hjälpmedel. Bland annat målen Tsavachidis, Amman och Rotaru visar att också det förstnämnda utgör ett intrång i privatlivet när det leder till en *systematisk inhämtning* av information om en enskild person.

5.3.3 Privatliv i icke-privata zoner: ljudupptagningar

I en rad länder fastställs rätt till skydd för hemmet, men inte till skydd för ”privatlivet” som sådant i grundlagen. Detta faktum har utnyttjats till försvar för att inte reglera inspelning med hjälp av tekniska medel av samtal *utanför hemmet*, eller åtminstone till att göra det till föremål för en lägre grad av reglering. Efter Bykovmålet framgår det dock ganska tydligt att domstolen betraktar detta som ett intrång i privatlivet. Även om Bykovmålet rörde ljudupptagning utförd av en person som deltog i samtalet, synes det stå klart att *alla* tekniska hjälpmedel för att ta upp samtal, t.ex. riktade mikrofoner, eller att manuellt eller genom fjärråtkomst ställa om en mobiltelefon till en inspelningsutrustning och sätta på den, innebär ett sådant intrång, oavsett var objektet befinner sig. I Koppmålet fastslog domstolen, vilket redan nämnts, att intrånget i detta sammanhang utgjordes av själva inspelningen, oavsett om den sedan användes till något eller inte (information eller bevisföring). Denna hårdare inställning kan förmodligen rättfärdigas av den större förväntan på privatliv som två personer (A och B) kan ha om de viskar till varandra på en offentlig plats, på avstånd från andra människor. Samtidigt vill jag återigen påpeka att detta kriterium är väldigt osäkert. Om alla har en mobiltelefon som med ett klick kan ställas om till en utrustning för ljudupptagning påverkar detta förmodligen också A och B:s ”legitima förväntningar” om deras skydd för privatlivet. Man kan hur som helst notera att domstolen utan tvekan betraktar dold ljudupptagning av en person utanför hemmet som ett intrång i den personens ”privatliv”, oavsett om personen kan sägas ha en ”rimlig förväntan på skydd för privatliv” eller inte.

5.3.4 Lokaliseringsinformation

Jag ska nu diskutera lokaliseringsinformation. Denna fråga kan behandlas mycket kortfattat. Sådan information finns i olika former, vilket jag noterade i avsnitt 2. Mobiltelefoner tillhandahåller alltid – även i standby-läge – lokaliseringsinformation till basstationen, vilket möjliggör en allmän kartläggning av en persons förehavanden. Mobiltelefoner kan också aktiveras på distans, vilket till och med gör det möjligt att spåra den när ägaren tror att den är avstängd. Nyckelkort anger var och när en person har beträtt ett visst område eller en viss zon. Genom bankkort får man reda på var och när en person har gjort en överföring. Utvecklingen av RFID-teknik (radiofrekvensidentifiering), där man för elektronisk övervakning kan placera identifieringstaggar på accessoarer och kläder, innebär att en person som bär något med en sådan tagg kan lokaliseras. Olika typer av sensorer kan placeras ut för att registrera att en person beträder, eller vistas på, ett visst område.

Man kan hävda att vissa typer av lokaliseringsinformation, framför allt tillgång till uppgifter om all mobiltrafik som registrerats på en basstation för mobiltelefoni under en särskild tidsperiod (basstationstömning), inte utgör ett intrång i en *enskild persons* privatliv. Det står dock klart att syftet med och följderna av åtgärden är att identifiera exakt vilka personer som *skulle kunna* ha befunnit sig inom ett visst område vid en viss tidpunkt.

Man kan likväl inta ståndpunkten att information om var en person har befunnit sig, eller till och med var personen befinner sig just nu, i realtid, vanligtvis inte bör betraktas som känslig. Om jag accepterar att min mobiloperatör kan spåra mig, eller att min bank genast vet var jag är om jag gör en elektronisk överföring, varför är det då ett intrång i mitt privatliv om polisen också har tillgång till denna information?

Detta argument handlar mer om intrångets *omfattning* än om det överhuvudtaget utgör ett intrång. Det relaterar därför till vilken form och grad av reglering som krävs, se nedan. I detta sammanhang kan dock två saker framhållas. För det första har jag *valt* att låta min mobiloperatör eller bank ha tillgång till denna lokaliseringsinformation *för sina syften* (syften som också tjänar mina egna – underlättande av kommunikation och säkerhet vid banköverföringar).[93] I detta sammanhang kan en modell med ”koncentriska

[93] Jfr domstolens yttrande i målet PG och JH i punkt 42 i anförda arbete: ”mätning som inte utgör en överträdelse av artikel 8 i sig själv om den, exempelvis, görs av telefonbolaget i

cirklar" användas.[94] Det ligger i den enskilda individens intresse att bestämma, eller åtminstone kunna påverka, vem som har tillgång till sådan information, och i vilket syfte. Jag har inte valt att låta polisen – eller skattemyndigheterna eller mitt barns skola eller min arbetsförmedlare – alltid veta var jag befinner mig. Lagstiftaren kanske beslutar att samhällsintresset av att, i ett enskilt fall, låta polisen kunna ta reda på var en person befinner sig eller har befunnit sig uppväger den berörda personens intresse av att inte låta polisen veta var han eller hon befinner sig/har befunnit sig. Men det är inte detsamma som att säga att personen inte har något intresse att hålla sin vistelseort hemlig för polisen eller andra myndigheter.

För det andra gör en *systematisk* inhämtning av sådan information det möjligt för staten att skapa en större bild av en persons privatliv än vad som är möjligt för en privatperson.

Min slutsats är att om information om vilka telefonnummer rings och om längden på ett telefonsamtal utgör intrång i privatlivet borde det även innebära ett intrång i privatlivet att inhämta "lokaliseringsinformation" om en person – manuellt eller med fjärråtkomst – genom att följa mobiler, läsa av nyckelkort osv.

Domstolen ställdes nyligen i Uzun-målet inför frågan om huruvida det är ett intrång i en persons privatliv att placera lokaliseringsutrustning i en bil. Lokaliseringsutrustning kan ge information som motsvarar spårning av en persons mobiltelefon, om utrustningen t.ex. placeras i en personens privata bil. I Uzun-målet placerades GPS-utrustning i en bil tillhörande sökandens medbrottsling, vilket gjorde att polisen kunde följa de två misstänkta och skapa sig en bild av deras förehavanden under en tremånadersperiod. Det underlättade också den visuella övervakningen (skuggningen) av dem, vilket i sin tur gjorde att det gick att samla in ytterligare bevis. Domstolen fastslog att "övervakning med hjälp av GPS skiljer sig genom sin natur från andra metoder för visuell och akustisk övervakning som, i regel, lättare utgör intrång i en persons rätt till respekt för privatlivet, eftersom de ger mer information om en persons beteende, åsikter och känslor"[95]. Man kom likväl till slutsatsen att detta utgjorde ett intrång i privatlivet.

Man kan hävda att domslutet i Uzun-målet inte med nödvändighet innebär att *all* användning av GPS- och liknande utrustning

---

faktureringssyfte ska till sin själva natur särskiljas från sådan avlyssning av samtal som skulle kunna vara oönskad och olaglig i ett demokratiskt samhälle om den är omotiverad".

[94] Se t.ex. Nagel, 1998.

[95] Punkt 52.

utgör ett intrång i privatlivet. När det gäller Uzun-målet identifierades den övervakade personen och syftet var att övervaka denna person. Andra situationer kan dock identifieras när intrånget i privatlivet inte är lika uppenbart. Exempelvis kan GPS-utrustning eller annan sändare kopplas till ett larm eller till ett objekt som är dolt någonstans, t.ex. en hemlig vapendepå, stöldgods eller en väska som innehåller en lösensumma i ett kidnappningsfall. Samtidigt skulle situationen kunna vara annorlunda om sändaren är kopplad till en mer avancerad utrustning som kan medföra identifiering, t.ex. om man skulle kunna ta bilder med utrustningen med hjälp av fjärrutlösning.

Situationen i Uzun-målet skiljer sig också från ett tänkbart fall där polis eller tulltjänstemän placerar liknande utrustning i t.ex. en container för att spåra stöldgods, smuggelgods eller förfalskade varor. I detta fall skulle syftet normalt vara att spåra det aktuella godset.

En tredje situation som jag skulle vilja påstå skiljer sig från Uzun-målet är om polisen bistår en fordonsägare genom att se till att denne får tillbaka sitt stulna fordon (eller vice versa). Många dyra bilar och lastbilar är utrustade med GPS, som kan användas som en stöldskyddsanordning med vilken ägare eller polis kan spåra ett stulet fordon.

Men även om man kan hävda att användning av GPS-utrustning i sådana eller liknande situationer inte nödvändigtvis utgör ett intrång i privatlivet, så underlättar den naturligtvis visuell övervakning.[96] Och i sådana fall där lagring sker av permanent eller systematisk information som avser visuell övervakning, föreligger det ett intrång. Dessutom måste man ta hänsyn till risken för missbruk. Om polisen fritt kan bestämma över användningen av GPS-utrustning i en typ av situation, finns det naturligtvis en risk för att tillämpningsområdet för denna typ av användning utvidgas i praktiken. Det förnuftiga verkar i detta fall vara att reglera all polisiär användning av GPS-utrustning på ett liknande sätt som för inhämtning av uppgift om elektronisk kommunikation.

[96] Jämför argumenten i avsnitt 5.2.2 ovan om delaktighet vid avlyssning.

5.3.5 Digitala privata utrymmen

Den sista frågan i detta avsnitt handlar om huruvida det är ett intrång i en persons privatliv att skaffa sig tillgång till hans eller hennes ”privata utrymme” på en server. Det framgår av Copeland och andra mål att övervakning av en persons *Internetåtkomst* utgör ett intrång i dennes privatliv. Jag anser att detta måste utvidgas till polisens tillgång till filer som fysiskt ligger på en server som ägs av en annan person, eller ett annat företag, som skulle kunna välja att låta polisen få tillgång till filerna. ”Datormoln” är något som blir allt vanligare. Redan idag finns det många människor i Sverige som inte lagrar privata filer, fotografier, filmer osv. på en dator som är fysiskt placerad i hemmet, utan lagrar dem på en server. Detta är på ett sätt säkrare, eftersom en utomstående person åtminstone inte kan få tillgång till uppgifterna genom att stjäla den dator de lagrats på, och de är inte heller lika utsatta för brand och andra olyckor. Det är också mer praktiskt, eftersom stora mängder uppgifter kan lagras på en server och en person kan få tillgång till och arbeta med uppgifterna var han eller hon än befinner sig, t.ex. på ett Internetcafé.

Man kan hävda att en person som på något sätt har lagrat personligt material på en server inte *bör* ha legitima förväntningar på att denna del av hans/hennes privatliv är skyddade. Så är utan tvekan fallet när en person väljer att lägga upp information – film, bilder, text osv. – på en offentlig anslagstavla eller webbplats, som YouTube. I detta sammanhang har informationen medvetet gjorts tillgänglig för alla som har tillgång till Internet, och polisen behöver ingen särskild befogenhet för att kopiera den (lika lite som en sådan befogenhet krävs för att fotokopiera en tidning).

Jag har inte gjort någon empirisk undersökning av personers subjektiva uppfattning om privat integritet vid lagring av uppgifter på *privata* utrymmen på Internet. Men jag misstänker att de flesta tror att den information de lagrar på servern är konfidentiell. Om en person följer avtalet med det företag som äger servern (t.ex. att inte lagra pornografiskt material osv.) så har denne säkerligen legitima förväntningar på att denna del av hans/hennes privatliv ska vara skyddade. Beviset på detta är att deras reaktion sannolikt skulle vara mycket negativ om det företag som kontrollerar servern skulle göra informationen tillgänglig för personer utöver dem som den berörda personen har beviljat tillgång till informationen (t.ex. till personer som han eller hon inte har som ”vän” på Facebook). Personlig information som lagras på servrar kan mycket väl vara lika känslig

som andra uppgifter, som man lagrar på sin egen dator. Ytterligare ett argument för detta är slutligen att obehörig tillgång till information som tillhör en annan person, *var den än lagrats*, är en brottsligt enligt svensk lag.[97] Det synes inte råda någon tvekan om att det också utgör ett intrång i en persons privatliv att skaffa tillgång till sådan information.

6 Krav på lagstiftningen enligt Europadomstolens doktrin om ”stöd av lag”

6.1 Allmänt

Kravet inom ramen för artikel 8.2 att ett intrång måste ha ”stöd av lag” är inte rent formellt, vilket redan har nämnts. Det har samband med kvaliteten på lagen. I Klass mot Förbundsrepubliken Tyskland uppstod ingen stor diskussion om denna fråga, eftersom den aktuella tyska lagen, ”G10”[98], på ett relativt detaljerat sätt klargör när och hur strategisk övervakning får ske.[99] I Klass mot Förbundsrepubliken Tyskland, samt i en rad tidigare beslut av kommissionen, betraktades frågor i samband med kvaliteten på lagen som en del av frågan om huruvida åtgärderna ” varit nödvändiga i ett demokratiskt samhälle”. I de flesta senare mål vid domstolen har sådana frågor emellertid behandlats under rubriken ”med stöd av lag”.

Det första teleavlyssningsmålet där man fastslog att en överträdelse hade skett av kravet på ”med stöd av lag” var Malone mot Förenade kungariket. Att en minister i regeringen kunde godkänna teleavlyssning var omnämnt i den dåvarande brittiska lagstiftningen, men lagstiftningen innehöll ingen egentlig sådan befogenhet. Det fanns administrativa riktlinjer som reglerade hur Ministern skulle gå till väga. Vissa av dessa riktlinjer var detaljerade och vissa vaga.[100] Domstolen godtog den brittiska statens åsikt att kraven på förutsebarhet måste vara lägre när det gäller hemlig övervakning. Det kan uppenbarligen inte krävas att en individ ska veta precis när han eller hon blir föremål för övervakning och på så sätt kunna anpassa sitt

[97] Brottsbalken, 4 kap., § 9 a.
[98] Lag om begränsning av brev-, post- och telefonhemligheten (lag till artikel 10 i den tyska grundlagen), nedan kallad ”G10”, av den 13 augusti 1968, Tysklands officiella tidning nr 1 s. 949. Varje delstat har sin egen G10-lag (lag om genomförande av G10-lagen). Den beskrivning av det federala kontrollsystemet som görs nedan gäller i tillämpliga delar för delstaterna.
[99] Punkt 63 i Klass-rapporten, punkterna 43 och 45 i Klass-domslutet.
[100] Se Cameron, 1986, sidorna 126 och 129.

beteende därefter. Domstolen fastslog ändå att ”lagen måste vara tillräckligt tydlig i fråga om att ge medborgarna en tillräcklig antydan om under vilka omständigheter och på vilka villkor som offentliga myndigheter har rätt att tillgripa ett sådant hemligt och potentiellt farligt intrång i rätten till respekt för privatliv och korrespondens”.[101] Domstolen tillade följande. ”Eftersom det praktiska genomförandet av åtgärder för hemlig teleavlyssning inte kan granskas av de berörda personerna vore det mot rättsstatsprincipen om den verkställande maktens lagenliga befogenhet i detta avseende tog sig utryck som en ohämmad makt”.[102] Domstolen ansåg vidare att den brittiska lagstiftningen om teleavlyssning stred mot detta krav, eftersom den inte ”klart och tydligt avgränsar omfattningen av dessa befogenheter och anger hur dessa ska utövas av de berörda myndigheterna”.[103] Malone-målet ledde till att Förenade kungariket antog 1985 års lag om avlyssning av kommunikation.[104]

I det brittiska system som det var fråga om i Malone-målet var det en minister som sanktionerade teleavlyssning utan att involvera åklagare eller domare. Men även system där rättsväsendet har godkänt teleavlyssning har vid flera tillfällen konstaterats innebära överträdelser av konventionen. Det första av dessa mål var Kruslin mot Frankrike[105] och Huvig mot Frankrike[106]. Stödet i fransk lag för att bevilja hemlig teleavlyssning (som baserades på artikel 100 i straffprocesslagen) blev föremål för viss debatt, men domstolen var beredd att acceptera att det fanns tillräcklig grund för detta i fransk lag och att denna praxis var tillräckligt. Men förundersökningsdomares rätt att bevilja hemliga teleavlyssningar var inte föremål för några begränsningar. Domstolen ansåg att detta var en överträdelse av kravet på förutsebarhet och att detta tillvägagångssätt därför inte tillämpades ”med stöd av lag”. Ett annat exempel är målet Valenzuela Contreras mot Spanien, som rörde teleavlyssning av sökanden vid en tidpunkt då den enda tydliga grunden för detta var konstitutionen. Det fanns inte någon genomförandelagstiftning. Även om

[101] Malone mot Förenade kungariket, punkt 67.
[102] Ibidem, punkt 68.
[103] Ibidem, punkt 79.
[104] Denna lag var ett exempel på att vidta absolut minsta möjliga åtgärder för att efterleva ett domslut som avkunnats av domstolen. När Förenade kungariket införlivade EKMR i den nationella lagstiftningen, vilket innebar att kompatibiliteten när det gäller lagen om avlyssning av kommunikation med konventionen kunde bestridas inför brittiska domstolar, blev det angeläget att ersätta den så snart som möjligt. Detta skedde 2000, med *Regulation of Investigative Powers Act* [lagen om undersökningsbefogenheter] (RIPA).
[105] Dom av den 24 april 1990, A/176 A.
[106] Dom av den 24 april 1990, A/176 B.

den domare som beviljade avlyssning i själva verket hade försökt minimera det intrång detta skulle utgöra i sökandens privatliv, innebar avsaknaden av tydliga bestämmelser med krav motsvarande dem som fastställts i målet Huvig och Kruslin mot Frankrike att den spanska åtgärden inte hade skett ”med stöd av lag”.

6.2 Förutsebarhet

Europadomstolens krav på rättslig ”förutsebarhet” inom detta område har sammanfattats på ett användbart sätt i målet Weber och Saravia, beslutet om upptagande till sakprövning, punkterna 93–95.[107]

”93. … förutsebarhet i samband med dolda spaningsåtgärder, som kommunikationsavlyssning, ska inte innebära att en person bör kunna veta på förhand när myndigheterna sannolikt avlyssnar dennes samtal, så att han eller hon kan anpassa sitt beteende därefter (se bland annat Leander mot Sverige, dom av den 26 augusti 1987, A/116 punkt 51). Risken för godtycklighet är emellertid uppenbar, i synnerhet när ett verkställande organ utövar sina befogenheter i det dolda (se bland annat Malone, punkt 67, Huvig, punkt 29 och Rotaru mot Rumänien, mål nr 28341/95, punkt 55, EKMR 2000 V). Det är därför mycket viktigt att ha tydliga, detaljerade regler för teleavlyssning, i synnerhet eftersom den teknik som används för detta ständigt blir alltmer avancerad (se Kopp mot Schweiz, dom av den 25 mars 1998, rapporter 1998 II, s. 542–43, punkt 72 och Valenzuela Contreras mot Spanien, dom av den 30 juli 1998, rapporter 1998 V, punkt 46). Den nationella lagstiftningen måste vara tillräckligt tydlig i fråga om att ge medborgarna en tillräcklig antydan om under vilka omständigheter och på vilka villkor som offentliga myndigheter har rätt att tillgripa sådana åtgärder (se Malone, ibidem, Kopp, punkt 64, Huvig, punkt 29 och Valenzuela Contreras, ibidem).

94. Eftersom det praktiska genomförandet av åtgärder för hemlig avlyssning av kommunikationer inte kan granskas av de berörda personerna skulle det dessutom strida mot rättsstatsprincipen om den verkställande maktens lagenliga befogenhet i detta avseende tog sig utryck som en ohämmad makt. För att individen ska få tillräckligt skydd mot godtyckliga intrång (se t.ex. beläggen i Malone,

[107] Jag har redigerat utdraget. Liknande framställningar återfinns i *Association for European Integration and Human Rights* och Ekimzhiev, punkterna 75–77 och i målet Liberty mot Förenade kungariket, punkt 62. Se Liberty-målet, som diskuteras nedan, för krav på tillgänglighet.

punkt 68, Leander, punkt 51 och Huvig, punkt 29) måste därför räckvidden för alla sådana befogenheter som de behöriga myndigheterna har, och det sätt de ska vidtas på, anges tillräckligt tydligt i lagen.

95. Domstolen har, i sin rättspraxis om dolda spaningsåtgärder, utarbetat följande minimigarantier som bör fastställas i lagstiftning för att undvika maktmissbruk: angivande av arten av de brott som skulle kunna leda till en begäran om avlyssning, en definition av de personkategorier som skulle kunna riskera att få sin telefon avlyssnad, en begränsning av avlyssningens varaktighet, förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtats, vidtagande av försiktighetsåtgärder vid överföring av information till andra parter samt angivande av de omständigheter under vilka inspelningarna kan eller måste raderas eller banden måste förstöras (se bland annat Huvig, punkt 34, Amann, punkt 76, Valenzuela Contreras, punkt 46 och Prado Bugallo mot Spanien, mål nr 58496/00, punkt 30, dom av den 18 februari 2003).”

6.3 Kontrollmekanismer

Kontrollmekanismer är nödvändiga för att se till att de miniminormer för förutsebarhet som fastställs ovan efterlevs. I *Association for European Integration and Human Rights* och Ekimzhiev fastslog domstolen att ”nationell lagstiftning i samband med dolda spaningsåtgärder av offentliga myndigheter måste tillhandahålla visst skydd mot godtycklig överträdelse av rättigheterna i artikel 8 på grund av bristen på offentlig granskning och risken för maktmissbruk […]. Domstolen måste vara säker på att det finns tillräckliga och effektiva garantier mot missbruk. Denna bedömning är beroende av alla omständigheter i målet, t.ex. åtgärdernas karaktär, räckvidd och hur länge de varar, vilka motiv som krävs för att ge order om dem, vilka myndigheter som har befogenhet att godkänna, utföra och övervaka dem samt vilken typ av rättsmedel som föreskrivs i den nationella lagstiftningen.”[108]

Domstolen har i allt högre grad betonat att det finns två steg i övervakningsprocessen, som båda måste vara föremål för oberoende kontroller. Det första steget rör beslutsprocessen och det andra rör

[108] Punkt 77 i anförda arbete (hänvisning saknas). Den sista delen av citatet är en upprepning av vad domstolen fastslog i Klass mot Förbundsrepubliken Tyskland, punkt 50.

själva utförandet av övervakningen och uppföljningsprocessen när övervakningen slutförts.[109]

I målet Klass mot Förbundsrepubliken Tyskland förespråkade domstolen tydligt ett system för rättslig kontroll av bemyndigandeförfarandet, och konstaterade att ”rättsstatsprincipen medför bland annat att den verkställande maktens inskränkningar av den enskildes rättigheter skall bli föremål för en effektiv prövning som normalt sett skall göras av den dömande makten, åtminstone i sista instans, eftersom en domstolskontroll erbjuder de bästa garantierna för oberoende, opartiskhet och ett korrekt förfarande.”[110] Den fastslog dock vidare att G10-kommissionen var en tillräckligt oberoende kontrollmekanism i fråga om strategisk övervakning.

I målet Popescu mot Rumänien[111] ansåg domstolen att den rumänska myndighet som beslutade om övervakning (åklagaren) inte var fristående från den verkställande makten. Den konstaterade att det ansvariga organet måste vara oberoende *och* att det tillståndsgivande organets verksamhet borde undergå antingen kontroll av en domare eller någon annan slags oberoende kontroll.[112] Trots att det fanns ett parlamentariskt tillsynsorgan i Rumänien ansåg domstolen att tillsynen utövats i teorin, inte i praktiken, och att detta under alla omständigheter inte kunde betecknas som något rättsmedel, eftersom den övervakade inte i efterhand informerades om att övervakning hade skett.[113]

Domstolen har betonat betydelsen av *skriven lag* för reglering av stora delar av befogenheterna för hemlig övervakning. Enbart stöd av rättspraxis är inte tillräcklig reglering för detta område, inte ens där detaljerade normer fastslagits av högsta domstolen eller författningsdomstolen.[114] Samtidigt behöver den rättsliga ramen inte vara

[109] Se Iordachi, punkt 42, och *Association for European Integration and Human Rights* och Ekimdzhiev, punkt 84.
[110] Klass, punkt 55. Domstolen konstaterade vidare att ”det, på ett område där missbruk så lätt kan ske i enskilda fall och kan få så skadliga följder för det demokratiska samhället i sin helhet, i princip är önskvärt att anförtro övervakningskontroll till en domare” (punkt 56). Konventionssystemets natur medför att domstolen är begränsad till att antyda för stater som inte är parter i ett aktuellt mål att det vore klokt att ändra otillfredsställande lagar. I fråga om antydningar är denna en ganska tydlig sådan.
[111] Mål nr 71525/01, dom av den 26 april 2007.
[112] Ibidem, punkterna 70–73.
[113] Ibid. “le contrôle du pouvoir législatif semblait plutôt théorique et, en tout cas, dépourvu d'effet pratique pour l'individu, dans la mesure où une personne mise sur écoute n'était pas censée prendre connaissance de l'existence de telles mesures secrètes à son égard”
(at para. 77).
[114] Se Heglas mot Republiken Tjeckien, punkt 74 i anförda arbete. Domstolen hade tidigare godkänt konkreta bestämmelser som fastställts av författningsdomstolen i Valenzuela Contreras mot Spanien, punkt 34, men så är inte längre fallet.

helt och hållet lagstadgad. En grad av konkretisering av normer kan fastställas i administrativa förordningar eller bindande rättspraxis.[115] Detta ger en grad av flexibilitet, vilket krävs om lagstiftaren vill reglera området på ett ”teknikneutralt” sätt (som i sin tur motiveras av behovet att undvika ständiga lagändringar för att polisen ska kunna hålla jämna steg med ny teknik).[116]

Rättspraxis (t.ex. målen Klass och *Association for European Integration and Human Rights* och Ekimzhiev) medför att kraven på förutsebarhet skiljer sig från behovet av skyddsåtgärder och rättsmedel, även om dessa två uppsättningar av krav är knutna till varandra.

Domstolen har lagt större betoning på kontrollmekanismer, antagligen för att den inser att listan över faktorer som ska regleras i lagen inte i sig själv kommer att leda till att missbruk eller överanvändning undviks. Kravet att ange vid vilka brott som teleavlyssning är tillåten är exempelvis inte ett så starkt skydd som det kanske verkar vara.[117] Brottsbeskrivningar är en fråga för den nationella lagstiftaren. Inom de otydliga gränserna föreskrivna av artikel 7 kan ett brott definieras i relativt allmänna termer.[118] I den nationella lagstiftningen kan ett krav fastställas om minimistraff för ett brott för att teleavlyssning ska vara tillåten vid utredningen av brottet. Men detta är inte heller ett tillräckligt skydd om den nationella lagstiftaren anser att en stor andel av alla brott når upp till denna lägsta tröskel.[119] Likadant kan man konstatera att ett lagstadgat krav enligt vilket andra utredningsmetoder sannolikt inte skulle vara framgångsrika i praktiken kan tas på allvar av utredande och tillståndsgivande myndigheter, eller behandlas som en

[115] Domstolen gick så långt som att anse i Kopp mot Schweiz att rättspraxis, doktriner och administrativa förordningar kan avvika något från ordalydelsen i lagstiftningen utan att detta är en överträdelse av konventionen, så länge som dessa är tillräckligt välkända (dom av den 25 mars 1998, punkterna 59–60). Men med tanke på den större uppmärksamhet som domstolen har visat i senare mål när det gäller behovet av att minimera missbruk på detta område ställer jag mig tveksam till att den skulle inta samma ståndpunkt i dag.

[116] Jfr *Skyddet för den personliga integriteten*, *Bedömningar och förslag, SOU 2008:3, s. 203.* ”En reglering bör vidare vara så teknikneutral som möjligt och undvika att söka uttömmande ange vilka metoder som avses.”

[117] Det bör i detta sammanhang tilläggas att domstolen godkänner att teleavlyssning inte måste knytas till ett specifikt brott i sådana stater som har en separat civilsäkerhetsstjänst utan polisbefogenheter (vilket diskuteras mer ingående nedan).

[118] Se Cantoni mot Frankrike, avsnitt 4 i anförda arbete, om den fällande domen mot en chef för en livsmedelsbutik för illegal försäljning av läkemedelsprodukter, vad gäller den relativt vaga normen för ”lag” som domstolen tillämpar i samband med artikel 7.

[119] Något som skulle kunna bidra till detta är en trend att höja straffnivåerna, delvis till följd av önskemål om harmonisering på EU-nivå. Se framför allt rambeslutet om bekämpande av terrorism som, åtminstone i vissa EU-stater, lett till en betydande ökning av sådana brott för vilka särskilda utredningsmetoder kan begäras.

formalitet. Slutligen är tillgången till teleavlyssning i praktiken beroende av både hur lagstiftaren anpassar den grad av misstanke som krävs innan en sådan åtgärd kan beordras och hur de utredande myndigheterna och de tillståndsgivande organen tolkar detta krav. I Iordachi m.fl. mot Republiken Moldavien[120] identifierade domstolen alla dessa problem.[121] Domstolen uttryckte åsikten att teleavlyssning i Moldavien överanvändes i hög grad och betonade att ”teleavlyssning är ett mycket allvarligt intrång i en persons rättigheter och att enbart *mycket allvarliga skäl* som grundas på en *rimlig misstanke* om att personen är inblandad i *allvarlig brottslig verksamhet* skall ligga till grund för ett beviljande”.[122]

Det finns ett antal frågor som kräver en mer detaljerad genomgång. En av dessa är, vilket redan har angetts, att konkretisera de oberoende kontroller som krävs på uppföljningsstadiet, med andra ord ”respekt för förfarandet för undersökning, användning och lagring av de uppgifter som inhämtats, vidtagande av försiktighetsåtgärder vid överföring av information till andra parter och angivande av de omständigheter under vilka inspelningarna kan eller måste raderas eller banden måste förstöras”. Det framgår av rättspraxis, framför allt målen Kopp mot Schweiz och Lambert mot Frankrike, att den nationella lagstiftningen måste tillhandahålla tillfredsställande mekanismer för övervakning av vad som sker med ”överskottsinformation”. Detta ämne faller huvudsakligen utanför mitt aktuella uppdrag.[123]

Målet Kennedy mot Förenade kungariket[124] står i kontrast till de kritiska ståndpunkter som intagits i målen *Association for European Integration and Human Rights* och *Iordachi*. Det brittiska systemet innehåller relativt begränsade skydd, i synnerhet i fall som

[120] Mål nr 25198/02, dom av den 10 februari 2009.
[121] ”Det har klargjorts att en person som misstänks för ett allvarligt, mycket allvarligt eller ett synnerligt allvarligt brott under vissa omständigheter riskerar att denna åtgärd tillämpas på henne eller honom. […] Definitionen av arten av sådana brott som skulle kunna leda till ett beviljande av avlyssning är, enligt domstolen, emellertid inte tillräckligt tydlig i den ifrågasatta lagstiftningen. Domstolen konstaterar i synnerhet att mer än hälften av de brott som anges i brottsbalken faller inom ramen för den brottskategori som berättigar till avlyssning […] Den noterar att språket i artikel 156, punkt 1, i brottsbalken är väldigt generellt vid hänvisning till sådana personer, och framhåller att avlyssning kan användas på en misstänkt, svarande eller annan person som är inblandad i ett brott. Man har inte gett någon förklaring i fråga om exakt vem som skulle ingå i kategorin ’annan person som är inblandad i ett brott […]’ (punkterna 43–44) Domstolen fastslår att det inte framgår tydligt i den moldaviska lagstiftningen hur rimlig en misstanke mot en person måste vara för att avlyssningstillstånd ska beviljas. Lagstiftningen omfattar inte heller några skydd annat än […] att avlyssning enbart bör ske när det är omöjligt att uppnå syftet på andra sätt” (punkt 51).
[122] Min kursivering, ibidem, punkt 51.
[123] Jag har diskuterat frågan i mer detalj i Cameron, 2000, sidorna 106–109.
[124] Mål nr 26839/05, dom av den 18 maj 2010.

rör nationell säkerhet, där RIPA-kommissionären [RIPA = Regulation of Investigatory Powers Act] kontrollerar först i efterhand den dokumentation som ligger till grund för de ansökningar som godkänts av den behöriga ministern. Den tid som kommissionären ägnar åt denna uppgift innebär i praktiken att endast ett fåtal, slumpvis utvalda, fall kan undersökas noggrant. Det görs inte heller någon uppföljningskontroll, där den vad som upptagits jämförs med den dokumentation som ska motivera upptagningen. Organet som handlägger klagomål, *Investigatory Powers Tribunal* (IPT) [ung. domstolen för undersökningsbefogenheter] har knappt godkänt några klagomål. Framgångsfrekvensen är anmärkningsvärt låg, även med beaktande av att väldigt många klagomål sannolikt är grundlösa.

Vad som likväl verkar ha varit avgörande för domstolen i Kennedy-målet är att det inte funnits ”något bevis för avgörande brister i tillämpning och funktion när det gäller övervakningsförfarandet” (punkt 162). Målet stöder på så sätt påståendet att en relativt begränsad kontroll-/tillsynsmekanism är tillåten i fall där domstolen slår fast att det rått en höggradig professionalism från polisens/säkerhetstjänsternas sida i fråga om att efterleva spanings- eller övervakningslagstiftningen.

Jag bör påpeka att jag inte håller med domstolens förhållandevis okritiska inställning i Kennedy-målet. Det må vara så att missbruk- eller överanvändningsproblemen inte är stora i Storbritannien. Icke desto mindre anser jag att en trovärdig kontrollmekanism kräver ett organ som i efterhand kan bedöma både lämpligheten och lagligheten av ett beslut att utsätta någon för övervakning. Dessutom bör ett sådant organ ha de resurser som behövs för att genomföra inspektioner m.m. när sådana bedöms vara nödvändiga. Så ställer sig förvisso Venedigkommissionen till frågan.[125] Det framgår emellertid tydligt att domstolen sätter tröskeln något lägre.

Detta är lyckligtvis inte något problem i Sverige. I Sverige har det nyligen upprättats efterhandskontroll i form av Säkerhets- och integritetsskyddsnämnden, och det är onödigt att gå in på detaljer om kraven i konventionen i detta sammanhang. Det räcker att säga att det system som inrättas inte bara måste omfatta en bestämmelse om att inspelningar av irrelevanta samtal måste förstöras, utan också om att ett behörigt externt organ, lämpligen med någon form av rättslig behörighet, måste genomföra en noggrann kontroll av att

[125] Europeiska kommissionen för demokrati genom lag (Venedigkommissionen), 2007, punkt 165.

denna bestämmelse efterlevs. Regelverket ska omfatta administrativa rutiner för att det externa organet ska kunna undersöka efterlevnad, t.ex. registrering av alla inspelade samtal, registrering av personal som närvarat, noggrant kontrollerad utrustning, inspelningsmetod som minskar risken för redigeringsbehov i efterhand osv.[126]

6.4 Frågor för vidare diskussion

Det finns två frågor som jag anser bör tas upp till diskussion i denna rapport. Den första är huruvida *alla former* av hemlig övervakning måste efterkomma de krav som anges ovan. Man skulle kunna hävda att olika spaningsmetoder som nämnts tidigare (ljudupptagning, bildupptagning, lokaliseringsinformation) i olika sammanhang och på olika platser (i ”hemmet” och på andra platser) utgör olika grader av intrång i privatlivet, och att olika grader av förutsebarhet följaktligen är tillåtna inom den rättsliga ramen. Europadomstolen accepterar olika grader av *skyddsåtgärder*.[127] Den accepterar i allmänhet, vilket anges i avsnitt 4 ovan, olika grader av förutsebarhet beroende på graden av intrång i de rättigheter som fastställs i konventionen. Den bekräftade nyligen, i Uzun-målet, att olika grader av förutsebarhet är tillåtna för olika typer av spaningsåtgärder som innebär intrång i artikel 8-rättigheter. Den fastslog att de striktare principerna (som anges ovan) ”inte är tillämpliga som sådana på fall som det aktuella, nämligen övervakning via GPS av förflyttning på offentliga platser, vilket följaktligen måste betraktas som ett mindre intrång i den berörda personens privatliv än avlyssning av dennes telefonsamtal […]”. Man kommer därför att tillämpa de mer allmänna principer om tillräckligt skydd mot godtycklig överträdelse av rättigheterna i artikel 8 som sammanfattas ovan” (punkt 66). Domstolen godtog att det vid tidpunkten befintliga generella bemyndigandet att använda ”tekniska medel” utgjorde en tillräcklig rättslig grund för åtgärden under de rådande omständigheterna. När den nådde denna slutsats beaktade den emellertid ett flertal andra faktorer som i praktiken begränsade användningen av

[126] Även om bestämmelser måste fastställas och iakttas så måste inte alla avvikelser från dessa regler från polisens eller de tillståndsgivande organens sida utgöra en överträdelse av konventionen, om missbruket eller felaktigheten avhjälps av en domstol i högre instans, t.ex. genom att man inte beaktar den bevisföring som införskaffats på det sättet. Se Remmers och Hamer mot Nederländerna, mål nr 29839/96, domslut av den 18 maj 1998. Se dock den mindre fordrande.

[127] Jfr PG och JH, ”Vad som krävs i fråga om skyddsåtgärder beror, åtminstone i viss utsträckning, på den aktuella upptagningens natur och omfattning” (punkt 46 i anförda arbete).

de tekniska åtgärderna, i synnerhet det faktum att de bara kunde användas för att utreda tillräckligt allvarliga brott och, vilket redan har påpekats, att de nationella domstolarna tillämpade ett proportionalitetstest och skulle kunna utesluta bevis. (Det kan påpekas att tysk lag senare ändrades för att införa judiciell prövning av övervakning med GPS-utrustning i fall där den aktuella tidsperioden överstiger en månad.)

Syftet med att exakt definiera befogenheter är att minska riskerna för missbruk, eller överanvändning. Om andra faktorer är likvärdiga så blir den potentiella skadan för privatlivet vid missbruk eller överanvändning av befogenheten större ju högre utsträckning befogenheten i fråga utgör ett intrång i privatlivet. Det verkar följaktligen vara rimligt att inta ståndpunkten att verksamhet och åtgärder som utgör större intrång i privatlivet borde tillhandahållas med tydligare bemyndiganden och bli föremål för fler restriktioner än verksamhet som utgör mindre intrång i privatlivet.[128] Genom precision fokuserar alla som är delaktiga i brottsutredningen och tillståndsprocessen på sitt ansvar, som i slutändan avgränsas av brottet tjänstefel. Samma sak gäller för tillståndsrutiner – oavsett om beslutet fattas av överordnade polistjänstemän som agerar som ”grindvakter” eller av åklagare – för användning av tvångsmedel, antingen i allmänhet eller i situationer som uppfattas som särskilt känsliga.

Samtidigt kan denna precisionsprincip bara vara en utgångspunkt. Argumentet kan missbrukas, t.ex. för att rättfärdiga låga precisionsgrader beträffande åtgärder som utgör ett mindre intrång i varje enskild övervakad persons privatliv, men vars kumulativa effekt till följd av att åtgärden används i stor omfattning kan bli ett stort globalt intrång. Man kan å andra sidan föreställa sig situationer där brist på tydlighet i fråga om reglering av befogenheter för hemlig övervakning kan kompenseras av tätare kontroller i efterhand. Man får inte mycket vägledning av domstolens oklara hänvisning i Uzun-målet (som det hänvisas till i avsnitt 5.3.4 ovan) beträffande intrång som ”ger mer information om en persons beteende, åsikter eller känslor”. Det är svårt att i fråga om bemyndigande rangordna de olika typer av hemlig statlig övervakning som angavs tidigare, utifrån i vilken grad var och en av dem utgör ett intrång i privatlivet.

[128] En domare i den brittiska appellationsdomstolens domslut i Woods-målet, anfört arbete, intog denna ståndpunkt, men de två andra vederlade – felaktigt, enligt min uppfattning – denna. Se också McDonald-kommissionens rapport, s. 514, som hävdade att tillståndsnivån (dvs. vilken nivå i rättskedjan som beviljar tillstånd att använda en viss tvångsmedel) borde vara högre ju större intrång tekniken innebär. Detta är emellertid också knutet till skyddsåtgärder, inte till precisionsgrad.

Detta beror delvis på att begreppet privatliv kan antas variera mellan olika kulturer och från tid till annan[129], även om vissa indikationer på ”gemensamma europeiska begrepp” kan utläsas ur sammanställningar över staternas praxis som gjorts av akademierna och Europarådet.[130]

Den andra frågan är om rättspraxis ger någon antydan om att det är tillåtet med en viss skillnad i detaljnivå och typ av normgivning, beroende på *i vilket syfte* spaningen genomförs – förebyggande eller brottsutredande – eller vilka *underliggande intressen* som ska skyddas – lagföring eller skydd för den nationella säkerheten. En annan aspekt i anslutning till denna fråga är huruvida rättspraxis ger utrymme för att fastställa situationer där till och med ”privilegierad kommunikation” kan avlyssnas. Frågan om nationell säkerhet har ett nära samband med frågan om vilken grad av tillgänglighet och förutsebarhet som krävs för strategisk övervakning. De båda frågorna kan med fördel behandlas tillsammans, vilket jag gör i avsnitt 6.6.

6.5 Olika standarder för olika spaningsformer

Till att börja med klargjorde domstolen i Bykov-målet att dold ljudupptagning utgör ett minst lika stort intrång i privatlivet som hemlig teleavlyssning, oavsett om den genomförs av någon som deltar i konversationen eller inte.[131] Man kan, på grund av de olika grader av ”rimlig förväntning på skydd för privatlivet” som påstås föreligga här, försöka att göra en åtskillnad mellan graden av intrång i privatlivet vid dold ljudupptagning på en privat plats och på en offentlig plats. Men i många fall av dold ljudupptagning på offentlig plats kan åtgärden mycket väl leda till mer – till och med mycket mer – ”överskottsinformation”, t.ex. information om andra personer, som kanske inte har någonting alls att göra med den övervakade personen. Därför bör enligt min uppfattning samma, eller mer eller mindre samma, rättsliga ram gälla för dessa båda situationer, även

[129] I en stat är t.ex. inkomstdeklarationer sekretessbelagda, medan de inte är det i en annan stat.
[130] Se framför allt Europarådet, 2005.
[131] ”Enligt domstolens uppfattning gäller dessa principer i lika hög grad för användning av utrustning som sänder via radiovågor som, i fråga om beskaffenhet och intrång, är så gott som identisk med teleavlyssning” (punkt 79). Jfr SOU 2007:22, s. 182 och Vetter mot Frankrike, där domstolen nöjde sig med att konstatera att buggning, som teleavlyssning, utgjorde ett allvarligt intrång i respekt för privat liv (punkt 26).

om intrånget på den övervakades privatliv kanske kan vara mindre i det ena fallet.

Jag ska nu övergå till den grad av lagstiftning som krävs för hemlig teleövervakning. Domstolen tog ställning till det brittiska systemet i målet P.G. och J.H. Enligt detta kan polisen kräva att telefonbolaget skulle lämna ut information om teleadresser m.m. Om bolaget vägrade att lämna ut informationen kunde polisen begära att en domstol utfärdade en order om utlämnande. Lagstiftningen i detta avseende utgjordes av undantag i relevanta sekretessbestämmelser. Med andra ord hade telefonbolaget rätt att lämna ut de uppgifter som polisen krävde utan sådan bestraffning som annars skulle tillfalla bolaget för utlämnande av personuppgifter. Domstolen noterade att ”informationen som inhämtades rörde vilka telefonnummer som ringts från B:s lägenhet mellan två specifika datum. Den innehöll inga uppgifter om innehållet i dessa samtal eller om vem som ringde eller tog emot dem. Den information som inhämtades, och vad den kunde användas till, var följaktligen mycket begränsad. Även om det inte verkar finnas några specifika lagregler (i motsats till interna riktlinjer för polisen) för lagring och förstörelse av sådan information är domstolen inte övertygad om att bristen på ett sådant detaljerat, formellt regelverk innebär någon risk för godtycklighet eller missbruk. Det framgår inte heller att det förelegat någon brist på förutsebarhet. Det är tillåtet att lämna information till polisen inom den relevanta rättsliga ramen om detta krävs för att upptäcka och förhindra brott, och materialet användes i detta fall vid rättegången mot sökandena för att bekräfta annan bevisning som var relevant för telefonsamtalens tidsramar. Det framgår inte tydligt att sökandena inte hade fått en tillräcklig indikation på under vilka omständigheter och på vilka villkor de offentliga myndigheterna hade befogenhet att tillgripa en sådan här åtgärd.”[132]

När en rättslig ram utarbetas för tillstånd till och kontroll av hemlig teleövervakning är det enligt min uppfattning rimligt att ta hänsyn till att det ligger de två syften bakom, nämligen inhämtande av underrättelsematerial och inhämtande av bevismaterial. De två syftena har naturligtvis ett nära samband, eftersom de delaktiga i en kriminell sammanslutning måste identifieras innan man samlar bevis mot dem. Underrättelsematerial kan i ett senare skede bli bevis. Information om att t.ex. A, enligt dennes mobiltelefon, befann sig på en viss plats vid en viss tidpunkt kan visa sig vara en mycket

[132] Punkterna 46–47.

värdefull indiciebevisning som motbevisar, eller bevisar, A:s version av händelseförloppet. Det skulle mycket väl kunna vara så att hemlig teleövervakning används mycket oftare i underrättelsesyfte än i bevissyfte. Om syftet är att samla information i underrättelseverksamheten är det polisen som är bäst lämpad att bestämma om teledata behövs och i så fall vilken sorts information och i vilken omfattning.[133]

Syftet med inhämtningen kan även påverka åtgärdens varaktighet. Dessutom har syftet avgörande betydelse för vilka rättsmedel som finns tillgängliga efter att åtgärden upphört. Ytterligare en skillnad rör ”överskottsinformation”. Om hemlig teleövervakning görs, för att inhämta uppgifter om en lös sammansatt grupp människor, eller ett fenomen, så kommer sannolikt en mindre andel av uppgifterna att betraktas som ”överflödig” jämfört med vid en utredning av ett specifikt brott som begåtts, eller som planeras, av en specifik grupp. (.)

Man kan med rätta säga att domstolen satte en låg standard för ”med stöd av lag” i målet P.G. och J.H. Det fanns inget uttryckligt bemyndigande för hemlig teleövervakning i det brittiska systemet. Frågan är om domstolen verkligen har insett vilken information som kan inhämtas vid hemlig teleövervakning nuförtiden.[134] Man kan, vilket redan har nämnts, hävda att uppgifter som handlar om Internetanvändning är känsligare än vilka mobiltelefonnummer som ringts, en uppgift som i sin tur är känsligare än lokaliseringsinformation. Det finns vissa empiriska bevis för att människor anser att lokaliseringsinformation är den minst känsliga typen av information.[135] Men i praktiken kan en person använda Internet från sin mobiltelefon, eller använda sin bärbara dator för att ringa ett samtal samtidigt som han eller hon surfar på nätet. Om man övervakar ett sådant användande, i realtid eller i efterhand, får man information om alla tre uppgiftskategorierna. Det verkar följaktligen inte gå att fastställa olika trösklar för reglering och kontroll över inhämtande av dessa tre olika typer av uppgifter.

Det verkar inte råda något tvivel om att hemlig teleövervakning är ett användbart utrednings- och informationsredskap.[136] I Sverige har dock bristen på tillgång till tillförlitlig information om hur ofta

[133] Samtidigt innebär det faktum att polisen bäst vet vilken sorts, och hur mycket, information som krävs inte att polisen är bäst lämpad att bedöma om fördelarna för polisutredningen uppväger förlusten av mänskliga rättigheter för den misstänkte och andra personer som kommer med i insamlingen av information – tvärtom.
[134] Jfr Lagerwall 2008, s. 64.
[135] van Loenen m.fl., 2008, s. 149.
[136] Se t.ex. Ianni 1990 och Krüpe-Gescher och Dorsch, 2005 (en sammanfattning av en undersökning av tysk praxis som utförts under ledning av Max Planck-institutet i Freiburg).

och på vilka sätt hemlig teleövervakning har främjat effektiviteten av undersökningar och utredningsarbete gjort det svårt att uppskatta *hur* användbar åtgärden har varit, och att väga detta mot det intrång i den personliga integriteten som den utgör.[137] När hemlig teleövervakning görs i underrättelsessyfte bör man vara tydlig med att legaliteten och proportionaliteten sällan kommer att kontrolleras i efterhand vid en rättegång. Någon form av kontroll i efterhand är därför nödvändig för att förhindra missbruk och överanvändning. I målet P.G. och J.H. tog man dock inte upp förekomsten och funktionen av de brittiska kontrollerna av upptagning av telekommunikationsuppgifter, och det gjorde man inte heller i Heglas-målet. Jag tror emellertid att det är mycket sannolikt att Europadomstolen i framtiden kommer att kräva någon form av system för efterföljande kontroll av hemlig teleövervakning om och när den konfronteras med denna fråga igen.

Jag kommer inte att gå in på det system för efterföljande kontroll av uppgifter om telemeddelanden som redan har föreslagits av polismetodutredningen. Jag vill dock påpeka en sak. Problemet med *missbruk* av åtgärden ska hanteras genom att Säkerhets- och integritetsskyddsnämnden (SIN) rapporterar till åklagaren. Problemet med *överanvändning* kommer dock sannolikt att i praktiken bli ett vanligare problem. Om eller när nämnden upptäcker ett överanvändningsmönster kommer detta sannolikt att framkomma en viss tid – eller en lång tid – efter att åtgärderna har slutförts. Ett bekräftat överanvändningsmönster måste rimligtvis leda till kritik mot den behöriga polismyndigheten. Kritiken har ett framåtblickande syfte, dvs. det skall leda till förbättring av systemet. Det måste emellertid också ingå ett bakåtblickande element. Jag har inte riktigt klart för mig hur SIN förväntas agera om den konstatera att överanvändning (men inte missbruk) har skett. Om det bara blir ett konstaterande att en viss överanvändning har ägt rum, men inga negativa konsekvenser för den berörda polismyndigheten, finns det risker att tillståndsgivande polis kommer att främja överanvändning av hemlig teleövervakning på grund av de operativa fördelar som detta kan ge.

Avslutningsvis vad gäller denna fråga kommer jag att ta upp bildupptagning både i och utanför hemmet. Även om det råder brist på rättspraxis i frågan anser jag att bildupptagning av hemmet eller annat ”privat utrymme”, som hotellrum, borde uppfylla liknande relevanta normer som dem som gäller för teleavlyssning och

[137] SOU 2007:22, s. 185.

dold ljudupptagning. Syftet med att kräva lagstadgat bemyndigande är (även om domstolen inte har sagt detta uttryckligen) att betydande intrång i privatlivet bör uppmärksammas och tas under noggrant övervägande av den lagstiftande församlingen. Om de tre typerna av övervakning anses innebära mer eller mindre samma grad av intrång i privatlivet så är den logiska följden att följande bör regleras *i lag* för bildupptagning av hemmet: vilka brottsbeskrivningar som berättigar till åtgärden, under vilka omständigheter man kan använda denna metod mot misstänkta eller personer som dessa kommer i kontakt med, en gräns för hur länge en bildupptagning får pågå, vilka förfaranderegler som bör gälla för undersökning, användning och lagring av uppgifter som inhämtats, vilka försiktighetsåtgärder som måste vidtas vid överföring av uppgifter till andra parter och under vilka omständigheter upptagningar kan eller måste raderas eller lagringsmedier måste förstöras.

Bildupptagningar *utanför* hemmet har hittills inte betraktats av domstolen som ett intrång i privatlivet, vilket redan framgått i de tidigare avsnitten. Bevarande av detta material kan emellertid mycket väl betraktas som ett sådant intrång. Det mål som främst diskuterar vilka krav som ställs för bevarande av personuppgifter i brottsbekämpningssyfte är S och Marper mot Förenade kungariket.[138] Detta mål, som behandlades av Europadomstolen (stora kammaren), handlade om bevarande av fingeravtryck och DNA-prov som tagits från en brottsmisstänkt person. Vid den tidpunkten fick sådana uppgifter bevaras på obestämd tid enligt engelsk lag, även om den misstänkte frikändes i det efterföljande straffrättsliga förfarandet. Domstolen började med att ta ställning till om bevarandet av tre olika identifieringskategorier, nämligen fingeravtryck, cellprov och DNA-profiler[139], innebar intrång i privatlivet. Den svarande regeringen hade hävdat att bevarandet av dessa uppgifter inte utgjorde intrång i de berörda personernas fysiska och psykiska integritet, och inte heller i deras rätt till personlig utveckling. Domstolen fastslog dock att bevarandet ”med tanke på beskaffenheten hos ett cellprov och den mängd personlig information som cellprov innefattar per se måste betraktas som ett intrång i privatlivet” (punkt 73). Vad gäller DNA-profiler fäste domstolen vikt vid att den information som ingår i dessa innebär att myndigheterna kan göra mer än

[138] Mål nr 30562/04 och 30566/04, dom av den 4 december 2008.
[139] En DNA-profil tas fram genom analys av ett referensprov från en individ. Den består av en uppsättning siffror som kan presenteras i form av en streckkod. Sedan kan man göra en automatiserad matchning av profilen med andra profiler.

att bara fastställa personers identitet. I fråga om fingeravtryck innebär den ”unika” information om den berörda personen som fingeravtryck bär på, vilket möjliggör en detaljerad identifiering i många olika situationer, även om de påverkar privatlivet i mindre grad, att ett bevarande av fingeravtryck utan personens medgivande ”inte kan betraktas som neutralt eller obetydligt”. Detta utgjorde följaktligen också ett intrång i rätten till respekt för privatlivet (punkterna 84–85).

Ett fotografi eller en film av en person kan betraktas som något oerhört känsligt av den person det berör, beroende på den subjektivt uppfattade risken för förlägenhet eller till och med skada när det gäller det personliga intresset som en spridning av sådan information till allmänheten, eller till särskilda personer, kan orsaka. Spridningen skulle också kunna tas emot med likgiltighet av den berörda personen, eller till och med välkomnas. Därför kan man inte säga att *alla* bildupptagningar i sig innefattar samma risk för intrång i privatlivet som alla DNA-prov gör. Å andra sidan kan man anse att en bildupptagning kan ge upphov till liknande integritetsfrågor som ett fingeravtryck. Även om det naturligtvis är möjligt att skilja mellan fingeravtryck och fotografier så anser jag att det finns starka skäl att samma krav bör gälla för båda.

Innebörden i det engelska systemet för bevarande av registrering av DNA och fingeravtryck var att det inte fanns någon mekanism tillgänglig med vilken man kunde balansera fördelen för polisen i deras arbete med att upptäcka och utreda brott mot det intrång i privatlivet som bevarandet av dessa dokumentationer innebar. I målet S och Marper slogs domstolen av ”den fullständiga och urskillningslösa natur som kännetecknade befogenheterna för bevarande i England och Wales. Materialet kunde bevaras oavsett brottets art och karaktär och den misstänktes ålder. Det fanns inte heller någon tidsbegränsning för bevarande, och en frikänd person hade bara begränsade möjligheter att avlägsnas från den landsomfattande databasen eller att låta förstöra materialet. Det fanns inte heller några bestämmelser om oberoende granskning av motiveringen till bevarandet” (punkt 119). Regeringen hade hävdat att enbart bevarande av uppgifterna inte kunde få några betydande följder för de berörda individerna, men domstolen höll inte med om det. Domstolen ansåg att presumtionen att någon är oskyldig (som fastställs i artikel 6.2) utgjorde en relevant del av tolkningssammanhanget, även om bevarande av uppgifter i sig inte utgör ett sådant ”uttryck för fortsatt misstanke”. Domstolen ansåg att det förelåg en tydlig risk för stig-

matisering med ett bevarande av uppgifter om alla, inklusive personer som hade frikänts, eller aldrig blivit åtalade, och att bevarande skulle kunna vara ”särskilt skadligt i ärenden som rör minderåriga, med tanke på deras särskilda situation och betydelsen av deras utveckling och integration i samhället” (punkterna 122 och 124). I detta avseende fäste domstolen uppmärksamhet vid den oro som uttrycktes över att ungdomar och etniska minoriteter var överrepresenterade i databasen. Avslutningsvis röstade domstolen enhälligt för att man, med den fullständiga och urskillningslösa natur som kännetecknar befogenheten att bevara alla tre kategorierna av personlig information, inte hade lyckats finna en rättvis balans mellan offentliga och privata intressen och att det förelåg en överträdelse av artikel 8.

Konsekvenserna av detta för bildupptagningar verkar bli som följer. Eftersom polisen har uppgiften att utreda och förhindra brottslighet kommer en viss grad av misstanke om ett tidigare, pågående eller till och med framtida brott att ge tillräcklig grund för bevarande av bildupptagningar med vilka man kan identifiera en viss person. Någon form av rättslig befogenhet verkar krävas för bevarande av fotografier av misstänkta som fotograferats i hemlighet, även om ingenting visar på att Europadomstolen skulle kräva att regleringen ska vara i lagform.[140] Den grad av misstanke som krävs för att berättiga bevarande av information kan rimligen förväntas variera i enlighet med brottets allvarlighetsgrad.[141] Behovet av sekretess när det gäller utredningsarbete (åtminstone när det gäller pågående och framtida brott, och tidigare brott som av någon anledning inte lett till lagföring, men där det fortfarande råder en rimlig misstanke mot en person) innebär när det gäller dolda visuella inspelningar att själva det faktum att det finns en inspelning kan hållas hemligt. Eftersom polisen måste ges omfattande handlingsutrymme på detta område är det, vilket nämndes tidigare, nödvändigt att någon form av extern kontrollmekanism finns tillgänglig, som kan övervaka och påverka den allmänna praxisen för bevarande. Eftersom

[140] Den tillämpliga rättsliga regleringen , rättegångsbalken och förordningen (1992:824) om fingeravtryck m.m. omfattar bara fotografering av anhållna personer. Se också RPSFS 2005:12 – FAP 473 1.

[141] Jfr domare Laws kommentar i Woods-målet, punkt 84 i anförda arbete: ”Domstolen måste noggrant väga det legitima syfte som eftersträvas, vikten av den rättighet som är föremål för intrång och omfattningen av intrånget. Ett intrång vars syfte är att skydda samhället från risken för terrorism anses följaktligen med större beredvillighet vara av rimlig proportion än ett intrång vars syfte är att skydda samhället för risken för kriminalitet på låg nivå eller störning av den allmänna ordningen.” Se också den tyska författningsdomstolens (BVerfG) ståndpunkt beträffande spridning av information, som noteras i nästa avsnitt.

detta gäller operativa beslut kommer enbart ett organ med kompetens i fråga om att väga fördelarna med utredningen mot intrånget i privatlivet att uppfylla kravet i konventionen på ”att vara nödvändig i ett demokratiskt samhälle”.[142] Man måste också tillhandahålla ett verksamt rättsmedel med en instans som kan göra proportionalitetsbedömningar när det gäller fortsatt bevarande av uppgifter som rör viss person om personen lämnar in ett klagomål.[143] Det bör återigen betonas att själva existensen, eller avsaknaden, av en upptagning kan hållas hemlig för den klagande om det finns behov av sekretess med avseende på utredningsarbetet i det enskilda fallet.

6.6 Proaktiv övervakning, nationell säkerhetsövervakning och strategisk övervakning

Det råder en betydande, men inte total, överlappning mellan kategorierna proaktiv övervakning (vilket innebär övervakning som utformats för att förhindra brottsliga gärningar), övervakning av nationella säkerhetsskäl och strategisk övervakning. Olika stater erbjuder olika sorters övervakning delvis beroende på huruvida de har en säkerhetstjänst med polisiära befogenheter (vilket tenderar att innebära ett starkare samband mellan övervakning och brott) och huruvida de har kapacitet till strategisk övervakning.

Intrång i privatlivet är tillåtet inte bara så vitt gäller utredning av pågående eller redan begångna brott. Enligt ordalydelsen i artikel 8 är ett sådant intrång tillåtet även för att förhindra brott eller störning av den allmänna ordningen. I målet Weber och Saravia accepterade exempelvis domstolen att det tyska systemet för strategisk övervakning, som inte måste bindas till brott, kunde rättfärdigas vid förhindrande av brott och skydd av den nationella säkerheten.[144]

Gränslinjen mellan ”förebyggande” och ”utredande” övervakning är inte fast. Den är beroende av hur brotten är utformade och det åtföljande nationella regelverket i den allmänna delen av straff-

[142] Syftet med denna rapport är att analysera kravet på ”med stöd av lag”, och därför kommer jag inte att gå in på denna fråga här. Jag vill dock påpeka att domstolen i målet Segerstedt-Wiberg mot Sverige, nr 62332/00, dom av den 6 juni 2006, inte ansåg att Datainspektionen var ett tillräckligt rättsmedel, eftersom den i praktiken inte ifrågasatte operativa beslut av säkerhetspolisen om att bevara uppgifter. Se Cameron, 2000, s. 222–258 för en allmän behandling av kontrollfrågorna.
[143] Jfr Segerstedt-Wiberg ibidem (överträdelse av artikel 13, eftersom inget organ fanns då som kunde fastställa proportionaliteten av att ge eller inte ge tillträde till säkerhetsakter).
[144] Punkt 104 i anförda arbete.

rätten angående brottsförberedelse och delaktighet i brottslig verksamhet (medverkan, stämpling, förberedelse, försök osv.). I synnerhet säkerhetsbrott tenderar att ”börja” tidigt i den meningen att även planeringsstadiet straffbeläggs.[145] Europadomstolens rättspraxis betonar precision i utformningen, att övervakning måste begränsas till de allvarligaste brotten och att det måste finnas tillräckliga skydd mot missbruk. Det är därför rimligt att dra slutsatsen av domstolens rättspraxis att övervakning enbart bör få användas för att förhindra antingen *allvarliga hot mot den nationella säkerheten* eller en *tydligt definierad* kategori av de *allvarligaste* säkerhetsbrotten som fastställts i ett lands strafflagar. Dessutom måste det för det första finnas goda skäl för att tro dessa brott eller hot ligger för handen och för det andra att övervakning skulle bidra till att förhindra dessa.

Det är rimligt att anta att förebyggande övervakning ofta, eller åtminstone i vissa fall, baseras på spekulativa uppgifter som inte uppfyller straffrättens normer för ”skälig anledning” att misstänka brott. På så sätt medför förebyggande övervakning en större risk för missbruk och överanvändning. Det är rimligt att anta att befogenheterna att tillgripa sådan övervakning måste definieras så noggrant det går, och, eftersom exaktheten ändå blir bristfällig, måste det finnas mer omfattande skydd mot missbruk och överanvändning vid den här typen av övervakning jämfört med övervakning i brottsutredande syfte.

Staterna har en tolkningsmarginal i hur de väljer att konstruera sina system för beviljande av tillstånd för övervakning av säkerhetsskäl. Jag kan dock påpeka att ett enkelt proportionalitetstest när det gäller att väga det aktuella brottets allvarlighet mot intrånget i den misstänktes privatliv, och andra personers privatliv som involveras i utredningen, innebär en risk för att bemyndigande ges rutinmässigt för mycket allvarliga brott, även om den faktiska fördelen för utredningen eller det förebyggandet arbetet är mycket liten eller obefintlig på grund av omständigheter i det enskilda fallet. Det skulle därför förmodligen vara klokt att ställa som villkor att följande successiva förutsättningar ska uppfyllas vid förebyggande övervakning: att sannolikheten är stor för att den övervakade personen ägnar sig eller har ägnat sig åt grov brottslighet *och* att sannolikheten är stor för att den hemliga övervakning som begärs kommer att bidra till att förhindra brottet.

[145] Se Asp och Cameron 2010 för en diskussion om kriminaliseringsstadierna vid brottet främjande av terrorism.

Vad gäller övervakning av nationella säkerhetsskäl har domstolen godtagit att detta inte behöver kopplas till konkreta brottsutredningar. Skälet till detta är att vissa stater har civila säkerhetstjänster utan polisära befogenheter.

Domstolen har inte försökt att definiera begreppet nationell säkerhet. Kommissionen ansåg tidigare att ”nationell säkerhet” inte kan definieras helt och hållet.[146] Domstolen har emellertid ställt sig alltmer skeptisk till staternas argument att den nationella säkerheten rättfärdigar en vagare och flexiblare inställning till kraven på förutsebarhet och tillgänglighet. Det är förvisso allt svårare att motivera att man inte ställer några krav på stater så vitt gäller övervakning av nationella säkerhetsskäl med tanke på att det ”polisära” området och säkerhetsområdet överlappar varandra, särskilt i fråga om terrorism. I målet Amann mot Schweiz var sökanden en affärsman som importerade hårborttagningsutrustning. År 1981 ringdes han upp av en kvinna från sovjetiska ambassaden som ville köpa en hårborttagningsapparat. Sovjetiska diplomaters samtal avlyssnades rutinmässigt av den schweiziska säkerhetspolisen och man öppnade en akt (om än bara ett kortregister) om sökanden som en ”kontaktperson”. Sökanden gjorde bland gällande annat att teleavlyssningen saknade stöd i lag. Enligt de nationella bestämmelser som tillämpades vid den tidpunkten (federala rådets föreskrifter om polisiära tjänster inom federala åklagarmyndigheten från 1958) fick polisen behörighet att bedriva ”övervakning och förebyggande av handlingar som skulle kunna utgöra ett hot mot Schweiziska edsförbundets inre eller yttre säkerhet”. En liknande formulerad bestämmelse återfinns i artikel 17 i den federala straffprocesslagen. Domstolen ansåg emellertid inte att dessa bestämmelser var tillräckligt förutsebara för att tjäna som grund för teleavlyssning, inte ens för ”passiv avlyssning”, som det rörde sig om i detta fall. Den fastslog att bestämmelserna inte innehåller något ”tillkännagivande i fråga om de personer som berörs av sådana åtgärder, under vilka omständigheter som åtgärderna kan tillämpas, vilka medel som används eller vilka förfaranden som måste iakttas. Dessa regler kan därför inte anses vara tillräckligt tydliga och detaljerade för att tillhandahålla

[146] Mersch m.fl. mot Luxemburg, mål nr 10439-41/83, 10452/83 och 10512-3/83, 43 DR 78 (1985). Se också M. mot Frankrike, mål nr 10078/82, 41 DR 103, 117 (1985). ”När det gäller den juridiska definitionen av brott mot den nationella säkerheten, territoriella integriteten och allmänna säkerheten är den enskilda statens myndigheter bäst lämpade att besluta om det krävs en restriktion som är utformad för att förhindra sådana brott.”

ett lämpligt skydd mot intrång av myndigheterna i sökandens rätt till skydd för privatliv och korrespondens."[147]

Mer allmänt kan man säga att domstolen blir alltmer medveten om utrymmet för missbruk av begreppet nationell säkerhet.[148] I *Iordachi*-målet angavs "nationell säkerhet" som en av grunderna för övervakningen. Domstolen kritiserade bristen på konkretisering av detta och andra begrepp som användes i den moldaviska lagstiftning som tillämpades.[149] I målen *Association for European Integration and Human Rights och Ekimdzhiev* hänvisade domstolen till behovet av att se till att "inte utvidga konceptet 'nationell säkerhet' bortom dess naturliga innebörd".[150] Målen *Liberty* och *Weber och Saravia*, som diskuteras nedan, illustrerar en snävare syn på nationell säkerhet. Och det finns flera andra mål som innehåller säkerhetsrelaterade befogenheter i olika sammanhang, t.ex. säkerhetskontroll och utvisning av säkerhetsskäl, där domstolen har uttryckt behov av stränga kontroller av tillämpning av säkerhetsbefogenheter för att förebygga missbruk.[151]

I ett avseende verkar domstolen ha godtagit att den nationella säkerheten gett utrymme för större frihet. I en rad europeiska länder, t.ex. i Tyskland och Storbritannien[152], är övervakning i brottsbekämpande syfte av särskilda kategorier av människor inte tillåten. Samtidigt framstår det som om det beviljas undantag för sådan övervakning när det motiveras av nationella säkerhetsskäl. Dessa förbud är utformade på olika sätt. Förbudet kan gälla för alla som

[147] Punkt 58.
[148] När det gäller en tidig varningssignal i detta avseende, se domare Pettitis separata yttrande i Kopp-målet: "Lagstiftningen i ett flertal EU-medlemsstater uppfyller inte artikel 8 när det gäller teleavlyssning. Länderna använder eller missbrukar koncepten tystnadsplikt och sekretess för att skydda den nationella säkerheten. De förvränger innebörden av detta begrepp om så krävs. Det krävs ett visst förtydligande av vad dessa koncept innebär för att systemet för förebyggande av terrorism ska förfinas och förbättras. […] Domstolens beslut i målen Klass, Malone, Huvig och Kruslin har i stort förblivit ineffektiva. De som styr de behöriga statliga myndigheterna slår dövörat till för dessa förelägganden och agerar i viss mån opåtalt […]."
[149] Punkt 46 i anförda arbete.
[150] Punkt 84 i anförda arbete.
[151] Se t.ex. Rotaru mot Rumänien, mål nr 28341/95, dom av den 4 maj 2000, Al-Nashif mot Bulgarien, mål nr 50963/99, dom av den 20 juni 2002, punkt 124 (utvisning av säkerhetsskäl), Turek mot Slovakien, mål nr 57986/00, dom av den 14 februari 2006 (påstådd tidigare medarbetare inom statlig säkerhetsmyndighet som inte kunnat bestrida registrering av honom i myndighetens akter i förfaranden som garanterar likabehandling av båda parter), Gulijev mot Litauen, mål nr 10425/03, dom av den 16 december 2008 (utvisning på grund av "hemlig" rapport från den statliga säkerhetsmyndigheten som inte visades för sökanden), A. m.fl. mot Förenade kungariket, mål nr 3455/05, dom av den 19 februari 2009 (internering av säkerhetsskäl), Nolan och K. mot Ryssland, mål nr 2512/04, dom av den 12 februari 2009 (utestängande av utländsk aktivist inom Enighetskyrkan ur landet, vilket ska ha skett av säkerhetsskäl: överträdelse av artikel 9).
[152] Se Europarådet, 2005.

befrias från skyldigheten att avge vittnesmål inom ramen för nationell lagstiftning (läkare, präster, journalister osv.)[153] eller enbart för mer begränsade kategorier, t.ex. en försvarsadvokat som uttryckligen eller underförstått anlitats av en misstänkt.[154] Bland annat målen Klass mot Förbundsrepubliken Tyskland, Kopp mot Schweiz och ett senare avlyssningsmål, Erdem mot Tyskland[155], visar att staterna enligt konventionen *inte* måste avhålla sig helt och hållet från att avlyssna ”konfidentiella meddelanden”, t.ex. mellan en försvarsadvokat och dennes klient.[156]

Nu ska jag gå vidare med strategisk övervakning. I målen *Weber och Saravia* hade sökandena hävdat att de tyska myndigheterna hade brutit mot internationell rätt genom att avlyssna privat kommunikation som inleddes och avslutades i ett annat land. Domstolen ansåg att begreppet ”lag” hänvisar till nationell lagstiftning, inklusive sådana regler inom folkrätten som tillämpas i den aktuella staten. Domstolen krävde dock bevis i form av ”överensstämmande slutsatser om att myndigheterna i den svarande staten har agerat extraterritoriellt på ett sätt som är oförenligt med den andra statens suveränitet och därmed strider mot internationell rätt” (punkt 87). Domstolen fastslog att ”signaler som sänds ut från andra länder övervakas genom radiospaning på tysk mark och de uppgifter som samlas in används i Tyskland” (punkt 88). Domstolen ansåg under dessa omständigheter inte att sökandena kunde styrka sina anklagelser.[157] Vad gäller lagens kvalitet drog domstolen slutsatsen att de bestämmelser i G10-akten i dess ändrade lydelse (dvs. efter den tyska författningsdomstolens [BVerfG] granskning, se nedan) som ifrågasatts innehåller de minimiskydd mot godtyckligt intrång som definieras i domstolens rättspraxis.[158]

---

[153] T.ex. artikel 125 h i förening med artikel 218 i den nederländska straffprocesslagen.

[154] T.ex. 27:22 RB. Denna definition innebär att inte alla samtal mellan en advokat och en misstänkt är skyddade. Jfr den bredare kategorin av personer i kapitel 36:5 RB.

[155] Mål nr 38321/97, dom av den 5 juli 2001.

[156] Se även Hewitt och Harman mot Förenade kungariket, mål nr 20317/92, där en av sökandena, en advokat, påstod att bland annat hennes samtal med klienter ingick i akter som bevarades. Kommissionen accepterade att det fanns en rimlig sannolikhet för att detta stämde, men kunde inte konstatera någon överträdelse av artikel 8. Domare Pettitti uttryckte i ett separat yttrande i Kopp-målet att övervakning av maken aldrig ska tillåtas, inte ens i säkerhetsärenden. Se också det brittiska målet, *In re McE (Appellant) (Northern Ireland)*, *In re M (Appellant) (Northern Ireland)*, *In re C (AP) and another (AP)(Appellants) (Northern Ireland) [2009] UKHL 15*, där överhuset framhöll att det i undantagsfall var möjligt att låta kontakter mellan advokat och klient vara föremål för hemlig övervakning.

[157] Möjligheten att avlyssna telekommunikation i andra länder, naturligtvis utan att söka rättsligt bemyndigande för detta, blev föremål för stor debatt och oenighet i samband med den europeiska konventionen om inbördes rättshjälp i brottmål den 12 juli 2000, EGT C 197.

[158] Se punkt 98 i domstolens beslut. De specifika normerna anges nedan i diskussionen om Liberty-målet.

Det bör i detta sammanhang påpekas att BVerfG tidigare hade granskat de ändringar som gjorts i den tyska lagstiftningen som tillät strategisk övervakning och kunnat konstatera att vissa av dem stred mot konstitutionen.[159] Vad gäller frågor som i huvudsak faller inom ramen för ”med stöd av lag” ansåg BVerfG att ett inbegripande av brottet penningtvätt inte var motiverat. Den ansåg också att föreskrifterna om överföring av information till polisen var oacceptabel. Förteckningen över brott i artikel 3.3 i G10 omfattar vissa mindre förseelser. BVerfG specificerade att indikationerna på att en viss person har begått ett brott måste vara mer konkreta ju mindre allvarligt brottet är innan överföring av information kan tillåtas. Också uppgörelsen om bevarande och användning av information av underrättelsetjänsten (avsnitt 3.4) och överföring av information till regeringen (avsnitt 3.3) ansågs vara för ospecificerad. Den tyska underrättelsetjänsten får naturligtvis all möjlig intressant information genom sitt fiskande i telekommunikationer. BVerfG framhöll att det i G10-lagen borde anges specifikt att enbart information som hör hemma inom underrättelsetjänstens verksamhet (dvs. berör landets säkerhet) får bevaras och användas av underrättelsetjänsten och överföras till regeringen. BVerfG angav mer allmänt att artikel 3.7 i G10-lagen var bristfällig, eftersom det inte fanns någon tydlig föreskrift om skyldigheten att ”markera” information som inhämtats genom strategisk övervakning, så att denna kunde identifieras (och så att användningen av den kunde kontrolleras). Slutligen borde information som hade använts på något sätt inte förstöras (en punkt som har samband med underrättelse). Således hade BVerfG ställt höga rättsstatskrav och det fanns inget behov för Europadomstolen att ställa högre krav.

I Liberty-målet ansåg domstolen däremot att det brittiska systemet för strategisk övervakning inte hade ”stöd av lag”. Storbritanniens regering hävdade i detta mål att tillgänglighetskraven borde vara lägre. Det som diskuterades var s.k. ”paragraf 6 föreskrifter”. Dessa är de tekniska sökparametrarna som utformats för att, tillsammans med instruktionerna till tjänstemännen om hur en underrättelseutvärdering görs av det upptagna råmaterialet och till vem dessa utvärderingar kan skickas, minimera insamlingen av överskottsinformation. Dessa hade inte offentliggjorts vid den tidpunkten. Än i dag har bara delar av dem offentliggjorts, i form av utdrag ur de riktlinjer som tjänstemännen ska använda. Till att börja med

[159] BVerfG, 1 BvR 2226/94, 2420/95 och 2437/95, av den 14 juli 1999, i NJW 2000, s. 55–68. Tack till Tobias Wagner för hjälp med översättningen.

hävdade regeringen att ett avslöjande av dessa riktlinjer skulle skada den nationella säkerheten, eftersom det skulle innebära att information om sökmetoder skulle tillkännages, vilket skulle ge eventuella övervakade personer möjlighet att ändra beteende. Den hävdade också, vilket jag anser undergräver det första argumentet, att dessa riktlinjer ändå var obegriplig för alla som inte har omfattande teknisk kunskap på detta område. Regeringen hävdade vidare att det inte var rättvist att göra jämförelser med det mycket öppnare tyska systemet. Dessutom var terrorhotet mot Storbritannien mycket större än mot andra länder, vilket borde ge landet rätt till ett större handlingsutrymme. Regeringen hävdade att det brittiska systemet hade helt andra skydd, i synnerhet tillsynen av en erfaren domare som bedriver kontroll av systemet i efterhand och bland annat undersöker hur paragraf 6-föreskrifterna fungerar (IOC-kommissionär). I detta avseende hänvisade regeringen till det tidigare målet Christie mot Förenade kungariket.[160] En av de frågor som kommissionen fick ta ställning till i detta fall var om det bemyndigande att avlyssna kommunikation när detta behövdes av ”nationell säkerhetsskäl” var tillräckligt tydligt och förutsebart. I Christie mot Förenade kungariket ansåg kommissionen att ett vagt begrepp kan ”förklaras med administrativa eller praktiska redogörelser eller instruktioner”[161]. Den hänvisade till det krav som fastställs i lagen på att minimera intrång och förstöra överskottsmaterial, den övervakningsbehörighet som IOC-kommissionären har och de påpekanden som denne gjort i två av sina årsrapporter beträffande begreppet ”nationell säkerhet”.[162] Den fastslog slutligen att lagen under rådande omständigheter uppfyllde kravet på ”med stöd av lag”.

Men om man tittar på dessa kommentarer ser man att IOC-kommissionären i själva verket inte specificerade begreppet ytterligare, utan helt enkelt erkände problemen med detta.[163] Medan konventionsorganen har ansett att genomförandebestämmelser (föreskrifter osv.) faller inom ramen för begreppet ”lag” kan man säga att det är en betydande utvidgning av begreppet att hävda att praktiska *redogörelser* kan göra det. Kommissionen sade i grund och

[160] Christie mot Förenade kungariket, mål nr 21482/93, 78A DR 119 (1994).
[161] S. 135, med hänvisning till domstolens utlåtande i Silver mot Förenade kungariket av den 25 mars 1983, A/61, punkterna 88–89.
[162] Kommissionärens rapporter för 1986 och 1988, Cm. 108 (1987) respektive Cm. 652 (1989).
[163] Kommissionären betonade också i sina kommentarer att alla inblandade uträttade sitt arbete ordentligt och att det inte fanns anledning till oro. En sådan förnyad försäkring är ett återkommande drag i det brittiska systemet, se t.ex. kommissionärens förklaring i dennes rapport för 1997, Cm. 4001 punkt 32, om varför man inte behöver oroa sig för otillåten avlyssning.

botten att själva existensen av en IOC-kommissionär räckte för att uppfylla kraven om lagens kvalitet.

Domstolen avvisade, enligt min uppfattning med rätta, samtliga av regeringens argument i målet Liberty. Domstolen fastslog att den ”inte anser att det finns någon anledning att tillämpa skilda principer beträffande tillgänglighet och tydlighet hos regler som gäller för avlyssning av enskilda kommunikationer å ena sidan och mer allmänna övervakningsprogram å den andra”. Domstolens inställning till kravet på förutsebarhet på detta område har därför utvecklats sedan kommissionen tog det brittiska övervakningssystemet i betraktande i målet Christie mot Förenade kungariket.[164]

Den tillade att IOC-kommissionären (nu RIPA-kommissionären), även om denne är ett ”viktigt skydd” mot maktmissbruk, inte ”bidrar till systemets tillgänglighet och tydlighet”.[165] Domstolen fortsatte med att ange alla saker som *borde* vara tillgängliga i skriven lag, med hänvisning till dess tidigare domslut i målet Weber och Saravia: ”I G10-akten stod det framför allt att den tyska underrättelsetjänsten enbart var behörig att övervaka kommunikation med stöd av sökvillkor som tjänade, och var lämpliga för, en undersökning av de risker som beskrevs i övervakningsordern, och vilka sökvillkor som måste anges i övervakningsordern. […] Dessutom angavs reglerna för lagring och förstöring av uppgifter som inhämtats genom strategisk övervakning i detalj i artikel 3.6 och 3.7 och i artikel 7.4 i G10-akten i dess ändrade lydelse. De myndigheter som lagrade uppgifter måste var sjätte månad intyga att dessa uppgifter fortfarande behövdes för att nå det syfte som de inhämtats eller överförts till dem för. Om så inte var fallet måste de förstöras och raderas från akterna eller så måste, åtminstone, tillträdet till dem blockeras. Förstörandet måste föras in i protokoll och sådana fall som angavs i artiklarna 3.6 och 7.4 måste övervakas av en medarbetare med behörighet till domaryrket. I G10-lagen fastställdes vidare detaljerade bestämmelser för överföring, bevarande och användning av uppgifter som inhämtats genom avlyssning av externa kommunikationer.”

Domstolens betoning av tillgänglighetskraven i detta fall beror förmodligen på den breda, och verkligen ”praktiskt taget ohämmade” (punkt 64), prövningsrätt som det tillståndsgivande organet gavs i

[164] Punkt 63.

[165] Punkt 67. Jag anser personligen, vilket redan har nämnts, att denna kommissionär inte kan beskrivas som ”viktig” i fråga om ett robust och välfungerande skydd, även om denne kan beskrivas som ett ”skydd”.

brittisk lag.[166] I en bemärkelse var det brittiska systemet, som den svarande regeringen själv hävdade, förutsebart. All kommunikation mellan Storbritannien och utlandet kunde avlyssnas, och blev det också. Under dessa omständigheter, och eftersom det inte fanns något, åtminstone inget nödvändigt, samband mellan insamlingen av information och specifika straffbara gärningar, blev dock följden att domstolen ansåg att det var ännu viktigare att lagstiftningen gav allmänheten en försäkran om att de uppgifter som samlades in enbart skulle användas i begränsade syften och under strikt kontroll.

I Kennedy-målet ansågs däremot det ”vanliga” brittiska övervakningssystemet, till och med övervakning som genomförts av nationella säkerhetsskäl, ha ”stöd av lag”. Utöver (den förmodade) specificeringen av begreppet av IOC-kommissionären var det skäl som domstolen angav till detta att de *formella* krav som existerar för ett sådant bemyndigande innebär att intrånget är mycket mer begränsat och specificerat än vid strategisk övervakning som bemyndigas av nationella säkerhetsskäl.[167] *Kennedy*-målet är följaktligen ett belägg för att inte behöva ange innebörden av ”nationell säkerhet” i närmare detalj, förutsatt att det finns andra formella krav som i praktiken begränsar eller specificerar de enskilda övervakade personerna.

Slutligen vill jag i fråga om *Liberty*-målet notera att det brittiska systemet för strategisk övervakning har en minister som tillståndsgivande organ, som – naturligtvis – inte är oberoende av det verkställande organet. I målen *Iordachi* och *Association for European Integration and Human Rights och Ekimdzhiev* betonade domstolen att det bör ske oberoende kontroller på såväl bemyndigandestadiet som uppföljningsstadiet. När ett system inte omfattar oberoende kontroller på bemyndigandestadiet är det rimligt att anta att mycket starka skydd bör finnas på uppföljningsstadiet.[168]

---

[166] Jfr Lagerwall, s. 64.

[167] Kennedy mot Förenade kungariket, punkt 160 i anförda arbete: ”Lagstiftningen måste innehålla en beskrivning av de kategorier av personer som i praktiken riskerar att bli avlyssnade. I detta avseende observerar domstolen att det råder en överlappning mellan villkoret att kategorierna av personer ska anges och villkoret att brottens art ska definieras tydligt. De relevanta omständigheter som skulle kunna leda till avlyssning och som diskuteras i föregående punkt ger anvisningar om vilka kategorier av människor som, i praktiken, sannolikt riskerar att bli avlyssnade. Slutligen påpekar domstolen att själva bemyndigandet vid intern kommunikation måste innehålla ett tydligt angivande, antingen med namn eller med beskrivning, av en person som avlyssningssubjekt eller av en enda lokal som är föremål för ansökan om bemyndigande (se punkterna 40-41 ovan). Namn, adresser, telefonnummer och annan relevant information måste specificeras i det register som hör till bemyndigandet.”

[168] Oaktat påståendet i Liberty-målet att RIPA-kommissionären utgör ett ”viktigt skydd”, och oaktat domslutet i Kennedy-målet beträffande denna kommissionärs tillräcklighet i samband med ”vanlig” avlyssning av kommunikation anser jag att det är tveksamt om det brittiska

7 Slutkommentarer

Jag behöver inte upprepa de slutsatser som jag dragit tidigare. Det räcker att säga att domstolens rättspraxis tydligt indikerar att vissa metoder som i nuläget inte regleras uttryckligen genom lagstiftning måste bli uttryckligen reglerade. Det saknas otvetydigt stöd i Europadomstolens rättspraxis för krav på reglering av vissa andra metoder. Riktningen i domstolens rättspraxis – en bredare syn på vad som är privatliv – är dock tydlig. Att under dessa omständigheter välja att inte reglera metoder som anses ligga nära gränsen för privatlivet är en riskfylld strategi.

Referenser

Asp, P. och Cameron, I. (2010), Terrorism and Legal Security – a Swedish and European perspective. *De Lege Årsbook 2009*. Iustus.

Breyer, P. (2005), Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *11 European Law Journal*, s. 365–375.

Cameron, I. (2007), European Court of Human Rights – April 2006–March 2007. *13 European Public Law*, s. 533–568.

Cameron, I. (2000), *National Security and the European Convention on Human Rights*. Iustus och Kluwer.

Commission of Inquiry into certain activities of the Royal Canadian Mounted Police [undersökningskommissionen för viss verksamhet inom Kanadas ridande polis] (1981), *2nd Report, Freedom and Security under the Law ("McDonald Commission Report").*

Europarådet (2005), *Terrorism, Special Investigative Techniques*.

Harris, D. J. m.fl. (2009), Law of the European Convention on Human Rights. *Oxford University Press*.

systemet med ministeriellt tillstånd för *strategisk* övervakning, som enbart omfattar en begränsad kontrollmekanism i efterhand, uppfyller konventionens krav. Detta är emellertid, lyckligtvis, inte ett system som Sverige har valt att ta efter.

Helmius, I. (2000), *Polisens rättsliga befogenheter vid spaning*. Iustus.

Hert, de P. (1997), European Data Protection as a Potential Framework for Electronic Visual Surveillance. *Proceedings of the First World Conference on New Trends in Criminal Investigation and Evidence*, Nijboer, J.F. och Riejntes, J.M. (red.). Haag.

Ianni, F. och Reuss-Ianni, E. (1990), Network Analysis. *Criminal Intelligence Analyses,* Andrews, P. P. och Peterson, M. B. (red.). Loomis och Cal.

Joubert, C. och Bevers, H. (1996), *Schengen Investigated*. Kluwer.

Krüpe-Gescher, C. och Dorsch, C. (2005), *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation und Anderer Verdeckter Ermittlungsmassnahmen*. Max Planck-sällskapet för internationell straffrätt.
http://www.mpg.de/bilderBerichteDokumente/dokumentation/jahrbuch/2005/strafrecht/forschungsSchwerpunkt/pdf.pdf

Lagerwall, A. (2008), *Privacy and Secret Surveillance from a European Convention Perspective*. Stockholms universitet. Uppsats för juris kandidatexamen.

Loughlin, M. (2009), *The Rule of Law In European Jurisprudence*. Europeiska kommissionen för demokrati genom lag. Avhandling 512/2009 CDL-DEM(2009)006.

Lustgarten, L. och Leigh, I. (1994), In From the Cold: National Security and Parliamentary Democracy. *Oxford University Press*.

Marx, G. T. (1998), *Undercover*. Berkley/Los Angeles/London.

Moreham, N. A. (2008), A Right to respect for private life in the European Convention on Human Rights – a reexamination. *EHRLR*, s. 44–79.

Nagel, T. (1998), Concealment and Exposure, *27 Philosophy and Public Affairs*, s. 3–30.

Naismith, S. H. (1996), Photographs, Privacy and Freedom of Expression. *EHRLR*, s. 151–158.

Ovey, C. och White, R. A. (2006), Jacobs and White: European Convention on Human Rights. *Oxford University Press* (4:e upplagan).

Ruiz, B. R. (1997), *Privacy in Telecommunications: A European and an American Approach.* Haag.

Europeiska kommissionen för demokrati genom lag, *Report on the democratic oversight of the security services*. 71:a plenarsammanträdet. Venedig, 1–2 juni 2007. CDL AD(2007)016.

Valkaneer, C. de (2000), *La tromperie dans l'adminstration de la preuve.* Larcier.

van Dijk P. m.fl. (red.) (2006), Theory and Practice of the ECHR. *Intersentia* (4:e upplagan).

van Loenen, B. m.fl. (2007), *Privacy versus national security: The impact of privacy law on the use of location technology for national security purposes.*
http://www.springerlink.com/content/r124077351051308/fulltext.pdf

Statens offentliga utredningar 2010

Kronologisk förteckning

1. Lätt att göra rätt – om förmedling av brottsskadestånd. Ju.
2. Ett samlat insolvensförfarande – förslag till ny lag. Ju.
3. Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. M.
4. Allmänna handlingar i elektronisk form – offentlighet och integritet. Ju.
5. Skolgång för alla barn. U.
6. Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. M.
7. Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. IJ.
8. En myndighet för havs- och vattenmiljö. M.
9. Den framtida organisationen för vissa fiskefrågor. Jo.
10. Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
11. Spela samman – en ny modell för statens stöd till regional kulturverksamhet. Ku.
12. I samspel med musiklivet – en ny nationell plattform för musiken. Ku.
13 Upphandling på försvars- och säkerhetsområdet. Fi.
14. Partsinsyn enligt rättegångsbalken. Ju.
15. Kriminella grupperingar – motverka rekrytering och underlätta avhopp. Ju.
16. Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. IJ.
17. Prissatt vatten? M.
18. En reformerad budgetlag. Fi.
19. Lärling – en bro mellan skola och arbetsliv. U.
20. Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. Fi.
21. Bättre marknad för tjänstehundar. Jo.
22. Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. Fö.
23. Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. N.
24. Avtalad upphovsrätt. Ju.
25. Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. Fö.
26. Flyttningsbidrag och unionsrätten. A.
27. Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. N.
28. Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. U.
29. En ny förvaltningslag. Ju.
30. Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. N.
31. Första hjälpen i psykisk hälsa. S.
32. Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. UD.
33. Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
34. På väg mot en ny roll – överväganden och förslag om Riksutställningar. Ku.
35. Kunskap som befrielse? En metanalys av svensk forskning om jämställdhet och skola 1969–2009. U.
36. Svensk forskning om jämställdhet och skola. En bibliografi. U.
37. Sverige för nyanlända utanför flyktingmottagandet. IJ.
38. Mutbrott. Ju.
39. Ny ordning för nationella vaccinationsprogram. S.

40. Cirkulär migration och utveckling – kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. Ju.
41. Kompensationstillägg – om ersättning vid försenade utbetalningar. S.
42. Med fiskevård i fokus – en ny fiskevårdslag. Jo.
43. Förundersökningsbegränsning. Ju.
44. Mål och medel – särskilda åtgärder för vissa måltyper i domstol. Ju.
45. Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. S.
46. Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. N.
47. Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. S.
48. Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. S.
49. Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. Ju.
50. Försvarsmaktens helikopterresurser. Fö.
51. Könsskillnader i skolprestationer – idéer om orsaker. U.
52. Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. U.
53. Pojkar och skolan: Ett bakgrundsdokument om "pojkkrisen". Översättning på svenska av engelsk rapport: Boys and School: A Background Paper on the "Boy Crisis". + Engelsk rapport. U.
54. Förbättrad återbetalning av studieskulder. U.
55. Romers rätt – en strategi för romer i Sverige. IJ.
56. Innovationsupphandling. N.
57. Effektivare planering av vägar och järnvägar. N.
58. Rehabiliteringsrådets delbetänkande. S.
59. Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. Ju.
60. Ett utvidgat skydd mot åldersdiskriminering. IJ.
61. Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. N.
62. Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. Fi.
63. EU:s direktiv om sanktioner mot arbetsgivare. Ju.
64. "Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. U.
65. Kompetens och ansvar. S.
66. Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. U.
67. I rättan tid? Om ålder och skolstart. U.
68. Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. Ju.
69. Förbättrad vinterberedskap inom järnvägen. N.
70. Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. IJ.
71. Sexualbrottslagstiftningen – utvärdering och reformförslag. Ju.
72. Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. Fö.
73. Svensk sjöfarts konkurrensförutsättningar. N.
74. Mer innovation ur transportforskning. N.
75. Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. U.
76. Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. N.
77. Sammanläggningar av landsting – övergångsstyre och utjämning. Fi.
78. Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. Fi.
79. Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. U
80. Skolan och ungdomars psykosociala hälsa. U.
81. En ny biobankslag. S.
82. Trafikverket ICT. N.

83. Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. U.
84. Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. U.
85. Vem arbetar efter 65 års ålder? En statistisk analys. S.
86. Personalförsörjningen i ett reformerat försvar. Fö.
87. Skadestånd och Europakonventionen. Ju.
88. Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. Fi.
89. Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. S.
90. En ny lag om ekonomiska föreningar. Del 1+2. Ju.
91. Planering på djupet – fysisk planering av havet. M.
92. En effektivare förvaltning av statens fastigheter. Fi.
93. Att skapa arbeten. Löner, anställningsskydd och konkurrens. Fi.
94. Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. Fi.
95. Se, tolka och agera – allas rätt till en likvärdig utbildning. U.
96. Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. U.
97. Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. U.
98. Gårdsförsäljning. S.
99. Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan. U.
100. Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? N.
101. Handlingsplan för att utveckla strategier i miljömålssystemet. M.
102. Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. S.
103. Särskilda spaningsmetoder. Ju.

Statens offentliga utredningar 2010

Systematisk förteckning

Justitiedepartementet

Lätt att göra rätt
– om förmedling av brottsskadestånd. [1]
Ett samlat insolvensförfarande – förslag till ny lag. [2]
Allmänna handlingar i elektronisk form
– offentlighet och integritet. [4]
Partsinsyn enligt rättegångsbalken. [14]
Kriminella grupperingar – motverka rekrytering och underlätta avhopp. [15]
Avtalad upphovsrätt. [24]
En ny förvaltningslag. [29]
Mutbrott. (38)
Cirkulär migration och utveckling
– kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. [40]
Förundersökningsbegränsning. [43]
Mål och medel – särskilda åtgärder för vissa måltyper i domstol. [44]
Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. [49]
Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. [59]
EU:s direktiv om sanktioner mot arbetsgivare. [63]
Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. [68]
Sexualbrottslagstiftningen – utvärdering och reformförslag. [71]
Skadestånd och Europakonventionen. [87]
En ny lag om ekonomiska föreningar. Del 1+2. [90]
Särskilda spaningsmetoder. [103]

Utrikespartementet

Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. [32]

Försvarsdepartementet

Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. [22]
Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. [25]
Försvarsmaktens helikopterresurser. [50]
Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. [72]
Personalförsörjningen i ett reformerat försvar. [86]

Socialdepartementet

Första hjälpen i psykisk hälsa. [31]
Ny ordning för nationella vaccinationsprogram. [39]
Kompensationstillägg – om ersättning vid försenade utbetalningar. [41]
Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. [45]
Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. [47]
Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. [48]
Rehabiliteringsrådets delbetänkande. [58]
Kompetens och ansvar. [65]
En ny biobankslag. [81]
Vem arbetar efter 65 års ålder? En statistisk analys. [85]
Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. [89]
Gårdsförsäljning. [98]
Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. [102]

Finansdepartementet

Upphandling på försvars- och säkerhetsområdet. [13]

En reformerad budgetlag. [18]

Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. [20]

Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. [62]

Sammanläggningar av landsting – övergångsstyre och utjämning. [77]

Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. [78]

Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. [88]

En effektivare förvaltning av statens fastigheter. [92]

Att skapa arbeten. Löner, anställningsskydd och konkurrens. [93]

Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. [94]

Utbildningsdepartementet

Skolgång för alla barn. [5]

Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [10]

Lärling – en bro mellan skola och arbetsliv. [19]

Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. [28]

Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [33]

Kunskap som befrielse? En metaanalys av svensk forskning om jämställdhet och skola 1969–2009. [35]

Svensk forskning om jämställdhet och skola. En bibliografi. [36]

Könsskillnader i skolprestationer – idéer om orsaker. [51]

Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. [52]

Pojkar och skolan: Ett bakgrundsdokument om pojkkrisen. Översättning på svenska av engelsk rapport: Boys and School: A Backgroundpaper on the "Boy Crisis". + Engelsk rapport.[53]

Förbättrad återbetalning av studieskulder. [54]

"Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. [64]

Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. [66]

I rättan tid? Om ålder och skolstart. [67]

Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. [75]

Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. [79]

Skolan och ungdomars psykosociala hälsa. [80]

Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. [83]

Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. [84]

Se, tolka och agera – allas rätt till en likvärdig utbildning. [95]

Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. [96]

Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. [97]

Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan.[99]

Jordbruksdepartementet

Den framtida organisationen för vissa fiskefrågor. [9]

Bättre marknad för tjänstehundar. [21]

Med fiskevård i fokus – en ny fiskevårdslag. [42]

Miljödepartementet

Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. [3]

Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. [6]

En myndighet för havs- och vattenmiljö. [8]

Prissatt vatten? [17]

Planering på djupet – fysisk planering av havet. [91]
Handlingsplan för att utveckla strategier i miljömålssystemet. [101]

Näringsdepartementet

Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. [23]
Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. [27]
Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. [30]
Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. [46]
Innovationsupphandling. [56]
Effektivare planering av vägar och järnvägar. [57]
Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. [61]
Förbättrad vinterberedskap inom järnvägen. [69]
Svensk sjöfarts konkurrensförutsättningar [73]
Mer innovation ur transportforskning. [74]
Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. [76]
Trafikverket ICT. [82]
Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? [100]

Integrations- och jämställdhetsdepartementet

Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. [7]
Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. [16]
Sverige för nyanlända utanför flyktingmottandet. [37]
Romers rätt – en strategi för romer i Sverige. [55]
Ett utvidgat skydd mot åldersdiskriminering. [60]
Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. [70]

Kulturdepartementet

Spela samman – en ny modell för statens stöd till regional kulturverksamhet. [11]
I samspel med musiklivet – en ny nationell plattform för musiken. [12]
På väg mot en ny roll – överväganden och förslag om Riksutställningar. [34]

Arbetsmarknadsdepartementet

Flyttningsbidrag och unionsrätten. [26]