Till statsrådet och chefen för Justitiedepartementet

Genom beslut den 20 december 2007 bemyndigade regeringen chefen för Justitiedepartementet att tillkalla en särskild utredare med uppdrag att överväga vissa straffprocessuella och polisrättsliga frågor angående de brottsbekämpande myndigheternas dolda spanings- och utredningsverksamhet.

Särskild utredare är chefsrådmannen Stefan Reimer.

Experter är professorn Petter Asp (Uppsala universitet), kanslichefen Joel Brorsson (Säkerhets- och integritetsskyddsnämnden), sakkunnige Ingvar Carlsson (Tullverket), kriminalkommissarien Sven-Olov Gustafsson (Rikskriminalpolisen), ämnesrådet Lotta Hardvik Cederstierna (Justitiedepartementet), kanslirådet Irja Hed (Justitiedepartementet), chefsjuristen Lars-Åke Johansson (Säkerhetspolisen), vice chefsåklagaren Katarina Johansson Welin (Åklagarmyndigheten), ämnesrådet Per Lagerud (Justitiedepartementet), ordföranden i Sveriges Advokatsamfund Tomas Nilsson, verksjuristen Camilla Philipson Watz (Post- och telestyrelsen), chefsjuristen Monica Rodrigo (Ekobrottsmyndigheten) och polisöverintendenten Anders Thornberg (Säkerhetspolisen).

Per Lagerud (se ovan) och hovrättsassessorn Martin Persson är utredningens sekreterare.

Utredningen, som tagit namnet Polismetodutredningen (Ju 2008:01), överlämnar härmed delbetänkandet *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* (SOU 2009:1).

Utredningens arbete fortsätter med andra utestående frågor.

Stockholm i januari 2009

Stefan Reimer

/Per Lagerud
Martin Persson

Innehåll

Bilagor

Förkortningar

Bet.	Betänkande
BRU	Beredningen för rättsväsendets utveckling (Ju 2000:13)
Dir.	Kommittédirektiv
Ds	Betänkande i departementsserien
DVFS	Domstolsverkets författningssamling
JK	Justitiekanslern
JO	Riksdagens ombudsmän (Justitieombudsmannen) eller Justitieombudsmännens ämbetsberättelse
JuU	Justitieutskottet
LEK	Lagen (2003:389) om elektronisk kommunikation
Lirb	Lagen (2000:562) om internationell rättslig hjälp i brottmål
Prop.	Proposition
PTS	Post- och telestyrelsen
RB	Rättegångsbalken
SOU	Statens offentliga utredningar

Sammanfattning

Bakgrund

De brottsbekämpande myndigheterna (i detta sammanhang avses åklagare, polis och tull) har i dag möjlighet att få tillgång till uppgifter om elektronisk kommunikation enligt två regelverk, bestämmelserna om hemlig teleövervakning i rättegångsbalken (RB) och utlämnande av uppgifter enligt 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation (LEK) från dem som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst (leverantörer). Myndigheterna får i princip samma uppgifter oavsett vilka bestämmelser som tillämpas. Det rör sig främst om uppgifter som svarar på frågorna *vilka teleadresser* kommunicerade med varandra, *när* skedde det, *var* befann sig de som kommunicerade och *vilken typ* av kommunikation användes. Myndigheterna får inte tillgång till innehållet i en kommunikation, t.ex. telefonsamtalet, sms-meddelandet, telefaxmeddelandet eller e-postmeddelandet, utan enbart till vad som brukar kallas trafikuppgifter. För att få innehållet i meddelandet krävs beslut om det mer ingripande tvångsmedlet hemlig teleavlyssning. Tillstånd till hemlig teleövervakning ger tillgång till såväl historiska uppgifter som framtida uppgifter medan lagen om elektronisk kommunikation enbart omfattar historiska uppgifter, alltså sådana uppgifter som redan finns hos leverantören när beslutet verkställs.

Förutsättningarna för *hemlig teleövervakning* enligt 27 kap. 19–21 §§ RB är följande.

1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra
   a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),
   b) dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling, eller

c) försök, förberedelse eller stämpling till brott under a) och b).
3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden ska avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.

Förutsättningarna för att de brottsbekämpande myndigheterna ska få tillgång till uppgifter enligt *6 kap. 22 § första stycket 3 LEK* är följande (i jämförelse med rättegångsbalken).

1. Det ska vara fråga om misstanke om brott för vilket det inte är föreskrivet lindrigare straff än två års fängelse (även anstiftan och medhjälp omfattas men inte försöks-, förberedelse- och stämplingsbrott).
2. Det behöver inte finnas en skäligen misstänkt person.
3. Åtgärden behöver inte vara av synnerlig vikt för utredningen.
4. Åtgärden är inte begränsad till vissa teleadresser.
5. Åtgärden beslutas av den brottsbekämpande myndigheten.

För att de brottsbekämpande myndigheterna ska få uppgifter om abonnemang från leverantörerna, t.ex. namn, adress, hemliga telefonnummer och IP-nummer, fordras inte samma svårhetsgrad rörande den misstänkta brottsligheten. I sådana fall är det enligt 6 kap. 22 § första stycket 2 LEK tillräckligt att det för brottet är föreskrivet fängelse och att det i det enskilda fallet kan bli fråga om annan påföljd än böter.

Under år 2007 lämnades tillstånd till hemlig teleövervakning i 1 315 fall. I samtliga fall där hemlig teleavlyssning beviljades under året (966 fall) hade domstolen samtidigt gett tillstånd till hemlig teleövervakning. I 349 fall hade tillstånd meddelats till enbart hemlig teleövervakning.

Det saknas statistik över antalet fall där de brottsbekämpande myndigheterna begär ut uppgifter med stöd av lagen om elektronisk kommunikation. Polisen har gjort beräkningar över antalet fall där man har begärt att få ut uppgifter enligt 6 kap. 22 § första stycket 3 LEK under år 2007 och uppskattat det till ca 9 500. Den siffran omfattar inte Säkerhetspolisens och Tullverkets ärenden. Mot bakgrund av kravet i lagen om elektronisk kommunikation på att det ska vara fråga om misstanke om brott med ett straffminimum på två års fängelse, står det klart att utredningarna enbart rör allvarlig

brottslighet och att myndigheterna många gånger har begärt uppgifter vid flera tillfällen i samma utredning. En anledning till det relativt stora antalet beslut är att det inledningsvis i många förundersökningar rörande grova brott saknas en skäligen misstänkt person och därmed finns det inte heller möjlighet att använda sig av hemlig teleövervakning enligt rättegångsbalken. En hjälp i arbetet med att identifiera misstänkta personer är att inhämta uppgifter om elektronisk kommunikation på och i närheten av en brottsplats, längs flyktvägar och liknande. En annan anledning till det relativt stora antalet beslut är användningen vid brottslighet av mobiltelefoner med anonyma kontantkort, där myndigheterna många gånger behöver inhämta uppgifter flera gånger i syfte att identifiera den som använder ett visst abonnemang.

Uppdraget som redovisas i detta betänkande

Tidigare utredningar har kommit med förslag om att de brottsbekämpande myndigheternas delvis parallella möjligheter att inhämta uppgifter om elektronisk kommunikation genom rättegångsbalken respektive lagen om elektronisk kommunikation ska föras samman i ett regelverk. Förslagen har hittills inte lett till lagstiftning. Frågan om myndigheternas användning av lagen om elektronisk kommunikation i underrättelseverksamhet togs inte upp i de sammanhangen.

Regeringen konstaterar i direktiven till den här utredningen att det finns ett operativt behov av att få tillgång till uppgifter om elektronisk kommunikation för att kartlägga brottslig verksamhet och i övrigt arbeta brottsförebyggande. Regeringen anger att såväl tekniken kring elektronisk kommunikation som polisens och tullens underrättelseverksamhet har genomgått stora förändringar under senare år och att det mot den bakgrunden kan ifrågasättas om bestämmelsen i 6 kap. 22 § första stycket 3 LEK är ändamålsenligt utformad.

Regeringen konstaterar också i direktiven att det i underrättelseverksamheten kan finnas behov av att även få tillgång till uppgifter om abonnemang (6 kap. 22 § första stycket 2 LEK) och att utredningen i den delen ska utgå från att det ska vara möjligt för de brottsbekämpande myndigheterna att få tillgång till sådana uppgifter, inklusive uppgift om vem som har haft ett visst IP-nummer vid ett

visst tillfälle, även vid misstanke om brott som i det konkreta fallet bör föranleda ett bötesstraff.

Utredningens uppdrag är bl.a. mot den bakgrunden att överväga behovet av mer ändamålsenliga regler för inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpningen. Det rör sig då inte om uppgifter från trådlös kommunikation, som radio- och satellitkommunikation, eftersom etern under lång tid har ansetts vara fri.

En allmän utgångspunkt

Inhämtning och bearbetning av olika former av elektronisk kommunikation är ett allt viktigare verktyg för de brottsbekämpande myndigheterna såväl i underrättelseverksamhet som i det brottsutredande arbetet. Samtidigt har elektronisk kommunikation ett starkt skydd i både regeringsformen och Europakonventionen. Den omfattas av skyddet rörande privat- och familjeliv och korrespondens i artikel 8 i Europakonventionen och skyddet mot undersökning av förtroligt meddelande i 2 kap. 6 § regeringsformen.

En grundläggande utgångspunkt för förslagen är att de inte bara ska syfta till att upprätthålla en effektiv brottsbekämpande verksamhet utan även till att förstärka och bygga ut rättssäkerheten och integritetsskyddet vid inhämtning av uppgifter om elektronisk kommunikation.

Tydliga och rättssäkra befogenheter för utfående av uppgifter om elektronisk kommunikation

Bestämmelsen i 6 kap. 22 § första stycket 3 LEK bryter leverantörernas tystnadsplikt och ställer som enda krav för att uppgifterna ska få hämtas in, att misstanken rör brottslighet av viss svårhetsgrad. Det saknas i den lagen bestämmelser såsom vid hemlig teleövervakning om exempelvis formerna för tillståndsgivningen, krav på synnerlig vikt för utredningen, hur överskottsinformation får användas, underrättelseskyldighet till enskild och om särskild tillsyn av Säkerhets- och integritetsskyddsnämnden.

Regleringen i lagen om elektronisk kommunikation uppfyller inte i tillräcklig grad de krav på rättssäkerhet och integritetsskydd

som måste finnas vid det här slaget av integritetskänsliga åtgärder. Den ska därför upphävas.

I förundersökningar ska uppgifter om elektronisk kommunikation kunna inhämtas från leverantörerna enbart efter beslut om hemlig teleövervakning.

I underrättelseverksamhet ska befogenheter att inhämta uppgifter från leverantörerna tas in i en ny lag om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Hemlig teleövervakning i förundersökningar

När ska inhämtning få ske?

När bestämmelsen i 6 kap. 22 § första stycket 3 LEK upphävs blir det, för att kunna upprätthålla en effektiv brottsbekämpning, nödvändigt att möjliggöra att hemlig teleövervakning avseende uppgifter om telemeddelanden som har befordrats (historiska uppgifter) får användas även när det saknas en skäligen misstänkt person. Det ska krävas att åtgärden är av synnerlig vikt för utredningen och att syftet är att fastställa vem som skäligen kan misstänkas för brottet eller utröna annan omständighet av väsentlig betydelse för utredningen. Det sistnämnda kan vara att fastställa var en målsägande eller ett vittne har befunnit sig eller var en brottsplats är belägen.

Ett strängare krav än när det finns en skäligen misstänkt person ska gälla för att åtgärden ska få användas i ett sådant tidigt skede i en förundersökning. Misstanken ska röra brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff, eller annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år. Det är alltså fråga om samma brott som krävs för hemlig teleavlyssning.

Vem ska fatta beslut?

Tillstånd till hemlig teleövervakning i förundersökningar där det finns en skäligen misstänkt person ges av domstol.

Det är av stor vikt i det brottsbekämpande arbetet att det finns möjlighet att snabbt få tillgång till uppgifter om elektronisk kommunikation. Snabbheten i förfarandet är en avgörande framgångs-

faktor. Ofta är möjligheten till ”minutoperativa” beslut avgörande för att säkra ett lyckat utredningsresultat. Det gäller särskilt som de personer som sysslar med grov brottslighet många gånger aktivt vidtar åtgärder i syfte att försvåra och omöjliggöra ett framgångsrikt arbete från de brottsbekämpande myndigheternas sida.

Åklagare ska få ge interimistiskt tillstånd till hemlig teleövervakning, om det kan befaras att inhämtande av rättens tillstånd skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. Har åklagaren gett ett sådant interimistiskt tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har ett interimistiskt tillstånd till hemlig teleövervakning upphört att gälla innan rätten har prövat ärendet, ska åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Beslut om hemlig teleövervakning innan det finns en skäligen misstänkt person ska vid sidan av domstol få fattas även av undersökningsledare eller åklagare (utan att det är fråga om interimistiska tillstånd). Det är fråga om fall som i dag omfattas av lagen om elektronisk kommunikation. Om åtgärden kan antas bli av stor omfattning eller av särskilt ingripande slag, ska domstolen dock fatta besluten. Detta ska gälla bl.a. när inhämtningen avser långa tidsperioder, ett stort antal personer eller någon som arbetar med källskyddad information på ett medieföretag.

Tillgång till uppgifter om elektronisk kommunikation i underrättelseverksamhet

När ska inhämtning få ske?

Bestämmelsen i 6 kap. 22 § första stycket 3 LEK anger i dag att brottsligheten ska ha ett minimistraff på två års fängelse för att inhämtning ska får ske. Det bör även fortsättningsvis gälla i de brottsbekämpande myndigheternas underrättelseverksamhet. Samtidigt finns det brott som faller inom Säkerhetspolisens ansvarsområde och som inte har denna stränga straffskala men där tillgången till uppgifterna i undersökningarna har sådan betydelse att inhämtning ska få ske trots ett lägre straffminimum. Det rör bl.a. sabotage, kapning, olovlig kårverksamhet, brott mot medborgerlig fri-

het, spioneri, obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet och företagsspioneri.

För att inhämtning ska få ske bör det finnas ett krav på att uppgifterna kan antas ha en påtaglig betydelse för undersökningen. Det bör uttryckas så att uppgifter om viss elektronisk kommunikation ska få hämtas in i underrättelseverksamhet när det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Såsom vid andra tvångsmedel ska inhämtning få beslutas och genomföras endast om 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.

Vem ska fatta beslut?

Det finns tungt vägande principiella skäl mot att allmän domstol eller åklagare ges en roll som beslutsfattare i polisens och tullens underrättelseverksamhet. Beslutanderätten bör därför ligga på annat organ.

Beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 3 LEK i underrättelseverksamhet fattas av polis och tull. Den ordningen bör gälla även i fortsättningen. Däremot är det nödvändigt att det etableras en fastlagd ordning för vem som inom den brottsbekämpande myndigheten ska vara behörig att besluta om inhämtning av uppgifter. Beslutanderätten ska tillkomma myndigheten som sådan, dvs. myndighetschefen. Denne ska dock ha möjlighet att i viss utsträckning delegera beslutanderätten. Det ska få ske till annan person på ledningsnivå.

I vilken omfattning ska uppgifterna få användas?

Uppgifter om elektronisk kommunikation som hämtas in i underrättelseverksamhet ska få användas för att förhindra brott.

Sådana uppgifter ska också få användas i förundersökningar om det är fråga om brott av så kvalificerat slag att det skulle ge myndigheterna möjlighet att använda hemlig teleövervakning för att inhämta uppgifterna. Det ska krävas att tillstånd till hemlig teleövervakning ges för att sådana uppgifter ska få användas i en förundersökning.

Tillgång till lokaliseringsuppgifter

Hemlig teleövervakning och inhämtning av uppgifter enligt 6 kap. 22 § första stycket 3 LEK kan för närvarande ge de brottsbekämpande myndigheterna tillgång till lokaliseringsuppgifter rörande en kommunikation, alltså uppgift om från vilket geografiskt område t.ex. ett mobilsamtal skedde. Genom bestämmelsen i lagen om elektronisk kommunikation har det också ansetts möjligt för myndigheterna att begära s.k. basstationstömning, en åtgärd som ger uppgift om samtliga de mobiltelefoner som var uppkopplade för kommunikation under en viss tid i ett avgränsat geografiskt område. De sistnämnda uppgifterna ska myndigheterna få tillgång till även i fortsättningen under samma förutsättningar som gäller för hemlig teleövervakning. Sådana uppgifter ska också få hämtas in i underrättelseverksamheten. De brottsbekämpande myndigheterna ska också kunna få tillgång till lokaliseringsuppgifter rörande mobiltelefoner som inte är uppkopplade för kommunikation utan enbart påslagna.

Inhämtning av uppgifter om abonnemang

Såväl i förundersökningar som i de brottsbekämpande myndigheternas underrättelseverksamhet ska myndigheterna även i fortsättningen ha rätt att inhämta uppgifter om abonnemang med stöd av bestämmelsen i 6 kap. 22 § första stycket 2 LEK. Skyldigheten för leverantörerna att lämna ut uppgifter om abonnemang till myndigheterna ska i motsats till vad som nu gäller inte vara begränsad till misstanke om brott av viss svårhetsgrad. Det betyder att t.ex. uppgift om vem som hade ett visst IP-nummer vid ett visst tillfälle ska kunna lämnas ut vid misstanke om brott, även om det kan förväntas enbart böter som påföljd i det enskilda fallet.

Överprövning

En domstols beslut om hemlig teleövervakning kan överklagas. När undersökningsledaren eller åklagaren har fattat beslut om en sådan åtgärd ska den som innehar den teleadress som övervakningen avser kunna begära rättens prövning av beslutet. Däremot ska beslut av den brottsbekämpande myndigheten om inhämtning av uppgifter i underrättelseverksamhet inte på motsvarande sätt kunna bli före-

mål för rättens prövning. I stället bör det för de fallen finnas andra rättssäkerhetsgarantier, bl.a. i form av en kontinuerlig och effektiv tillsyn av Säkerhets- och integritetsskyddsnämnden.

Underrättelse till enskild

Sedan den 1 januari 2008 gäller att den som är eller har varit brottsmisstänkt eller den som innehar en teleadress som hemlig teleövervakning har avsett som huvudregel ska underrättas i efterhand om tvångsmedlet. Det ska gälla även för de nya fallen av hemlig teleövervakning, dvs. när syftet med åtgärden är att fastställa vem som skäligen kan misstänkas för brottet m.m. Förundersökningsledaren ska ansvara för att underrättelse sker.

Vissa undantag från underrättelseskyldigheten ska införas. När det har skett en basstationstömning ska underrättelse inte behöva lämnas till de personer som kommunicerade med exempelvis en mobiltelefon på den plats åtgärden avsåg. Inte heller ska den åtgärd som sker omedelbart därefter, när de brottsbekämpande myndigheterna kontrollerar samtliga de abonnentnummer som framkom genom basstationstömningen, behöva föranleda underrättelse i efterhand. Undantag ska också finnas för det fallet att det t.ex. är fråga om mobiltelefoner med anonyma kontantkort där det inte fastställs vem som innehar teleadressen.

Det ska inte finnas någon underrättelseskyldighet till enskilda som berörts av åtgärden att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet. Även här blir bl.a. den särskilda tillsyn som Säkerhets- och integritetsskyddsnämnden ska genomföra av stor vikt som en rättssäkerhetsgaranti.

Särskild tillsyn av Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden har redan i dag tillsyn över användningen av hemlig teleövervakning.

Säkerhets- och integritetsskyddsnämnden ska utöva löpande tillsyn även över användningen av de nya befogenheterna att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet. För att uppväga att de brottsbekämpande myndigheterna själva ska få fatta beslut om inhämtning ska nämndens kapaci-

tet förstärkas med ett eller flera granskningsombud som hos myndigheterna kontrollerar hur befogenheterna har beslutats och använts.

Granskningsombud ska utses av Säkerhets- och integritetsskyddsnämnden för en bestämd tid, högst fyra år. Ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Ett granskningsombud får inte vara ledamot av nämnden.

Säkerhets- och integritetsskyddsnämnden ska även vara skyldig att på begäran av en enskild person kontrollera om han eller hon har utsatts för inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet och om användningen av tvångsmedel och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning.

Regeringens redovisning till riksdagen

Regeringen redovisar i en årlig skrivelse till riksdagen användningen av hemlig teleövervakning i brottsbekämpningen.

Skrivelsen bör också redovisa inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. På motsvarande sätt som i dag bör uppgifter som rör Säkerhetspolisens användning av tvångsmedel inte redovisas.

Sekretess och tystnadsplikt

I sekretesslagen ska det införas undantag från meddelarfriheten såvitt avser uppgifter om användning av befogenheten att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet.

I lagen om elektronisk kommunikation ska det införas en tystnadsplikt för leverantörer såvitt avser uppgifter som hänför sig till användning av befogenheten att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet. En tystnadsplikt ska även införas i den lagen med avseende på åtgärd att begära in uppgift om abonnemang.

Ikraftträdande

Förslagen ska träda i kraft den 1 januari 2010.

1 Författningsförslag

1.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken (1942:740)
dels att 27 kap. 19–21, 23 och 33 §§ ska ha följande lydelse,
dels att det i balken ska införas tre nya paragrafer, 27 kap. 20 d, 21 a och 21 b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	27 kap.
	19 §[1]
Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram.	Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram. *Vad som sägs om hemlig teleövervakning ska även gälla inhämtning i hemlighet av lokaliseringsuppgifter. Med sådana uppgifter avses* *1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, eller* *2. uppgifter om i vilket*

[1] Senaste lydelse 2003:1146.

avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.

Hemlig teleövervakning får användas vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader,

2. brott enligt 4 kap. 9 c § brottsbalken, brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, brott enligt 1 § narkotikastrafflagen (1968:64), brott enligt 6 § första stycket lagen (2000:1225) om straff för smuggling, eller

3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om sådan gärning är belagd med straff.

I fall som avses i 20 d § får hemlig teleövervakning dock användas endast vid förundersökning angående brott som kan föranleda hemlig teleavlyssning enligt 18 § andra stycket.

20 §[2]

Hemlig teleavlyssning och hemlig teleövervakning får ske endast om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

Hemlig teleavlyssning och hemlig teleövervakning får, *om inte annat följer av 20 d §*, endast ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

1. en teleadress 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, eller

2. en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.

Avlyssning eller övervakning får inte avse telemeddelanden som endast befordras eller har befordrats inom ett telenät som med hänsyn till sin begränsade omfattning och omständigheterna i

[2] Senaste lydelse 2003:1146.

övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt.

20 d §

Utöver vad som anges i 20 § får hemlig teleövervakning avseende uppgifter om telemeddelanden som har befordrats eller inhämtning av lokaliseringsuppgifter ske, om åtgärden är av synnerlig vikt för utredningen och syftet är att fastställa vem som skäligen kan misstänkas för brottet eller utröna annan omständighet av väsentlig betydelse för utredningen.

21 §[3]

Frågor om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning prövas av rätten på ansökan av åklagaren.

Frågor om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning prövas av rätten på ansökan av åklagaren. *Om hemlig teleövervakning inte kan antas bli av stor omfattning eller av särskilt ingripande slag, får frågor enligt 20 d § även prövas av undersökningsledaren eller åklagaren.*

I ett beslut att tillåta åtgärder enligt första stycket ska det anges vilken tid tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

I ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning ska det anges vilken teleadress som tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga telenät.

I ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning ska det anges vilken teleadress som tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga telenät. *I ett*

[3] Senaste lydelse 2008:855.

beslut att tillåta inhämtning av lokaliseringsuppgifter ska det anges vilken teleadress eller vilket avgränsat geografiskt område tillståndet avser.

I ett tillstånd till hemlig kameraövervakning ska det anges vilken plats tillståndet gäller.

21 a §

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

Har åklagaren gett ett sådant interimistiskt tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har ett interimistiskt beslut om övervakning upphört att gälla innan rätten har prövat ärendet ska åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

21 b §

Har hemlig teleövervakning avseende en viss teleadress beslutats utan rättens prövning enligt 21 § får den som innehar teleadressen begära rättens prövning av beslutet. Rätten ska skyndsamt

	pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har beslutet om övervakning upphört att gälla innan rätten har prövat ärendet ska undersökningsledaren eller åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.
23 §[4]	
Om det inte längre finns skäl för ett beslut om hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning, ska åklagaren eller rätten omedelbart häva beslutet.	Om det inte längre finns skäl för ett beslut om hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning, ska *undersökningsledaren*, åklagaren eller rätten omedelbart häva beslutet.

33 §[5]

Om det gäller sekretess enligt 2 kap. 1 eller 2 §, 5 kap. 1 § eller 9 kap. 17 § sekretesslagen (1980:100) för uppgifter som avses i 32 §, ska en underrättelse enligt 31 § skjutas upp till dess att sekretess inte längre gäller.

Har det på grund av sekretess enligt första stycket inte kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, får underrättelsen underlåtas.

En underrättelse enligt 31 § ska inte lämnas, om förundersökningen angår

1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
2. brott som avses i 13 kap. 4 eller 5 § brottsbalken,
3. brott som avses i 18 kap. 1, 3, 4, 5 eller 6 § eller 19 kap. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 eller 13 § brottsbalken,
4. brott som avses i 3 eller 4 kap. brottsbalken, om brottet är av det slag som anges i 18 kap. 2 § eller 19 kap. 11 § samma balk,
5. brott som avses i 2 § lagen (2003:148) om straff för terroristbrott eller 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., eller

[4] Senaste lydelse 2008:855.
[5] Senaste lydelse 2007:981.

6. försök, förberedelse eller stämpling till brott som anges i 1–5 eller underlåtenhet att avslöja sådant brott, om gärningen är belagd med straff.

En underrättelse enligt 31 § ska inte heller lämnas när

1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område har inhämtats,

2. integritetsintrånget för den enskilde annars kan antas vara ringa, eller

3. uppgift om vem som innehar teleadressen inte fastställs.

Denna lag träder i kraft den 1 januari 2010.

1.2 Förslag till lag (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs följande.

1 § Denna lag innehåller bestämmelser om brottsbekämpande myndigheters rätt att i underrättelseverksamhet i hemlighet hämta in uppgifter om viss elektronisk kommunikation från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Om det i annan lag finns bestämmelser som avviker från denna lag ska de bestämmelserna gälla.

2 § Inhämtning får avse

1. uppgifter om telemeddelanden som har befordrats till eller från en viss teleadress,
2. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, eller
3. uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.

3 § Inhämtning av uppgifter får ske i en undersökning om det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 4, 5 a första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. olovlig kårverksamhet eller brott mot medborgerlig frihet enligt 18 kap. 4 eller 5 § brottsbalken,
4. spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet enligt 19 kap. 5, 7, 8 eller 10 § brottsbalken,

5. företagsspioneri enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning, eller

6. brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

4 § Inhämtning av uppgifter beslutas av chefen för den brottsbekämpande myndigheten. Myndighetschefen får delegera beslutanderätten.

5 § I ett beslut om inhämtning av uppgifter ska det anges vilken tid och, i förekommande fall, vilken teleadress och vilket avgränsat geografiskt område tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

Inhämtning av uppgifter får beslutas och genomföras endast om 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.

6 § Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter ska beslutet omedelbart hävas.

7 § Om det genom inhämtningen av uppgifter har kommit fram information om förestående brott, får uppgifterna användas för att förhindra brott.

Om det genom inhämtningen av uppgifter har kommit fram information som är av betydelse för utredningen av ett brott, får uppgifterna användas i utredningen endast om beslut om hemlig teleövervakning har fattats.

8 § Uppteckningar av uppgifter ska granskas snarast möjligt.

Uppteckningar ska, i de delar de är av betydelse för att förebygga eller förhindra brott, bevaras så länge det behövs för att förebygga eller förhindra brott. De ska därefter förstöras.

Trots vad som sägs i andra stycket får brottsbekämpande myndigheter behandla uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag.

9 § I lagen (2007:908) om tillsyn över viss brottsbekämpande verksamhet finns bestämmelser om Säkerhets- och integritetsskyddsnämndens tillsyn på eget initiativ och på begäran av enskild.

Denna lag träder i kraft den 1 januari 2010.

1.3 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 16 kap. 1 § sekretesslagen (1980:100) ska ha följande lydelse.

Nuvarande lydelse

16 kap.

1 §[6]

Att friheten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter i vissa fall är begränsad framgår av 7 kap. 3 § första stycket 1 och 2, 4 § 1–8 samt 5 § 1 och 3 tryckfrihetsförordningen och av 5 kap. 1 § första stycket samt 3 § första stycket 1 och 2 yttrandefrihetsgrundlagen. De fall av uppsåtligt åsidosättande av tystnadsplikt, i vilka nämnda frihet enligt 7 kap. 3 § första stycket 3 och 5 § 2 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 3 yttrandefrihetsgrundlagen i övrigt är begränsad, är de där tystnadsplikten följer av

3. denna lag enligt	
5 kap. 1 §	såvitt avser 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
9. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation	
6 kap. 21 § lagen (2003:389) om elektronisk kommunikation	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag eller om hemlig teleavlyssning och hemlig tele-

[6] Senaste lydelse 2008:815.

	övervakning på grund av beslut av domstol, undersökningsledare eller åklagare

Föreslagen lydelse

16 kap.

1 §

Att friheten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter i vissa fall är begränsad framgår av 7 kap. 3 § första stycket 1 och 2, 4 § 1–8 samt 5 § 1 och 3 tryckfrihetsförordningen och av 5 kap. 1 § första stycket samt 3 § första stycket 1 och 2 yttrandefrihetsgrundlagen. De fall av uppsåtligt åsidosättande av tystnadsplikt, i vilka nämnda frihet enligt 7 kap. 3 § första stycket 3 och 5 § 2 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 3 yttrandefrihetsgrundlagen i övrigt är begränsad, är de där tystnadsplikten följer av

3. denna lag enligt	
5 kap. 1 §	såvitt avser 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, *eller inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*
9. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation	
6 kap. 21 § lagen (2003:389) om elektronisk kommunikation	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag eller om hem-

lig teleavlyssning och hemlig teleövervakning på grund av beslut av domstol, undersökningsledare eller åklagare, *eller inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*

Denna lag träder i kraft den 1 januari 2010.

1.4 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation,

dels att 6 kap. 8, 21 och 22 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 6 kap. 10 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
8 §[7]	
Bestämmelserna i 5–7 §§ gäller inte	
1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 5 § för att lösa tvister,	
2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning, eller	2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning, *inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*, eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	

[7] Senaste lydelse 2005:493.

10 a §

Bestämmelserna i 9 och 10 §§ gäller inte när lokaliseringsuppgifter omfattas av beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

21 §[8]

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 *eller* 19 § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål, *och*

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18, 19 *eller 20 d* § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, och

[8] Senaste lydelse 2008:719.

5. begäran om utlämnande enligt 22 § första stycket 2.

22 §[9]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket *skall* på begäran lämna

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket *ska* på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (1970:428), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som *skall* ingripa mot brottet, *om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,*

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som *ska* ingripa mot brottet,

3. uppgift som avses i 20 § första stycket 3 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv

3. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv

[9] Senaste lydelse 2006:737.

verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),

6. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten *skall* kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

7. uppgift som avses i 20 § första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten *skall* kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

Ersättning för att lämna ut

verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

4. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),

5. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten *ska* kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

6. uppgift som avses i 20 § första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten *ska* kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

7. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

Ersättning för att lämna ut

uppgifter enligt första stycket *8 skall* vara skälig med hänsyn till kostnaderna för utlämnandet.	uppgifter enligt första stycket *7 ska* vara skälig med hänsyn till kostnaderna för utlämnandet.

Denna lag träder i kraft den 1 januari 2010.

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

Härigenom föreskrivs i fråga om lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

dels att 2 § ska ha följande lydelse,

dels att nuvarande 6 § ska betecknas 7 §,

dels att det ska införas en ny paragraf, 6 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
Nämnden *skall* utöva sin tillsyn genom inspektioner och andra undersökningar.	Nämnden *ska* utöva sin tillsyn genom inspektioner och andra undersökningar.
	Nämnden ska biträdas av granskningsombud med uppgift att löpande följa tillämpningen av lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Ombud ska till nämnden anmäla förhållanden av betydelse för nämndens tillsyn.
Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och *skall* verka för att brister i lag eller annan författning avhjälps.	Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och *ska* verka för att brister i lag eller annan författning avhjälps.
	4 §
Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Även domstolar samt de förvaltningsmyndigheter som inte omfattas av till-	Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Även domstolar samt de förvaltningsmyndigheter som inte omfattas av till-

synen är skyldiga att lämna nämnden de uppgifter som den begär.	synen är skyldiga att lämna nämnden de uppgifter som den begär. *Granskningsombud har inom ramen för sitt uppdrag motsvarande rätt till uppgifter och biträde.*
	6 §
	Nämnden utser ett eller flera granskningsombud för en tid av högst fyra år. Ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet samt får inte vara ledamot av nämnden.

Denna lag träder i kraft den 1 januari 2010.

1.6 Förslag till förordning om ändring i förundersökningskungörelsen (1947:948)

Härigenom föreskrivs att 14 b § förundersökningskungörelsen (1947:948) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	14 b §[10]
Underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken, 8 § lagen (1995:1506) om hemlig kameraövervakning eller 15 § lagen (2007:978) om hemlig rumsavlyssning, ska fullgöras av den *åklagare* som är eller har varit förundersökningsledare.	Underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken, 8 § lagen (1995:1506) om hemlig kameraövervakning eller 15 § lagen (2007:978) om hemlig rumsavlyssning, ska fullgöras av den som är eller har varit förundersökningsledare.
När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket rättegångsbalken, 8 § lagen om hemlig kameraövervakning eller 15 § lagen om hemlig rumsavlyssning, ska den *åklagare* som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.	När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket rättegångsbalken, 8 § lagen om hemlig kameraövervakning eller 15 § lagen om hemlig rumsavlyssning, ska den som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.
Om den *åklagare* som avses i denna paragraf inte kan fullgöra underrättelseskyldigheten enligt första och andra styckena ska denna i stället fullgöras av en annan åklagare.	Om den *förundersökningsledare* som avses i denna paragraf inte kan fullgöra underrättelseskyldigheten enligt första och andra styckena ska denna i stället fullgöras av annan åklagare, *polisman eller tjänsteman vid Tullverket.*

Denna förordning träder i kraft den 1 januari 2010.

[10] Senaste lydelse 2007:1142.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Utredningens uppdrag enligt huvuddirektiven (Dir. 2007:185, se bilaga 1) innebär att utredningen ska överväga vissa straffprocessuella och polisrättsliga frågor angående de brottsbekämpande myndigheternas dolda spanings- och utredningsverksamhet. I uppdraget ingår bl.a. att

1. 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,
2. 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,
3. 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,
4. 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,
5. överväga en ändamålsenlig författningsreglering av sådan användning av tekniska spaningsmetoder som utgör ett intrång i enskildas integritet eller av andra skäl bör lagregleras,

6. 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 person, och att
7. utifrån övervägandena lägga fram de förslag till lagändringar som utredningen finner lämpliga.

2.2 Vad behandlas i detta betänkande?

Enligt huvuddirektiven (Dir. 2007:185) ska utredningen i ett delbetänkande senast den 19 juni 2008 redovisa resultatet av övervägandena i vissa frågor om tekniska metoder för att hämta in uppgifter i polisens och tullens brottsbekämpande verksamhet. I den delen har utredningen i uppdrag att

1. 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, och att
2. 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, 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 person.

I tilläggsdirektiv (Dir. 2008:91, se bilaga 2) har regeringen bestämt att den del av uppdraget som framgår av punkten 1 ovan, dvs. frågor som rör de brottsbekämpande myndigheternas inhämtning av uppgifter om elektronisk kommunikation med egna tekniska hjälpmedel, ska redovisas i utredningens slutbetänkande och att det ska ske senast den 1 oktober 2009.

Frågan om de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation hänger samman med

frågan om skyldigheten för leverantörer att lagra uppgifterna för brottsbekämpande ändamål under viss tid. Trafikuppgiftsutredningen (Ju 2006:04) har i betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76) föreslagit hur EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter ska genomföras i svensk rätt. Förslaget innebär bl.a. att leverantörerna ska vara skyldiga att lagra uppgifterna under ett års tid. Vissa delar av EG-direktivet ska vara genomförda i svensk rätt senast den 15 september 2007 och övriga delar senast den 15 mars 2009. Det är också bakgrunden till att regeringen har satt en kort tid för utredningens arbete med frågorna i detta betänkande. Regeringen har dock i tilläggsdirektiven förlängt den ursprungliga tiden för den redovisningen till den 31 december 2008.

2.3 Utredningens arbete

Utredningen har haft sammanträden och mer informella kontakter med experterna. I den kretsen finns företrädare för Justitiedepartementet, Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, Rikskriminalpolisen, Säkerhets- och integritetsskyddsnämnden, Tullverket, Post- och telestyrelsen, Uppsala universitet och Sveriges Advokatsamfund. Utredningen har också haft särskilda samråd med Säkerhetspolisen och Rikskriminalpolisen.

2.4 Betänkandets disposition

I ett inledande avsnitt om den rättsliga bakgrunden m.m. redovisas bl.a. bestämmelserna i rättegångsbalken och lagen om elektronisk kommunikation, som reglerar de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation m.m. (avsnitt 3). Utredningen redogör därefter i avsnitt 4 och 5 för myndigheternas tillgång till uppgifterna i dag och för tidigare utredningsförslag. Utredningens överväganden, bl.a. rörande de effektivitets-, rättssäkerhets- och integritetsfrågor som aktualiseras, och förslagen i frågan om en mer rättssäker inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpningen finns i avsnitt 6. Konsekvenser och genomförandefrågor behandlas i avsnitt 7.

3 Den rättsliga bakgrunden m.m.

3.1 Allmänt om de brottsbekämpande myndigheternas uppgifter

Till polisens uppgifter hör att förebygga brott och att bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Åklagare ansvarar för ledningen av alla kvalificerade brottutredningar där det finns en skäligen misstänkt person. Åklagare har också till uppgift att besluta i åtalsfrågor och att föra det allmännas talan i brottmålsprocessen.

Förfarandet vid den utredning som föregår ett beslut om åtal, förundersökningen, är reglerat i bl.a. rättegångsbalken och förundersökningskungörelsen (1947:948). Enligt 23 kap. 1 och 3 §§ RB ska polismyndighet eller åklagare fatta beslut om förundersökning så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Om förundersökning har inletts av polismyndighet och saken inte är av enkel beskaffenhet, ska ledningen av förundersökningen övertas av åklagare så snart någon skäligen kan misstänkas för brottet. Åklagare ska också i annat fall överta ledningen när det är nödvändigt av särskilda skäl. Motsvarande ordning finns på bl.a. Tullverkets område enligt 19 § lagen (2000:1225) om straff för smuggling.

Förundersökningen har flera syften. Ett syfte är att utröna om brott föreligger, vem som skäligen kan misstänkas för brottet och att skaffa tillräckligt material för bedömning av frågan om åtal ska väckas. Ett annat syfte är att bereda målet så att bevisningen kan läggas fram i ett sammanhang vid huvudförhandlingen. Ett tredje syfte är att ge den misstänkte vetskap om utredningsmaterialet och möjliggöra för honom eller henne att få detta justerat och berikat. Ytterligare ett syfte är att utreda om det finns något enskilt anspråk och vilka omständigheter det i så fall grundas på.

3.2 Underrättelseverksamhet

3.2.1 Allmänt

Polisen, Säkerhetspolisen, Ekobrottsmyndigheten, Kustbevakningen, Tullverket och Skatteverket bedriver även underrättelseverksamhet. Denna verksamhet är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås.

Ett övergripande mål med underrättelseverksamheten är att förse de brottsbekämpande myndigheterna med kunskap som kan omsättas i operativ verksamhet. T.ex. ska polisens kriminalunderrättelsetjänst vara delaktig i strategisk och operativ verksamhetsplanering och utgöra ett direkt stöd för operativ polisverksamhet, ge underlag till ledningsverksamheten på olika nivåer inom polisen samt medverka när effekterna av genomförda insatser analyseras.

I underrättelseverksamheten samlar myndigheterna in, bearbetar eller analyserar uppgifter som senare kan ha betydelse för att utreda, förebygga och förhindra brott.

Det första ledet i underrättelseprocessen där information förädlas till underrättelser är planeringsfasen. I planeringsfasen tas ställning t.ex. till vilka områden som är prioriterade för underrättelseverksamheten och vilka uppgifter som ska inhämtas.

Inhämtningen kan ske från olika källor. Det kan t.ex. ske genom rutinmässig rapportering, spaning eller användning av överskottsinformation från hemliga tvångsmedel men även genom nationell och internationell samverkan samt information från tipsare och informatörer. En annan källa för inhämtning är information som publicerats i tidningar eller på Internet.

När informationen inhämtats sker en bearbetning genom att informationen struktureras, systematiseras och värderas, t.ex. genom jämförelser med sedan tidigare tillgängliga uppgifter. Därefter vidtar den avgörande fasen i underrättelseprocessen – analysen. Genom analysen tydliggörs sammanhang och den bearbetade informationen tillförs mervärden. Det kan handla om t.ex. hot- och riskanalys, analys av brottsmönster samt kartläggning av mer eller mindre löst sammansatta kriminella nätverk och grupperingar.

Efter inhämtning, bearbetning och analys delges informationen lämpliga mottagare. Det framtagna underrättelsematerialet kan läggas till grund för t.ex. beslut om att inleda förundersökning eller beslut om att vidta särskilda åtgärder för att förebygga, förhindra

eller upptäcka brott. Det kan alltså handla om allt från en redovisning till berörda chefer till att gå ut i media för att förebygga ett visst brottsligt tillvägagångssätt. En annan form av förebyggande verksamhet är att de berörda personerna kontaktas och därigenom blir medvetna om den brottsbekämpande myndighetens intresse, vilket många gånger leder till att den brottsliga verksamhet som var i görningen aldrig kommer till stånd.

Genom att slutligen utvärdera resultatet av vidtagna åtgärder och underrättelsernas betydelse i sammanhanget kan verksamheten tillföras ny kunskap för det fortsatta arbetet.

Utredningen redovisar i det följande något om den underrättelseverksamhet som bedrivs vid polisen, Säkerhetspolisen, Ekobrottsmyndigheten och Tullverket och kommer därefter in på de regelverk som finns för verksamheterna.

3.2.2 Polisens underrättelseverksamhet

Polisens arbete ska bedrivas enligt vad som kallas polisens underrättelsemodell. Det är en modell för ledning och styrning av planlagd operativ polisverksamhet där beslut om inriktning, prioritering och genomförande av polisiär verksamhet baseras på underrättelser och annan relevant kunskap. Underrättelseverksamhet har därför en central roll i modellen.

Kriminalunderrättelsetjänstens övergripande uppdrag är att förse polisen med kunskap som kan omsättas i operativ verksamhet eller strategiska beslut. Enligt polisens underrättelsemodell ska kriminalunderrättelsetjänstens verksamhet bedrivas på lokal, regional och nationell nivå med gemensam inriktning.

Den lokala kriminalunderrättelsetjänsten utgör grunden i underrättelseverksamheten. Den arbetar dels med de problem som är viktiga för den egna polismyndigheten, dels medverkar den i underrättelseverksamhet som har regional, nationell och internationell bäring.

På regional nivå finns sju samverkansområden. Kriminalunderrättelsetjänstens organisation på den regionala nivån bestäms av hur samverkansavtalen ser ut mellan polismyndigheterna. Den regionala kriminalunderrättelsetjänsten ska vara samverkans- och samordningsfunktion för den lokala kriminalunderrättelsetjänsten. Den ska svara för samverkansområdets gemensamma verksamhet med inriktning mot strategiska frågor samt länsöverskridande och

myndighetsgemensam brottslighet. Vidare ska regional kriminalunderrättelsetjänst utgöra en länk till Rikskriminalpolisens kriminalunderrättelsetjänst i den operativa och strategiska verksamheten samt rörande utbildning och metodutveckling.

Vid tre polismyndigheter finns även regionala underrättelsecentrum vari ingår, förutom polismyndigheter, t.ex. Ekobrottsmyndigheten, Skatteverket, Tullverket och Kronofogdemyndigheten. Antalet underrättelsecentrum kommer att utökas med ytterligare fem.

Den nationella kriminalunderrättelseverksamheten bedrivs vid Rikskriminalpolisen och är huvudsakligen inriktad mot grova brott och grov organiserad brottslighet på nationell och internationell nivå. Rikskriminalpolisen ska inom vissa prioriterade områden bedriva långsiktiga operativa underrättelseprojekt samt strategiska projekt. Eftersom projekten även drivs internationellt krävs nationell samordning. Det är Rikskriminalpolisen som svarar för samordningen av polisens underrättelseverksamhet och har mandat att besluta om inriktningen för denna verksamhet i hela landet.

Vid Rikskriminalpolisens underrättelsesektion har Tullverket, Skatteverket, Kriminalvården och Kustbevakningen placerat sambandsmän. Avsikten är att underrättelseinformation om den grova organiserade brottsligheten ska samordnas på en nationell och myndighetsöverskridande nivå. Underrättelsesektionen vid Rikskriminalpolisen utgör således ett nationellt underrättelsecentrum.

Rikskriminalpolisen tar emot, grundbearbetar och registrerar en stor mängd inkommande underrättelseuppslag i kriminalunderrättelseregister. Informationen kommer framför allt från polismyndigheter, där registrering i kriminalunderrättelseregister görs, och andra brottsbekämpande myndigheter i Sverige, från de i andra länder utstationerade sambandsmännen samt från Europol och Interpol. Efter registreringen skickas grundhandlingen med information vidare för ytterligare åtgärder.

Arbetet i underrättelseverksamheten bedrivs i underrättelseprocessen där information ”förädlas” till underrättelser. Den insamlade informationen bedöms för registrering i kriminalunderrättelseregistret. Efter beslut kan informationen registreras även i särskilda undersökningsregister. Genom analys länkas uppgifter samman och sammanhang, nätverk och skeenden värderas. Resultatet blir ett underlag för strategiska och operativa beslut i polisverksamheten som sedan delges berörd beslutsfattare. Genom att utvärdera resultatet av vidtagna operativa åtgärder och underrättelsernas

betydelse för dessa tillförs verksamheten ny kunskap som kan användas i framtiden.

3.2.3 Säkerhetspolisens underrättelseverksamhet

Enligt 2 § förordningen (2002:1050) med instruktion för Säkerhetspolisen ska Säkerhetspolisen leda och bedriva polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet, bekämpa terrorism samt fullgöra de uppgifter som Rikspolisstyrelsen har att utföra enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Med säkerhetsskydd avses skydd mot bl.a. spioneri liksom mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Säkerhetspolisen har enligt förordningen också uppdrag att leda och bedriva det bevakningsoch säkerhetsarbete som avser den centrala statsledningen eller som har samband med statsbesök och liknande händelser.

Uppdraget att förebygga och avslöja brott mot rikets säkerhet innebär att Säkerhetspolisen ska motverka olaglig eller oanmäld underrättelseverksamhet som bedrivs i Sverige. Likaså ska Säkerhetspolisen förhindra att organisationer, grupper, nätverk eller enskilda individer bedriver säkerhetshotande verksamhet som syftar till att hota eller störa det demokratiska styrelseskicket eller enskildas rätt att utöva sina demokratiska rättigheter. Uppdraget att bekämpa terrorism innebär att Säkerhetspolisen ska minska risken för att terroristbrott begås i Sverige och utomlands samt motverka att Sverige och svenska förhållanden utnyttjas som bas för stöd till terroristverksamhet. När det gäller skyddet av den centrala statsledningen ska Säkerhetspolisen verka för att den och de personer i övrigt som omfattas av Säkerhetspolisens personskyddsverksamhet ska kunna utföra sina åtaganden under trygga och säkra former. Säkerhetspolisens uppdrag är således i allt väsentligt brottsförebyggande och uppdraget är i mycket detsamma som för en säkerhetstjänst. Den brottsutredande verksamheten kommer härigenom i andra hand och utgör en mycket begränsad del av uppdraget. Detta avspeglar sig också tydligt i Säkerhetspolisens resursfördelning mellan brottsförebyggande och brottsutredande arbete.

För att Säkerhetspolisen ska kunna fullgöra sitt uppdrag måste myndighetens verksamhet inriktas utifrån den hotbild som finns mot de företeelser som Säkerhetspolisen ska skydda. Det är dels

fråga om en strategisk hotbild för att inrikta verksamheten långsiktigt, dels hotbilder som är knutna till en viss person, en viss händelse eller vissa företeelser. Hotbilden bestäms utifrån en bedömning av vilken avsikt och förmåga som en aktör har när det gäller att begå aktuella brott.

Säkerhetspolisens underrättelseverksamhet syftar i allt väsentligt till att lägga grunden för hotbildsbedömningarna och därigenom det brottsförebyggande arbetet. Tillförlitliga hotbilder och relevanta skyddsåtgärder förutsätter att underrättelseverksamheten kan följa olika aktörer och fånga upp varningssignaler redan innan en viss person vidtagit konkreta åtgärder för att begå ett brott. Det kan handla om att kartlägga utländsk underrättelseverksamhet i Sverige eller grupper som tydligt manifesterat en vilja att hota eller begå andra brott för att störa personer i syfte att få dem att sluta bedriva en viss politik. Det kan naturligtvis förekomma att Säkerhetspolisen får uppgifter som gör att en förundersökning ska inledas. Syftet med underrättelseverksamheten är dock inte att få fram uppgifter till underlag för en sådan bedömning.

Säkerhetspolisen tillämpar i princip samma modell som den övriga polisen för att styra underrättelsearbetet. Modellen innebär i korthet att ett väl definierat underrättelsebehov leder till en beställning av uppgifter. Beställningen resulterar i att olika inhämtningsåtgärder vidtas. De inhämtade uppgifterna bearbetas och analyseras varefter resultatet rapporteras till beställaren. Resultatet ligger sedan till grund för beslut om fortsatta åtgärder. Genom att tillämpa modellen blir inhämtningen aldrig slumpartad. Underrättelseverksamheten är tydligt avgränsad och det finns ett väl definierat mål för arbetet.

De inhämtningsmetoder som Säkerhetspolisen använder i sin underrättelseverksamhet är inte reglerade i särskild lagstiftning. Liksom beträffande den öppna polisen sätter de allmänna principer för polisingripande som anges i 8 § polislagen den yttre ramen för verksamheten. Säkerhetspolisen har alltså att beakta såväl behovs- som proportionalitetsprincipen innan en åtgärd beslutas. Säkerhetspolisens inhämtningsmetoder skiljer sig härigenom inte från de metoder som används inom polisen i övrigt. Det kan exempelvis vara fråga om inhämtning genom fysisk spaning, liksom genom öppna eller egna källor. Även såväl nationell som internationell samverkan med andra myndigheter har stor betydelse för underrättelseverksamheten.

3.2.4 Ekobrottsmyndighetens underrättelseverksamhet

Sedan den 1 januari 2004 har Ekobrottsmyndigheten möjlighet att bedriva kriminalunderrättelseverksamhet. I förarbetena till lagändringarna i polisdatalagen (1998:622) uttalades att kriminalunderrättelseverksamhet typiskt sett är en renodlad polisverksamhet och därför inte bör ledas av Ekobrottsmyndigheten såsom varande åklagarmyndighet (prop. 2002/03:144 s. 17). Verksamheten bör enligt förarbetena i stället ledas av Rikspolisstyrelsen.

Av 7 § förordningen (2007:972) med instruktion för Ekobrottsmyndigheten följer att de polismän som tjänstgör på Ekobrottsmyndigheten tillkallas av Rikspolisstyrelsen samt att Ekobrottsmyndigheten leder den verksamhet som polismännen ska delta i vid myndigheten, med undantag för åtgärder i verksamheten som enligt lag eller annan författning endast får utföras av anställda inom polisen. Polisverksamheten vid Ekobrottsmyndighetens leds av Rikspolisstyrelsen genom Ekobrottskansliet.

Kriminalunderrättelseverksamheten vid Ekobrottsmyndigheten är inriktad mot att förhindra, upptäcka och avbryta grov och organiserad ekonomisk brottslighet och den brottslighet som har samband med annan organiserad och allvarlig brottslighet. Kriminalunderrättelseverksamheten ska även arbeta brottsförebyggande med en hög grad av samverkan med andra myndigheters kriminalunderrättelseverksamhet. Den huvudsakliga uppgiften består i att aktivt skapa och underhålla kontakter inom och utanför Ekobrottsmyndigheten. Detta sker för att hämta in och sammanlänka upplysningar, identifiera och bedöma misstänkta brottslingar och kriminella strukturer. Kriminalunderrättelseverksamheten syftar också till att på ett tidigt stadium identifiera nya brottsliga företeelser och förändringar i brottslighet. Den ska dels utgöra ett direkt stöd för operativ verksamhet, dels ge underlag till beslut om resurskraftsamling och långsiktig inriktning av verksamheten.

3.2.5 Tullverkets underrättelseverksamhet

Underrättelseverksamhet i Tullverket utgör ett stöd för den brottsbekämpande verksamheten genom att tillföra aktuell och bearbetad information om förväntad eller pågående brottslig verksamhet samt kunskap om och förståelse av brottslig verksamhet.

Underrättelseverksamhet i Tullverket bedrivs genom insamling/inhämtning, bearbetning och analys av uppgifter. Syftet är att förhindra eller upptäcka brottslig verksamhet.

Resultatet av underrättelseverksamhet, de slutsatser eller produkter som tas fram, delges beslutsfattare på olika nivåer och ingår som beslutsunderlag dels vid beslut om inriktning och prioriteringar av Tullverkets brottsbekämpande verksamhet (strategisk underrättelse), dels vid beslut om direkt operativa åtgärder (operativ underrättelse).

Det finns fyra kärnområden för Tullverkets underrättelseverksamhet.

- Att utarbeta och löpande uppdatera profiler på objekt i de olika trafikflöden som från smugglingssynpunkt bör kontrolleras. Arbetet bygger bl.a. på återrapporter och iakttagelser från kontrollerande personal, på uppgifter i tillgängliga register och på uppgifter från samverkansmyndigheter.
- Att utarbeta underlag för beslut om direkt operativ åtgärd mot viss person eller grupp eller för beslut om att påbörja tullkriminalärende eller förundersökning. Detta sker genom inhämtning och bearbetning av uppgifter som kan förknippas med brottslig verksamhet.
- Att utarbeta underlag för beslut om inriktning och prioritering på något längre sikt av brottsbekämpande åtgärder. Dessa underlag kan avse visst trafikflöde, viss typ av transportmedel eller visst geografiskt område. Underlagen bygger på inhämtning och bearbetning av uppgifter som kan förknippas med brottslig verksamhet.
- Att löpande inhämta, kvalitetssäkra och systematisera uppgifter om misstänkt brottslighet.

I begreppet ”förhindra eller upptäcka” ligger att underrättelseverksamhet inte avser åtgärd mot ett redan begånget konkret brott utan i stället avser att söka avslöja om viss brottslighet har förekommit, pågår eller kan förutses. Man kan säga att verksamheten ofta börjar med en låg misstankegrad (anledning anta) om viss brottslig verksamhet. Genom riktad inhämtning och bearbetning av ytterligare uppgifter kan man antingen verifiera och komplettera till en högre misstankegrad, identifiera misstänkta och ett mer konkret brott eller avskriva den ursprungliga misstanken. Ju tidigare man kan

komma fram till en grundad uppfattning i dessa avseenden desto bättre. Här har det visat sig att inhämtning av uppgifter om elektronisk kommunikation enligt 6 kap. 22 § första stycket 3 LEK i många fall är ett snabbt och effektivt hjälpmedel.

3.2.6 Regelverk för polisens underrättelseverksamhet

I motsats till hur det förhåller sig med den brottutredande verksamheten är stora delar av myndigheternas underrättelseverksamhet inte lagreglerad. I stället sätter de allmänna principerna för ingripanden, som behovs- och proportionalitetsprinciperna, en ram för verksamheten. Viss lagreglering som rör underrättelseverksamhet finns dock.

Polisdatalagen reglerar behandlingen av personuppgifter. Den gäller utöver personuppgiftslagen (1998:204) och innehåller både allmänna regler om behandling av personuppgifter och regler om vissa särskilda register.

Med underrättelseverksamhet avses i polisdatalagen 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. Kriminalunderrättelseverksamhet definieras som annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen.

Personuppgifter får behandlas i kriminalunderrättelseverksamhet endast inom ramen för en särskild undersökning eller i kriminalunderrättelseregister, som är ett av de register som regleras särskilt i polisdatalagen. Register som inte regleras där förs t.ex. med stöd av Datainspektionens tillstånd.

En särskild undersökning är en undersökning i kriminalunderrättelseverksamhet som innebär 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. Den särskilda undersökningen ska ha inletts under ledning av Rikspolisstyrelsen eller en polismyndighet och det ska finnas anledning att anta att allvarlig brottslighet verksamhet har utövats eller kan komma att utövas. Med sådan verksamhet avses i polisdatalagen verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver. Uppgifter om en person som det inte finns någon misstanke mot ska förses med en upplysning om detta förhållande. Beslutet om att behandla personuppgifter i

en särskild undersökning ska innehålla uppgifter om ändamålet med behandlingen och de villkor i övrigt som behövs för att förebygga otillbörligt intrång i de registrerades personliga integritet. Uppgifterna ska gallras senast ett år efter det att beslutet om behandlingen av personuppgifter fattades. Om det är av särskild betydelse för att den särskilda undersökningen ska kunna avslutas, får dock uppgifterna behandlas under längre tid.

Kriminalunderrättelseregister får föras endast för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslig verksamhet eller för att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet. Ett kriminalunderrättelseregister får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet utövats eller kan komma att utövas och den som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva denna verksamhet. Uppgifter om transportmedel eller varor som kan antas ha samband med allvarlig brottslig verksamhet eller om hjälpmedel som kan antas ha använts i samband med sådan verksamhet får dock registreras, även om de kan hänföras till en enskild person som det inte finns någon misstanke mot. De ska därvid förses med upplysning om att det inte finns någon misstanke mot denne. I 20 § polisdatalagen finns närmare bestämmelser om vad ett kriminalunderrättelseregister får innehålla. Uppgifterna i ett kriminalunderrättelseregister om en registrerad person ska gallras senast tre år efter det att uppgifter om att denne skäligen kan misstänkas för att ha utövat eller komma att utöva allvarlig brottslig verksamhet senast infördes. Om en särskild undersökning som rör en registrerad person har inletts, får dock uppgifterna stå kvar till dess att undersökningen har avslutats.

Bestämmelsen i 9 d § personuppgiftslagen om att personuppgifter som samlats in för ett ändamål inte får behandlas för något annat oförenligt ändamål gäller även för polisens verksamhet.

SÄPO-registret är ett annat av de register som regleras i polisdatalagen (32–35 §§). SÄPO-registret har till ändamål att underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet och bekämpa terroristbrott samt att utgöra underlag för registerkontroll enligt säkerhetsskyddslagen. SÄPO-registret får innehålla uppgifter som kan hänföras till en enskild person endast om den person uppgifterna gäller kan misstänkas för att ha utövat eller komma att utöva brottslig verksamhet som innefattar hot mot rikets säkerhet eller terroristbrott, om personen har undergått

registerkontroll enligt säkerhetsskyddslagen eller om det med hänsyn till registrets ändamål annars finns särskilda skäl till det. SÄPO-registret får endast innehålla identifieringsuppgifter, uppgifter om grunden för registrering och hänvisning till de ärenden där uppgifter om den registrerade behandlas. Även gallringsregler finns i lagen.

Enligt en promemoria som tagits fram av en arbetsgrupp bestående av tjänstemän i Justitiedepartementet (Ds 2007:43) ska polisdatalagen ersättas av en ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det övergripande syftet med lagen är att skydda människor mot att deras personliga integritet kränks vid polisens behandling av personuppgifter. Förslaget till ny lag har tagits fram för att komma till rätta med olika problem som den nuvarande regleringen har visat sig ge upphov till, bl.a. när det gäller möjligheten att behandla personuppgifter för att förebygga, förhindra och upptäcka brottslig verksamhet. Den nya lagen ska också skapa förutsättningar för ett bättre samarbete mellan de brottsbekämpande myndigheterna genom ändrade bestämmelser om utlämnande av uppgifter. Den föreslagna lagen är heltäckande och reglerar, med några få undantag, all polisens behandling av personuppgifter i den brottsbekämpande verksamheten vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Personuppgifter ska enligt förslaget få behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott, eller fullgöra de förpliktelser som följer av internationella åtaganden. Särskilda bestämmelser föreslås för sådan behandling som sker hos Säkerhetspolisen. För behandling av personuppgifter som fler än ett fåtal personer har åtkomst till (gemensamt tillgängliga uppgifter) föreslås olika begränsande bestämmelser för att trygga den personliga integriteten. Det föreslås också en särskild lag som reglerar polisens allmänna spaningsregister. Personuppgiftsbehandling i sådan verksamhet som inte är brottsbekämpande, exempelvis den hjälpande verksamheten, omfattas inte av lagförslagen utan förutsätts, liksom i dag, regleras av personuppgiftslagen. Lagförslagen bereds inom Regeringskansliet.

3.2.7 Regelverk för tullens underrättelseverksamhet

Lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet gäller för Tullverkets behandling av personuppgifter, bl.a. om behandlingen är helt eller delvis automatiserad. Bestämmelserna i lagen tillämpas, med vissa undantag, i stället för personuppgiftslagen. Uppgifter får behandlas i Tullverkets brottsbekämpande verksamhet om det behövs för att förhindra eller upptäcka brottslig verksamhet, utreda eller beivra visst brott eller fullgöra det arbete som Tullverket är skyldigt att utföra enligt lagen (2000:1219) om internationellt tullsamarbete. Uppgifter får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i författningsreglerad brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Skatteverket och Kustbevakningen.

För att förhindra eller upptäcka brottslig verksamhet får sådana uppgifter behandlas som kan hänföras till en person, bl.a. om de behandlade uppgifterna ger anledning att anta att sådan verksamhet utövats eller kan komma att utövas som innefattar brott för vilket är föreskrivet fängelse i minst två år och gör att personen skäligen kan misstänkas för att ha utövat eller komma att utöva verksamheten. Uppgifter får också behandlas om de avser en person som utan att vara skäligen misstänkt kan antas ha samband med sådan verksamhet liksom uppgifter som avser transportmedel, varor eller hjälpmedel som kan antas ha samband med verksamheten. För att utreda eller beivra visst brott får uppgifter om den som kan misstänkas för brottet och om andra personer behandlas när det behövs.

I lagen finns också bestämmelser om den s.k. tullbrottsdatabasen, som är en samling av uppgifter och handlingar som med hjälp av automatiserad behandling används gemensamt i verksamheten, och vilka uppgifter som får behandlas i den.

3.3 Kraftsamling mot grov organiserad brottslighet

Regeringen tog under hösten 2007 initiativ till en nationell mobilisering mot grov organiserad brottlighet. I maj 2008 lämnade sex experter förslag på åtgärder som ska skapa förutsättningar för en effektivare och mer uthållig bekämpning av den grova organiserade brottsligheten (Ds 2008:38). Med utgångspunkt i de förslagen

fattade regeringen i juli 2008 beslut som innebär en förstärkning av insatserna mot den grova organiserade brottsligheten. Bl.a. har Rikspolisstyrelsen fått i uppdrag att inrätta särskilda aktionsgrupper med totalt 200 poliser vid åtta polismyndigheter och vid Rikskriminalpolisen. Vidare har Säkerhetspolisen fått ett nationellt huvudansvar för att, genom bl.a. underrättelsearbete, förebygga, kartlägga och motverka den grova organiserade brottslighetens påverkan på viktiga samhällsfunktioner som politiker, myndighetsföreträdare och journalister.

3.4 Underrättelseinhämtning för vissa polisiära behov

Signalspaning har sedan länge varit en viktig inhämtningsmetod i underrättelseverksamheten, inte minst för Säkerhetspolisens del. Metoden är emellertid resurskrävande. Försvarets radioanstalt har i hög grad bidragit till underrättelseinhämtning om utländska förhållanden när det gäller bl.a. internationell terrorism, annan grov gränsöverskridande brottslighet och främmande underrättelseverksamhet mot svenska intressen. Underrättelser som inhämtats av Försvarets radioanstalt har utgjort ett viktigt underlag för Säkerhetspolisens och Rikskriminalpolisens verksamheter.

Mot bakgrund av en politisk överenskommelse hösten 2008 kommer Försvarets radioanstalt framöver endast att bedriva signalspaning i försvarsunderrättelseverksamhet enligt den inriktning som regeringen, Regeringskansliet och Försvarsmakten bestämmer. Regeringen har därför gett en särskild utredare i uppdrag att kartlägga Säkerhetspolisens och Rikskriminalpolisens behov av underrättelser om utländska förhållanden, att utreda hur detta behov ska kunna tillgodoses på ett rättssäkert och effektivt sätt samt lämna fullständiga författningsförslag i frågan (Dir. 2008:120). Utredaren ska redovisa uppdraget senast den 30 juni 2009.

3.5 Straffprocessuella tvångsmedel

Straffprocessuella tvångsmedel används i brottsutredande syfte eller för att en rättegång i brottmål ska kunna genomföras. Normalt innefattar de tvång mot person eller egendom. Husrannsakan, kroppsvisitation, kroppsbesiktning och beslag utgör exempel på

straffprocessuella tvångsmedel liksom gripande, anhållande och häktning. Samtliga dessa åtgärder har som gemensam nämnare att de innebär ett intrång i en persons rättssfär och att de kan genomföras med direkt verkande tvång.

Hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och hemlig rumsavlyssning betraktas också som straffprocessuella tvångsmedel, trots att de saknar inslag av tvång. Det torde bero på det grundlagsskydd som finns i 2 kap. 6 § regeringsformen, och möjligen också på att den avlyssnade eller övervakade skulle motsätta sig åtgärden om han eller hon kände till den.

För all tvångsmedelsanvändning gäller tre allmänna principer. Ändamålsprincipen innebär att en myndighets befogenhet att använda tvångsmedel ska vara bunden till det ändamål för vilket tvångsmedlet har beslutats. Behovsprincipen innebär att en myndighet får använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden.

3.6 Hemlig teleavlyssning enligt rättegångsbalken

Hemlig teleavlyssning enligt 27 kap. 18–33 §§ RB innebär att telemeddelanden som befordras från det att tvångsmedlet börjar verkställas (*avlyssning i realtid*) eller som har befordrats innan tvångsmedlet börjat verkställas (*avlyssning av historiska meddelanden*), avlyssnas eller spelas in i hemlighet genom ett tekniskt hjälpmedel. Här är det alltså inte *uppgifter om* utan *innehållet i* telemeddelandet, t.ex. telefonsamtalet, SMS-meddelandet, telefaxmeddelandet eller e-postmeddelandet, som görs tillgängligt för de brottsbekämpande myndigheterna.

Tillstånd till hemlig teleavlyssning får ges av rätten när förundersökningen rör ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till ett sådant brott. Tillstånd till hemlig teleavlyssning får även ges genom en s.k. straffvärdeventil, när minimistraffet inte uppgår till fängelse i minst två år men straffvärdet i det enskilda fallet kan antas överstiga två års fängelse (prop. 2002/03:74, bet. 2003/04:JuU2).

Hemlig teleavlyssning får användas endast om någon är skäligen misstänkt för ett visst brott. Begreppet skälig misstanke används i vissa fall som en förutsättning för tillämpningen även av andra tvångsmedel enligt rättegångsbalken, t.ex. gripande, reseförbud, kvarstad och kroppsbesiktning.

För att hemlig teleavlyssning ska tillåtas fordras att åtgärden är av synnerlig vikt för utredningen om brottet. Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen ska ge avgörande bevisning som omedelbart kan leda till fällande dom men inrymmer däremot ett kvalitetskrav beträffande de upplysningar som åtgärden kan ge. Det måste vara fråga om uppgifter som har betydelse för att föra utredningen om brottet framåt. Uttrycket omfattar också ett krav på att utredningsläget ska göra avlyssningen nödvändig (prop. 1988/89:124 s. 44 f.).

Tillståndstiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad, såvitt gäller tid som infaller efter beslutet, alltså vid framtida meddelanden (realtid). Tillstånd kan dock förnyas på begäran av åklagaren.

Beslutet får avse en 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. Exempel på det sistnämnda kan vara en teleadress som innehas av en närstående till en misstänkt eller en teleadress på den misstänktes arbetsplats. Beslutet får även avse en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.

Telemeddelanden mellan den misstänkte och hans eller hennes försvarare får inte avlyssnas. Om ett sådant meddelande råkar avlyssnas, ska avlyssningen avbrytas och upptagningen i denna del omedelbart förstöras.

En upptagning eller uppteckning som gjorts vid hemlig teleavlyssning ska granskas snarast möjligt.

3.7 Hemlig teleövervakning enligt rättegångsbalken

Hemlig teleövervakning enligt 27 kap. 19–33 §§ RB innebär att det i hemlighet hämtas in uppgifter om telemeddelanden som befordras eller har befordrats till eller från en teleadress. Det är alltså fråga om såväl *realtidsuppgifter* (uppgifter som genereras från det att beslutet om tvångsmedlet börjat verkställas) som *historiska uppgifter*.

Om hemlig teleövervakning avser ett telefonnummer kan en brottsbekämpande myndighet med hjälp av åtgärden få uppgift om bl.a. till vilka telefonnummer samtal befordras eller har befordrats från det övervakade numret, från vilka telefonnummer samtal befordras eller har befordrats till det numret, vid vilka tidpunkter samtalen sker eller har skett och längden på samtalen. Är det i stället fråga om elektronisk post, finns möjligheten att genom tvångsmedlet få liknande uppgifter, exempelvis till vilka adresser meddelanden har expedierats från den övervakade adressen. Hemlig teleövervakning kan även innebära att ett telemeddelande hindras att nå fram till eller nå från en viss teleadress. Den möjligheten kan användas för att exempelvis förhindra kontakter, t.ex. varnande samtal, mellan personer som är missänkta för brott. Ett annat exempel är att kommunikation med en mobiltelefon förhindras för att tvinga en misstänkt person att i stället använda sig av en viss annan telefon (SOU 1998:46 s. 477). I fråga om mobiltelefonsamtal är det också möjligt att genom hemlig teleövervakning få reda på från vilket geografiskt område ett telefonsamtal rings och var mottagaren av samtalet befinner sig (lokaliseringsuppgifter).

Tillstånd till hemlig teleövervakning kan ges av rätten när förundersökningen rör brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, brott enligt 4 kap. 9 c § brottsbalken (dataintrång), brott enligt 16 kap. 10 a § brottsbalken (barnpornografibrott som inte är att anse som ringa), brott enligt 1 § narkotikastrafflagen (1968:64, narkotikabrott) eller brott enligt 6 § första stycket lagen om straff för smuggling (narkotikasmuggling). Vidare får tillstånd meddelas vid misstanke om försök, förberedelse eller stämpling till de nämnda brotten.

Liksom vid hemlig teleavlyssning finns det vid hemlig teleövervakning krav på att någon ska vara skäligen misstänkt för brottet, att åtgärden ska vara av synnerlig vikt för utredningen och att tillståndstiden inte får överstiga en månad, såvitt gäller tid som infaller efter beslutet. Även vid hemlig teleövervakning kan tillståndet

förnyas på begäran av åklagaren. Vidare finns samma begränsning till vilka teleadresser som övervakningen får avse, dvs. teleadresser 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 samt teleadresser som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta. Dessutom finns det fr.o.m. den 1 januari 2008 krav på att även upptagningar och uppteckningar som gjorts vid hemlig teleövervakning ska granskas snarast möjligt. Till skillnad mot bestämmelserna om hemlig teleavlyssning finns ingen begränsning som går ut på att telemeddelanden mellan den misstänkte och försvararen inte får övervakas.

3.8 Hemlig teleavlyssning och hemlig teleövervakning enligt vissa andra lagar

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns förutom i rättegångsbalken även i en del andra lagar. Lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott gäller för allmänfarliga brott, brott mot rikets säkerhet och terroristbrott. Enligt den behöver ett misstänkt brott i vissa fall inte vara så allvarligt att det omfattas av bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken för att tillstånd ska få ges till åtgärderna. Dessutom får åklagare i brådskande fall ge tillfälliga tillstånd.

Även enligt lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. får åklagare under vissa förutsättningar fatta sådana interimistiska beslut. Enligt lagen (1991:572) om särskild utlänningskontroll får domstol ge tillstånd till hemlig teleavlyssning och hemlig teleövervakning även i visst förebyggande syfte. Dessutom finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning i lagen (2000:562) om internationell rättslig hjälp i brottmål (se avsnitt 3.9).

Sedan den 1 januari 2008 gäller lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Enligt den får bl.a. hemlig teleavlyssning och hemlig teleövervakning användas även innan en förundersökning ska inledas, dvs. innan det finns anledning att anta att ett brott har förövats (jfr 23 kap. 1 § RB). Tillstånd till

åtgärderna får meddelas om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva viss allvarlig brottslig verksamhet. Det gäller vissa allmänfarliga brott, brott mot rikets säkerhet och terroristbrott, dvs. den brottslighet som faller inom Säkerhetspolisens ansvarsområde. Lagen gäller även vissa andra brott, som mord och människorov, om avsikten är att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd. I övrigt är förutsättningarna för åtgärderna likartade de förutsättningar som gäller enligt rättegångsbalken. Bl.a. får åtgärden enbart avse teleadresser med viss anknytning till den aktuella personen. Dessutom ska åtgärden vara av synnerlig vikt för att förhindra brottslig verksamhet. Liksom enligt rättegångsbalken lämnas tillstånd av domstol. Tillståndstiden får inte vara längre än en månad åt gången för framtida avlyssning och övervakning. Hemlig teleavlyssning får inte avse telemeddelanden mellan den person åtgärden avser och dennes försvarare. Upptagningar eller uppteckningar ska granskas snarast möjligt.

3.9 Lagen om internationell rättslig hjälp i brottmål

Bestämmelser om internationell rättslig hjälp i brottmål finns i lagen om internationell rättslig hjälp i brottmål (Lirb), i förordningen (2000:704) med samma namn och i tillkännagivande (2005:1207) av överenskommelser som avses i lagen om internationell rättslig hjälp i brottmål. Innehållet i flera internationella överenskommelser som Sverige har tillträtt eller annars är bundet av har arbetats in i den svenska lagen eller förordningen.

Lagen är tillämplig på det internationella rättsliga samarbetet, dvs. på det samarbete som tar sikte på rättsliga förfaranden som gäller utredning om och lagföring för brott. Lagen tillämpas av svenska åklagare och domstolar men är inte tillämplig i det internationella polissamarbetet. I fråga om utlämning, överförande av lagföring och delgivning finns särskilda bestämmelser.

Enligt lagen kan rättslig hjälp bl.a. omfatta hemlig teleavlyssning och hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning samt tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning (1 kap. 2 § första stycket 6–8 Lirb).

En ansökan om rättslig hjälp i form av *hemlig teleavlyssning eller hemlig teleövervakning i Sverige* handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för den begärda åtgärden och ansöka om rättens tillstånd. I förhållande till EU-stater samt Island och Norge får hemlig teleavlyssning eller hemlig teleövervakning verkställas genom omedelbar överföring av telemeddelanden eller uppgifter om telemeddelanden till den ansökande staten om det kan ske under betryggande former. Tillstånd till hemlig teleavlyssning eller hemlig teleövervakning lämnas under samma förutsättningar som gäller för motsvarande åtgärder under en svensk förundersökning enligt rättegångsbalken och enligt de särskilda bestämmelserna i lagen om internationell rättslig hjälp i brottmål (2 kap. 1 § första stycket och 4 kap. 25 och 25 a §§ Lirb). Vid prövningen om åtgärden kan vidtas i Sverige ska gärningen bedömas enligt svensk rätt. Kopplingen i 2 kap. 1 § Lirb till bestämmelserna i rättegångsbalken innebär automatiskt ett krav på dubbel straffbarhet och att de strafftrösklar som gäller enligt rättegångsbalken (27 kap. 18 och 19 §§ RB) även tillämpas gentemot den andra staten. Kravet på dubbel straffbarhet framgår dessutom uttryckligen i 2 kap. 2 § Lirb.

En ansökan om rättslig hjälp i form av *tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning i Sverige* prövas av åklagare. Sådan rättslig hjälp kan lämnas i förhållande till EU-länder samt Island och Norge och bygger på att telemeddelanden kan överföras omedelbart till den ansökande staten samt att meddelanden ska avlyssnas och tas upp där och inte i Sverige. Svenska myndigheters insatser begränsas till att tekniskt hjälpa till med att överföra telemeddelanden till den ansökande statens myndigheter, dvs. att möjliggöra verkställighet av det utländska beslutet. För att en ansökan ska beviljas krävs att beslut om hemlig teleavlyssning eller hemlig teleövervakning har meddelats i den ansökande staten och att överföringen kan ske under betryggande former. Rättslig hjälp i form av tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning i Sverige lämnas i enlighet med bestämmelserna i 2 kap. 1 § andra stycket samt 4 kap. 25 b och 25 c §§ Lirb. Vid denna form av rättslig hjälp krävs inte dubbel straffbarhet.

Tillstånd till *gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning, utan svenskt bistånd, av någon som befinner sig i Sverige*, lämnas av domstol. En utländsk ansökan om sådan rättslig hjälp handläggs av åklagare enligt bestämmelserna i 4 kap. 26–26 b §§ Lirb. Åklagaren ska genast pröva om förutsättningar för

åtgärden finns och i så fall ansöka om rättens tillstånd. Av 2 kap. 2 § Lirb framgår att det krävs dubbel straffbarhet.

Den åklagare eller domare som handlägger ansökan om rättslig hjälp prövar också om de förutsättningar som gäller enligt lagen, t.ex. angående ansökans innehåll, krav på dubbel straffbarhet eller viss strafftröskel är uppfyllda. Om så inte är fallet ska ansökan avslås efter att den ansökande utländska myndigheten fått tillfälle att komma in med komplettering (2 kap. 9 § och 15 § andra stycket Lirb).

Avslag på grund av hänsyn till Sveriges suveränitet, rikets säkerhet och svenska allmänna intressen och liknande prövas av regeringen (2 kap. 14 § och 15 § första stycket Lirb). Om en åklagare finner att en ansökan om rättslig hjälp bör avslås på någon sådan grund, ska ansökan, efter att samråd skett med riksåklagaren, överlämnas till Justitiedepartementet.

Om en begäran om rättslig hjälp bifalls, kan särskilda villkor ställas upp som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt, t.ex. att uppgifterna inte får föras vidare till annan stat eller att de ska förstöras efter att de har använts i den utredning de har begärts in för. Villkor får dock inte ställas upp om de strider mot en internationell överenskommelse som är bindande för Sverige (5 kap. 2 § Lirb).

Om uppgifter som den andra staten efterfrågar skulle finnas hos en svensk myndighet, t.ex. hos polisen efter en verkställd hemlig teleövervakning, gäller även bestämmelserna i sekretesslagen (1980:100). Enligt 1 kap. 3 § tredje stycket den lagen får sekretessbelagd uppgift inte röjas för utländsk myndighet annat än om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten.

Svenska åklagares och domstolars egna möjligheter att utomlands begära rättslig hjälp styrs i huvudsak av lagstiftningen i den andra staten och av de internationella åtaganden som den staten har gjort i förhållande till Sverige. Förutom att det finns vissa allmänna regler om vad en sådan ansökan ska innehålla och vart den ska skickas, finns vissa särskilda bestämmelser i lagen om internationell rättslig hjälp i brottmål som tar sikte på svenska åklagares handläggning av ärenden om hemlig teleavlyssning och hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning och hemlig

teleövervakning, samt tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning utomlands.

I enlighet med bestämmelserna i lagen om internationell rättslig hjälp i brottmål får åklagare ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med hemlig teleavlyssning eller hemlig teleövervakning av någon som befinner sig i en annan stat eller i Sverige. Av ansökan ska framgå under vilken tid åtgärden önskas samt sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Den andra staten kan kräva att ansökan ska prövas av domstol i Sverige. Det ankommer då på åklagaren att begära att rätten ska pröva frågan om att tillåta den hemliga teleavlyssningen eller hemliga teleövervakningen (4 kap. 26 § Lirb).

Om svensk domstol beslutat om hemlig teleavlyssning eller hemlig teleövervakning och den person som åtgärden avser befinner sig i en annan EU-stat eller på Island eller i Norge, och Sverige har möjlighet att vidta åtgärden utan bistånd av den andra staten, ska åklagaren ansöka om tillstånd till åtgärden från den andra staten (4 kap. 26 c § Lirb). Ett sådant tillstånd bör om möjligt sökas innan åtgärden har påbörjats eller annars omedelbart sedan det framkommit att den person som åtgärden avser befinner sig i den andra staten. Ansökan om tillstånd till åtgärden görs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden beräknas pågå. Ansökan ska också innehålla uppgift om det svenska domstolsbeslutet om tvångsmedlet.

3.10 Lagen om elektronisk kommunikation

3.10.1 Leverantörernas behandling av trafikuppgifter

Lagen om elektronisk kommunikation är en i huvudsak näringsrättslig lagstiftning som syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet (1 kap. 1 § LEK). Lagen omfattar t.ex. telefoni och datakommunikation samt utsändningar till allmänheten av program i ljudradio och TV.

I 6 kap. finns bestämmelser om behandling av personuppgifter och annat som rör integritetsskydd vid leverantörernas tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Huvudregeln för sådan behandling

framgår av 6 kap. 5 § LEK och innebär att trafikuppgifter, som i princip motsvarar uppgifter som ges vid hemlig teleövervakning och som avser användare eller abonnenter som är fysiska personer och som lagras eller behandlas på annat sätt av den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § LEK, ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande.

Lagen tillåter dock att uppgifterna sparas för viss behandling. Enligt 6 kap. 6 § första stycket LEK får de trafikuppgifter som krävs för abonnentfakturering och betalning av avgifter för samtrafik behandlas till dess att fordran är betald eller preskription har inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften. Enligt bestämmelsens andra stycke får uppgifterna också behandlas för att bl.a. marknadsföra elektroniska kommunikationstjänster, om den abonnent eller användare som uppgifterna avser har samtyckt till det.

Även i 6 kap. 8 § LEK finns bestämmelser som tillåter att trafikuppgifter sparas. Det rör för det första fallet att en myndighet behöver ha tillgång till sådana uppgifter för att lösa tvister. För det andra rör det elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning eller hemlig teleövervakning. Det tredje fallet gäller när trafikuppgifterna är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Enligt förarbetena (prop. 2002/03:110 s. 392) får uppgifterna inte sparas längre än vad som är nödvändigt för syftet. Längre tid än ett år bör inte godtas, om det inte föreligger särskild anledning, som att tvist har uppkommit eller förundersökning inletts i ett särskilt fall. I propositionen anfördes också att bestämmelsen även omfattar lagring av uppgifter för utredning och lagföring av brott, förutsatt att det sker i syfte att förhindra eller avslöja en obehörig användning av nätet eller tjänsten i fråga.

Ytterligare undantag från huvudregeln i 6 kap. 5 § LEK om att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande finns i 6 kap. 13 § LEK. Enligt den bestämmelsen får skyddet mot nummerpresentation temporärt åsidosättas för att spåra störande samtal. Det kan vara fråga om hotfulla samtal eller rena okynnessamtal. Om en abonnent begär spårning av sådana samtal, får uppgifter som

identifierar den anropande abonnenten lagras och hållas tillgängliga för abonnenten på begäran.

3.10.2 Brottbekämpande myndigheters tillgång till uppgifter

Allmänt om tystnadsplikten

I lagen om elektronisk kommunikation finns bestämmelser som ger de brottsbekämpande myndigheterna möjligheter att under särskilt angivna omständigheter utan domstolsprövning få tillgång till i princip samma uppgifter som vid hemlig teleövervakning. Det rör sig här enbart om historiska uppgifter.

Regleringen i lagen om elektronisk kommunikation har sin utgångspunkt i att trafikuppgifterna av integritetshänsyn omfattas av tystnadsplikt hos leverantörerna. När uppgifterna lämnas ut till brottsbekämpande myndigheter sker det med stöd av särskilda bestämmelser om undantag från tystnadsplikten. Bestämmelsen i 6 kap. 20 § LEK om tystnadsplikt har följande lydelse.

> Den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till
> 1. uppgift om abonnemang,
> 2. innehållet i ett elektroniskt meddelande, eller
> 3. annan uppgift som angår ett särskilt elektroniskt meddelande, får inte obehörigen föra vidare eller utnyttja det han fått del av eller tillgång till.
>
> Sådan tystnadsplikt gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på annat sätt har sänt eller tagit emot ett sådant meddelande.
>
> Tystnadsplikt i fråga om uppgifter som avses i första stycket 1 och 3 gäller inte heller i förhållande till innehavare av ett abonnemang som använts för ett elektroniskt meddelande.

Som följer av bestämmelsens första stycke gäller tystnadsplikten alla leverantörer. Det krävs inte att det nät eller den tjänst som leverantören tillhandahåller är allmänt respektive allmän. Uttrycket i bestämmelsen om vem som träffas av tystnadsplikten (”den som i samband med tillhandahållande”) innebär att tillämpningsområdet inte är begränsat till leverantören utan att också andra aktörer omfattas av tystnadsplikten, t.ex. den som på uppdrag av leverantören utför delar av tillhandahållandet av nätet eller tjänsten (se om detta och om undantag från tystnadsplikten Post- och telestyrel-

sens [PTS] ”Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter” från 2006-11-28).

Enligt 6 kap. 21 § LEK har leverantörerna dessutom tystnadsplikt för uppgift om bl.a. hemlig teleavlyssning, hemlig teleövervakning och kvarhållande av försändelser. Denna tystnadsplikt gäller även mot abonnenten.

Det är främst genom de *undantag* från tystnadsplikten som regleras i 6 kap. 22 § första stycket 2 och 3 LEK som de brottsbekämpande myndigheterna har möjligheter att begära och få ut uppgifter i liknande situationer som vid hemlig teleövervakning. Bestämmelserna lyder på följande sätt.

> Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket skall på begäran lämna
> /---/
> 2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,
> 3. uppgift som avses i 20 § första stycket 3 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,
> /---/

Uppgift om abonnemang

Tystnadsplikt enligt 6 kap. 20 § första stycket 1 LEK för uppgift om abonnemang avser uppgifter som identifierar en abonnent eller ett abonnemang (”kataloguppgifter”), framför allt namn, titel, adress och abonnentnummer, t.ex. telefonnummer. Även s.k. IMSI-nummer (International Mobile Subscriber Identity, ett nummer som är kopplat till abonnentens telefonnummer) har ansetts falla in under kategorin uppgift om abonnemang.

IP-nummer har också ansetts utgöra uppgift om abonnemang. Det gäller oavsett om IP-numret är fast eller dynamiskt (jfr dock Ds 2005:6 s. 324). Ett IP-nummer är en teknisk uppgift som krävs för att terminaler ska kunna identifiera och kommunicera med varandra i ett datornätverk med hjälp av kommunikationsprotokollet Internet Protocol (IP). Ett IP-nummer har koppling till ett abonnemang och det är genom IP-numret möjligt att identifiera

vilken abonnent som vid en viss tidpunkt varit uppkopplad mot Internet. Varje leverantör disponerar ett visst antal IP-nummer, som ”lånas ut” till abonnenterna. Tilldelningen av IP-nummer kan ske på permanent basis omfattande den tid som följer av avtalet mellan slutanvändaren och leverantören, s.k. fasta IP-nummer. Tilldelningen av ett dynamiskt IP-nummer avser i stället en kortare period, vilken bestäms vid ett anslutningstillfälle. En användare kan därmed erhålla olika dynamiska IP-nummer vid olika tillfällen. Samma dynamiska IP-nummer kan dock även komma att tilldelas en och samma användare vid olika tillfällen.

PTS har i ett yttrande den 11 juli 2001 (dnr 01-13584) kommit till slutsatsen att både fasta och dynamiska IP-nummer får anses utgöra uppgift om abonnemang. Även om PTS i sitt remissyttrande över BRU:s (Beredningen för rättsväsendets utveckling, Ju 2000:13) delbetänkande Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38) har framfört att det kan finnas anledning för myndigheten att överväga en förändring av denna inställning, har någon sådan förändring inte skett.

Uppgifter om abonnemang ska som framgår av bestämmelsen lämnas ut om fängelse är föreskrivet för brottet och brottet enligt den brottsbekämpande myndighetens bedömning kan föranleda annan påföljd än böter.

Annan uppgift som angår ett särskilt elektroniskt meddelande

Tystnadsplikt enligt 6 kap. 20 § första stycket 3 LEK för annan uppgift som angår ett särskilt elektroniskt meddelande har ansetts avse bl.a. uppgift om mellan vilka telefonnummer eller IP-nummer som ett elektroniskt meddelande har förmedlats, när och under hur lång tid förbindelsen var uppkopplad, från vilken basstation ett visst samtal skett samt det s.k. IMEI-numret (International Mobile Equipment Identity, ett nummer som ger identiteten på utrustningen eller hårdvaran).

Uttrycket uppgift som angår ett särskilt elektroniskt meddelande ska inte förstås så att den brottsbekämpande myndigheten måste specificera enskilda meddelanden, t.ex. genom att ange en viss abonnent och tidpunkt för meddelandet. Vid en basstationstömning begär myndigheterna uppgifter som omfattas av tystnadsplikt om t.ex. samtliga mobiltelefoner som har varit uppkopplade för kommunikation och haft kontakt med en basstation i närheten

av en brottsplats under en begränsad tid. En basstation är en radiosändare och radiomottagare som håller radiokontakt med mobilnätets mobiltelefoner och terminaler. Varje basstation har en eller flera antenner, som vanligtvis sitter monterade på en mast eller en byggnad. En antenn betjänar ett visst geografiskt område (en cell). När myndigheterna begär en basstationstömning måste det geografiska området specificeras så att myndigheten med hjälp av leverantören kan bestämma vilka celler som är aktuella. Dessutom måste en avgränsning i tiden göras. Uttrycket basstationstömning framstår därför i och för sig som något oegentligt, eftersom det normalt inte är en hel basstation som töms på uppgifter, utan enbart sådana uppgifter om kommunikation som registrerats i de celler som täcker ett utpekat geografiskt område under en begränsad tid. Det handlar vidare inte om uppgifter som rör en enbart påslagen telefon, utan endast uppgifter som genereras när ett samtal eller meddelandeutbyte äger rum. Uppgifterna har ansetts vara annan uppgift som angår ett särskilt elektroniskt meddelande.

Uppgifterna ska lämnas ut till de brottsbekämpande myndigheterna om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år. Det innebär att inga försöks-, förberedelse- eller stämplingsbrott omfattas av regleringen (23 kap. 1 och 2 §§ brottsbalken).

När uppgifter lämnas ut enligt lagen om elektronisk kommunikation är det inte domstol som fattar beslut om utlämnande, utan begäran till leverantören kommer direkt från polis-, åklagar- eller tullmyndighet. Enligt JO bör ett inhämtande av uppgifterna alltid underställas förundersökningsledaren (JO 1998/99 s. 95).

Det finns inte någon formell begränsning i tiden för den information som får begäras ut, eller med andra ord hur ”gammal” informationen får vara. En praktisk begränsning i möjligheten för de brottsbekämpande myndigheterna att få uppgifter från leverantörer finns dock i den nuvarande skyldigheten för leverantörerna att utplåna eller avidentifiera uppgifter (6 kap. 5 § LEK). Trafikuppgiftsutredningen har i betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76) föreslagit hur EG:s direktiv om lagring av trafikuppgifter ska genomföras i svensk rätt. Förslaget innebär bl.a. att leverantörerna ska vara skyldiga att lagra trafikuppgifter för brottsbekämpande ändamål under ett års tid. Förslaget bereds för närvarande inom Regeringskansliet.

De aktuella bestämmelserna i lagen om elektronisk kommunikation är inte begränsade till en förundersökningssituation utan har

ansetts kunna användas även i underrättelseverksamheten. Bestämmelserna är inte heller begränsade till att gälla uppgifter som har anknytning till en person (jfr exempelvis 27 kap. 20 § första stycket RB). Det är med andra ord inte nödvändigt att som vid hemlig teleövervakning ha en skäligen misstänkt person för att undantaget från tystnadsplikten ska bli tillämpligt och uppgifterna lämnas ut. Inte heller behöver den teleadress som begäran avser ha en särskild anknytning till en eventuell misstänkt person.

Vissa andra uppgifter

Det finns uppgifter hos leverantörerna som inte omfattas av tystnadsplikten enligt 6 kap. 20 § LEK. Det gäller t.ex. uppgift om den s.k. PUK-koden (Personal Unblocking Key, Personlig UpplåsningsKod) och lokaliseringsuppgifter som inte samtidigt är trafikuppgifter (6 kap. 9 § LEK), såsom uppgifter om position från satellit (GPS) (se prop. 2002/03:110 s. 260 f.). I sådana fall har leverantören inte någon skyldighet att lämna ut uppgifterna till en brottsbekämpande myndighet enligt bestämmelsen i 6 kap. 22 § LEK. Myndigheten kan i dessa fall få tillgång till uppgifterna genom beslag och editionsföreläggande (se avsnitt 3.12 och 6.5.2). Om myndigheten i stället begär ut uppgifterna får leverantören pröva frågan om utlämnande med tillämpning av andra bestämmelser, t.ex. personuppgiftslagen.

3.11 Sekretesslagen

I sekretesslagen finns bestämmelser om sekretess som gäller för myndigheter som driver televerksamhet. Enligt 1 kap. 9 § sekretesslagen ska aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner eller landsting utövar ett rättsligt bestämmande inflytande jämställas med myndighet vid tillämpningen av sekretesslagen. Enligt 6 kap. 2 § LEK ska sekretesslagen tillämpas i det allmännas verksamhet i stället för 6 kap. 20–23 §§ LEK, dvs. i stället för bestämmelserna om tystnadsplikten och undantagen från denna.

I 9 kap. 8 § andra stycket sekretesslagen föreskrivs att sekretess gäller för en uppgift som angår ett särskilt telefonsamtal eller annat telemeddelande hos en myndighet som driver televerksamhet. En

sådan uppgift som angår misstanke om brott får emellertid, som huvudregel, lämnas till en myndighet som har att ingripa mot brottet, om det är föreskrivet fängelse i minst ett år för brottet (14 kap. 2 § fjärde och femte styckena sekretesslagen). Såväl innehållet i ett telemeddelande som uppgifter om ett telemeddelande (både realtidsuppgifter och historiska uppgifter), torde kunna lämnas ut (jfr SOU 1992:70 s. 328 och prop. 1992/93:200 s. 311). Det är den utlämnande myndigheten som prövar om det enligt sekretesslagen finns förutsättningar för att lämna ut en uppgift till den brottsbekämpande myndigheten. Liksom för utlämnande enligt lagen om elektronisk kommunikation krävs inget domstolsbeslut. Bestämmelserna i sekretesslagen är inte heller begränsade till att gälla situationer när det finns en skäligen misstänkt person eller till teleadresser med särskild anknytning till denne.

Sedan Televerket som myndighet upphörde att bedriva verksamhet har möjligheten att med stöd av sekretesslagen hämta in uppgifter om telemeddelanden kommit att i princip sakna praktisk betydelse för de brottsbekämpande myndigheternas verksamhet. I stället fick den numera upphävda telelagen (1993:597) och senare lagen om elektronisk kommunikation den betydelse som sekretesslagen tidigare hade.

3.12 Beslag och editionsföreläggande

Det har i praxis förelegat en osäkerhet huruvida beslag och editionsföreläggande kan användas för att få uppgifter som finns om telemeddelanden *hos leverantörer*. Det har förekommit att de brottsutredande myndigheterna har berett sig tillgång till uppgifterna med hjälp av reglerna om husrannsakan och beslag i 27 och 28 kap. RB eller genom att utverka editionsföreläggande enligt 38 kap. 4 § RB. Det rör alltså sådana fall där det annars finns regler om utlämnande av uppgifter enligt rättegångsbalken och lagen om elektronisk kommunikation (SOU 1998:46 s. 71 och JO 1997/98 s. 47 ff.). Regeringen har uttalat att uppgifter om telemeddelanden, eller, med det uttryck som används i 6 kap. 20 § första stycket 3 LEK, ”uppgifter som angår ett särskilt elektroniskt meddelande”, hos leverantörer inte kan hämtas in med stöd av editionsföreläggande och husrannsakan i förening med beslag i fall där annars dessa andra regler för utfående av uppgifter gäller. Enligt regeringen får detta anses följa redan av allmänna principer och

något lagstiftningsbehov finns därför inte (prop. 2002/03:74 s. 45 f.).

Det bör nämnas att regeringens uttalande inte avser möjligheten för de brottsutredande myndigheterna att genomföra t.ex. husrannsakan i förening med beslag *hos annan än leverantör* för att få fram uppgifterna. Det kan t.ex. röra sig om innehållet i en telefonsvarare som enbart den enskilde förfogar över eller band med inspelade telemeddelanden som förvaras av den enskilde (SOU 1998:46 s. 373).

Teleövervakningsuppgifter hos den enskilde kan finnas t.ex. i en nummerpresentatör eller i en mobiltelefon samtidigt som dessa uppgifter finns i leverantörens system. Det kan röra uppgift om inkomna eller utgående samtal och senast slagna nummer, När det gäller uppgifter som finns *både hos den enskilde och hos leverantören* kan uppgifterna bli åtkomliga för de brottsutredande myndigheterna på båda sätten, genom t.ex. hemlig teleövervakning eller genom beslag eventuellt i kombination med husrannsakan hos den enskilde (SOU 1998:46 s. 373).

När det gäller uppgifter som inte omfattas av reglerna om utlämnande i rättegångsbalken och i lagen om elektronisk kommunikation kan beslag och editionsföreläggande användas, se avsnitt 6.5.2.

3.13 Rättssäkerhetsgarantier vid användning av hemliga tvångsmedel, m.m.

3.13.1 Allmänt

Det är av grundläggande betydelse i en demokratisk rättsstat att post- och telehemligheten liksom rätten till privatliv och korrespondens respekteras. För en effektiv brottsbekämpning är det visserligen ibland nödvändigt att det görs vissa ingrepp i enskildas personliga sfär, t.ex. genom hemlig teleavlyssning och hemlig teleövervakning. De regler som styr tvångsmedelsregleringen bygger på en avvägning mellan å ena sidan samhällets och medborgarnas intresse av en effektiv brottsbekämpning och å andra sidan intresset av att skydda enskildas integritet. Med hänsyn till den integritetskränkande arten av sådana åtgärder är det av största vikt att de vidtas med stor urskillning och att riskerna för missbruk minimeras.

Skyddet mot missbruk av tvångsmedel som inte är hemliga ligger till viss del i att den som utsätts för tvångsmedlet är eller blir medveten om åtgärden och kan få den prövad av domstol eller på annat sätt. Något motsvarande gäller i praktiken inte beträffande hemliga tvångsmedel. Det ligger i det hemliga tvångsmedlets natur att den enskilde ska vara omedveten om åtgärden. Hemlighållandet ökar risken för en oriktig tillämpning av reglerna om hur hemliga tvångsmedel får användas. Mot det bakgrunden är det givetvis angeläget att förutsättningarna för användandet av de hemliga tvångsmedlen är tydliga. Även andra rättssäkerhetsinstrument har stor betydelse i fråga om de hemliga tvångsmedlen, t.ex. olika former av rättslig tillsyn och parlamentarisk kontroll. Det integritetsintrång åtgärden typiskt sett medför är avgörande för vilka rättssäkerhetsgarantier som behöver finnas.

3.13.2 Regeringsformen

I 2 kap. regeringsformen finns bestämmelser som skyddar medborgarna mot ingrepp från det allmänna. Bestämmelserna har betydelse för vilken användning av hemliga tvångsmedel och andra s.k. särskilda arbetsmetoder som får förekomma i brottsbekämpningen.

Bestämmelsen i 2 kap. 6 § regeringsformen innehåller regler som skyddar den enskilde mot bl.a. kroppsvisitation, husrannsakan och annat liknande intrång från det allmännas sida. Paragrafen ställer också upp hinder för det allmänna att inhämta information genom undersökning av brev eller andra förtroliga försändelser eller genom hemlig avlyssning eller upptagning av telefonsamtal eller andra förtroliga meddelanden. Det skydd som 2 kap. 6 § regeringsformen ger den enskilde får enligt 2 kap. 12 § begränsas men endast genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får därtill aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen.

3.13.3 Europakonventionen

Användandet av hemliga tvångsmedel, liksom de brottsbekämpande myndigheternas dolda spaningsarbete m.m., berörs främst av artiklarna 6, 8 och 13 i Europakonventionen. I 2 kap. 23 § reger-

ingsformen finns ett förbud mot att meddela lag eller annan föreskrift i strid med Sveriges åtaganden på grund av konventionen.

Artikel 6 innehåller bestämmelser om rätten till en rättvis rättegång, som bl.a. anses innebära att en åtalad ska underrättas om allt utredningsmaterial.

I artikel 8 finns bestämmelser om rätten till respekt för privat- och familjeliv, hem och korrespondens. Skyddet får visserligen inskränkas men endast under vissa förutsättningar. Bland annat får inskränkningen ske endast med stöd av lag och endast om det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa bestämda intressen, däribland statens säkerhet, den allmänna säkerheten och förebyggandet av oordning eller brott. Rätten till privatliv ska i detta sammanhang förstås i vid mening. Också rätten till respekt för korrespondens har en vid betydelse och omfattar många slag av medelbar kommunikation som avsändaren och mottagaren kan förvänta sig ska förmedlas utan att andra tar del av innehållet.

Enligt artikel 13 ska var och en, vars fri- och rättigheter enligt konventionen har kränkts, ha tillgång till ett effektivt rättsmedel inför nationell myndighet. Med att ett rättsmedel är effektivt avses att det medger en tillfredsställande prövning av ett klagomål. Det krävs inte att prövningen sker i domstol. Även administrativa rättsmedel kan uppfylla konventionskraven. Det är inte nödvändigt att ett enda rättsmedel ensamt uppfyller kravet på ett effektivt rättsmedel utan flera rättsmedel i den nationella lagstiftningen kan tillsammans uppfylla kravet.

3.13.4 FN:s konvention om medborgerliga och politiska rättigheter

Förenta Nationernas generalförsamling antog år 1948 en allmän förklaring om de mänskliga rättigheterna. I artikel 12 i den allmänna förklaringen slås fast att ingen får utsättas för godtyckliga ingripanden i fråga om privatliv, familj, hem eller korrespondens. Grundsatsen har arbetats in i 1966 års FN-konvention om medborgerliga och politiska rättigheter (artikel 17).

3.13.5 Den enskildes rätt till insyn m.m.

Brottsmisstänkta som åtalas har en vidsträckt rätt till partsinsyn i utredningsmaterialet. Innan åtal beslutas ska den misstänkte och försvararen underrättas om förundersökningsmaterialet. Detta sker normalt på så sätt att ett preliminärt förundersökningsprotokoll görs tillgängligt för den misstänkte och försvararen (23 kap. 18 § RB).

Sekretess innebär inte någon begränsning i en parts rätt enligt rättegångsbalken att få ta del av alla omständigheter som läggs till grund för ett avgörande av ett mål eller ärende (jfr 14 kap. 5 § sekretesslagen). Inte heller får några förbehåll uppställas för den misstänktes eller försvararens förfoganderätt över kopian av förundersökningsprotokollet och innehållet i detta eller andra handlingar som han eller hon har rätt att ta del av enligt 23 kap. 18 § RB (jfr 14 kap. 10 § sekretesslagen).

Dessutom föreskrivs i förundersökningskungörelsen att alla omständigheter av betydelse ska antecknas i förundersökningsprotokollet. Särskilt anges att beslut om användning av tvångsmedel ska antecknas (20 §). Visserligen får åklagaren låta bli att ta med uppgifter i förundersökningsprotokollet som enligt åklagarens bedömning är betydelselösa för utredningen. Åklagaren måste dock iaktta objektivitet och får inte låta bli att ta med uppgifter som ur försvarets synvinkel kan vara betydelsefulla.

När åklagarens ansökan om tillstånd till hemlig teleavlyssning, hemlig kameraövervakning, hemlig rumsavlyssning och åtgärder enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet. Det offentliga ombudet, som ska vara eller ha varit advokat eller ha varit ordinarie domare, stärker enskildas rättssäkerhet genom att bevaka deras integritetsintressen. Ett offentligt ombud företräder dock inte någon misstänkt eller någon annan särskild person utan företräder enskildas intressen i allmänhet.

Sedan den 1 januari 2008 gäller att den som är eller har varit misstänkt för brott som huvudregel ska underrättas i efterhand om hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning som han eller hon har blivit utsatt för. I något fall ska underrättelse lämnas även enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Underrättelse ska lämnas så snart det kan ske utan men för utredningen,

dock senast en månad efter det att förundersökningen avslutades. 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.

3.13.6 Organ för löpande tillsyn och kontroll

Enskilda som blir föremål för hemliga tvångsmedel har begränsade möjligheter att påkalla en rättslig prövning genom överklagande av tillståndet till tvångsmedelsanvändningen. Det är därför betydelsefullt att det finns andra medel som kan användas mot eventuellt felaktiga beslut.

Utöver den kontroll i förhand som kravet på tillstånd av domstol för användning av hemliga tvångsmedel innebär finns det i gällande rätt olika slag av tillsyn och kontroll som utövas i efterhand. Justitieombudsmannen och Justitiekanslern utövar tillsyn över bl.a. den brottsbekämpande verksamheten och Datainspektionen liksom Säkerhets- och integritetsskyddsnämnden (se nedan) har tillsyn över personuppgiftsbehandling.

I åtskilliga andra länder har det vid sidan av tillsynen av domstolarna och förvaltningen överlag inrättats särskilda, ofta parlamentariskt anknutna organ för en löpande tillsyn av den verksamhet där hemliga tvångsmedel och andra dolda arbetsmetoder används. Sådana organ kan även bedriva tillsyn och kontroll på anmälan av enskild. Förekomsten av ett sådant organ har betydelse för bedömningen av om Europakonventionens krav på effektivt rättsmedel är uppfyllt. Europadomstolen bedömde i juni 2006 i målet Segerstedt-Wiberg m.fl. mot Sverige (Appl. No. 62332/00) att ordningen med Justitieombudsmannen, Justitiekanslern, dåvarande Registernämnden eller Datainspektionen, var för sig eller tillsammans, inte uppfyllde kravet på effektivt rättsmedel i artikel 13 i Europakonventionen.

Mot den bakgrunden inrättades Säkerhets- och integritetsskyddsnämnden från och med den 1 januari 2008 och övertog då samtliga uppgifter som Registernämnden hade haft. Säkerhets- och integritetsskyddsnämnden har till uppgift att med inspektioner och

andra undersökningar utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet samt över Säkerhetspolisens behandling av personuppgifter. Nämnden ska även på begäran av enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel eller har varit föremål för Säkerhetspolisens personuppgiftsbehandling och om tvångsmedelsanvändningen och därmed sammanhängande verksamhet eller personuppgiftsbehandlingen har skett i enlighet med lag eller annan författning.

Riksdagen utövar en parlamentarisk kontroll över regeringen och de statliga myndigheterna. Den parlamentariska kontrollen sker bl.a. på grundval av skrivelser av olika slag från regeringen men även från riksdagens egna tillsynsorgan såsom Justitieombudsmannen och Riksrevisionen.

3.13.7 Integritetsskyddskommittén

I mars 2007 överlämnade Integritetsskyddskommittén delbetänkandet Skyddet för den personliga integriteten (SOU 2007:22) med kartläggning och analys av sådan lagstiftning som rör den personliga integriteten. Kommittén konstaterade att det på en rad rättsområden finns brister i fråga om hur integritetsskyddet har tillvaratagits. Dessa brister beskrevs utförligt och kommittén analyserade orsakerna. Kommittén pekade framför allt på en felaktig metodik och strukturella brister som leder till att integritetsskyddsaspekterna inte beaktas tillräckligt när lagstiftningen utarbetas.

I sitt slutbetänkande Skyddet för den personliga integriteten (SOU 2008:3) gjorde Integritetsskyddskommittén den bedömningen att grundlagsskyddet för den personliga integriteten behöver stärkas bl.a. genom att regeringsformen kompletteras med ett nytt stadgande av innebörd att varje medborgare är skyddad gentemot det allmänna mot intrång som sker i hemlighet eller utan samtycke och som i betydande mån innebär övervakning eller kartläggning av den enskildes personliga förhållanden. En sådan bestämmelse menade kommittén skulle träffa de allt mer kvalificerade former av övervakning och sådan kartläggning som sker i form av registrering och hantering av personuppgifter inom ramen för omfattande informationssamlingar hos myndigheter. Bestäm-

melsen skulle även träffa hemliga straffprocessuella tvångsmedel, eftersom dessa åtgärder är särskilt känsliga från integritetsskyddssynpunkt genom att de används i hemlighet och genom att övervakningen vid exempelvis hemlig kameraövervakning och hemlig teleövervakning ständigt pågår med utnyttjande av fast anordnad apparatur under den tid som tillståndsbeslutet gäller. Kommittén bedömde dock att ett sådant grundlagsskydd inte skulle ge några omedelbara konsekvenser för tvångsmedlen, eftersom dessa typer av integritetsintrång redan är reglerade i gällande lagstiftning. Däremot var kommitténs slutsats att ett grundlagsskydd får till konsekvens att varje integritetsbegränsande ändring i den aktuella tvångsmedelslagstiftningen ska underkastas proportionalitetsprincipen och det kvalificerade förfarande som i övrigt anges i 2 kap. 12 § regeringsformen och att grundlagsenligheten av sådan lagstiftning kommer att kunna prövas enligt 11 kap. 14 § regeringsformen.

3.14 Internationell utblick

3.14.1 Danmark

I Danmark regleras polisens möjligheter till inhämtning av uppgifter om telemeddelanden i 71 kap. rättegångslagen (lov om rettens pleje). Regleringen gäller både den öppna polisen och säkerhetspolisen (Politiets Efterretningstjenste). Enligt 780 § i rättegångslagen får polisen, genom ingrepp i telehemligheten och utan innehavarens tillåtelse, inhämta uppgifter om vilka telefoner eller andra motsvarande kommunikationsapparater som har varit i förbindelse med en viss telefon eller motsvarande kommunikationsapparat (teleoplysning). Enligt samma paragraf får polisen också inhämta uppgifter om vilka telefoner eller motsvarande kommunikationsapparater som inom ett avgränsat geografiskt område har kommunicerat med andra telefoner eller kommunikationsapparater (udvidet teleoplysning). För att uppgifterna ska få inhämtas krävs att det finns misstanke (bestemte grunde til at antage) att en av parterna i kommunikationen är misstänkt i en undersökning (dock inte vid udvidet teleoplysning), att ingreppet kan antas vara av avgörande betydelse för undersökningen och att undersökningen rör ett brott med fängelse i sex år eller mer i straffskalan, eller vissa andra i 781 §, genom hänvisning till främst strafflagen, angivna brott.

Enligt 791 a § får polisen inhämta uppgifter om lokaliseringen av en mobiltelefon (teleobservation), som kan antas användas av en misstänkt person. För att uppgifterna ska få inhämtas krävs att de är av väsentlig betydelse för utredningen och att utredningen rör ett brott som kan medföra fängelse i ett och ett halvt år eller däröver.

Beslut om inhämtning av teleoplysning, udvidet teleoplysning eller teleobservation fattas av domstol. I brådskande fall får även polisen fatta beslut om sådan åtgärd. I sistnämnda fall ska polisens beslut snarast, och senast 24 timmar efter beslutets verkställande, underställas domstolen för prövning. Om domstolen finner att åtgärden inte borde ha beslutats ska domstolen underrätta Justitiedepartementet.

Innan domstolen fattar beslut ska en advokat utses för den som inhämtningen berör. Advokaten ska ges tillfälle att yttra sig. Advokaten har tystnadsplikt och får inte utan polisens samtycke sätta sig i förbindelse med den person vars rätt han eller hon ska bevaka. Domstolen kan besluta att advokaten i ett senare skede inte får verka som försvare i eventuella rättegångar rörande den aktuella brottligheten.

När inhämtningen av uppgifter avslutats ska innehavaren av den aktuella telefonen underrättas. Ansvarig för underrättelsen är den domstol som fattat beslutet. Polisen har möjlighet att begära att underrättelse ska fördröjas eller underlåtas. Skäl för att fördröja eller underlåta underrättelse kan vara t.ex. att en underrättelse kan vara till skada för aktuell eller annan brottsutredning eller att det behövs för att skydda hemliga uppgifter om polisens arbetsmetoder.

Några särskilda regler om inhämtning av uppgifter om telemeddelanden i förebyggande syfte eller i underrättelseverksamhet finns inte. Däremot är kravet på misstankegrad för inhämtning inom ramen för en förundersökning satt något lägre än i Sverige, vilket ansetts medföra att det i Danmark inte föreligger ett lika stort behov av att inhämta information inom ramen för underrättelseverksamheten.

3.14.2 Finland

I Finland regleras möjligheterna till inhämtning av uppgifter om telemeddelanden dels i 5 a kap. tvångsmedelslagen, dels i polis- respektive tullagarna.

Med teleövervakning avses enligt tvångsmedelslagen inhämtning av hemliga identifieringsuppgifter om ett telemeddelande som har sänts från eller mottagits av en teleanslutning, teleadress eller teleterminalutrustning som är kopplad till ett allmänt kommunikationsnät. Vidare avses inhämtning av uppgift om en mobilteleapparats läge.

Enligt tvångsmedelslagen får teleövervakning användas mot den som är skäligen misstänkt för brott för vilket det föreskrivna straffet är fängelse i minst fyra år samt vissa andra brott som t.ex. övergrepp i rättssak och olaga hot. Teleövervakning får även användas mot den som är skäligen misstänkt för försök till dessa brott eller förberedelse till brott som begås i terroristiskt syfte. Övervakningen får avse en teleanslutning, teleadress eller teleterminalutrustning som den misstänkte innehar eller kan antas använda om de uppgifter som inhämtas kan antas vara av synnerlig vikt för utredningen av brottet. Övervakningen kan även, med målsägandens samtycke, avse en teleanslutning eller teleadress som målsäganden innehar eller annars använder.

Den brottsutredande myndigheten kan avseende angivna brott även få uppgifter om vilka mobilteleapparater som har registrerats i telesystemet via en basstation som finns i närheten av en förmodad brottsplats eller någon annan plats som är av betydelse för utredningen av brottet, om inhämtandet av uppgifterna kan antas vara av synnerlig vikt för utredningen av brottet.

Beslut om inhämtning fattas av domstol efter ansökan av åklagare eller vissa särskilt angivna polis- och tulltjänstemän. I brådskande fall får åklagare eller särskilt angivna polis- och tulltjänstemän fatta interimistiskt beslut om inhämtning. Beslutet ska underställas domstolen så snart som möjligt, dock ska ansökan om domstolsprövning alltid göras senast 24 timmar efter att åtgärden har inletts. Frågan prövas vid ett sammanträde. Den misstänkte eller innehavaren av teleadressen ska inte höras. Dock ska en målsägande, i de fall övervakningen avser teleadress som innehas eller disponeras av målsäganden, normalt ges tillfälle att bli hörd.

Offentliga ombud ska förordnas av domstol i samband med prövningen av frågor om tillstånd till viss teknisk avlyssning. När det gäller teleövervakning förordnas dock inte offentliga ombud.

Tillstånd till teleövervakning kan beviljas för högst en månad åt gången. Tillståndet kan också beviljas för viss tid före tillståndsbeslutet. Denna tid kan vara längre än en månad.

Efter ett år eller när ärendet har överlämnats till åklagaren för prövning eller det annars har beslutats att förundersökningen ska avslutas ska den misstänkte underrättas om inhämtningen. På framställning av undersökningsledaren kan dock domstolen, av viktiga skäl som har samband med utredningen, besluta att underrättelse ska ske senare eller inte alls.

Teleövervakning kan även ske enligt polislagen och tullagen. I polislagens 3 kap. finns bestämmelser om inhämtning av information. Enligt denna reglering får polisen använda teleövervakning för att förhindra eller avslöja ett brott om det på grund den berörda personens uttalanden, hotelser, uppträdande eller annars finns grundad anledning att anta att personen gör sig skyldig till ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år eller vissa andra brott motsvarande vad som gäller enligt tvångsmedelslagen. Polisen har också rätt att utföra teleövervakning om det är nödvändigt för att avvärja fara för liv eller hälsa. Om det är av synnerlig vikt för förhindrande av samma brottslighet får polisen inhämta uppgifter om vilka mobilteleapparater som registrerats i telesystemet vid en basstation i närheten av en viss plats. På motsvarande sätt som enligt tvångsmedelslagen fattas besluten av domstol med en interimistisk beslutanderätt för polisen. När åtgärden avslutats ska polisen underrätta den som varit föremål för åtgärden om det inte skulle äventyra ändamålet för vilket inhämtningen skett eller förundersökningen av ett brott. Det finns dock inte någon skyldighet att underrätta de som har berörts av en inhämtning av uppgifter om vilka mobilteleapparater som registrerats i telesystemet vid en basstation i närheten av en viss plats.

Inrikesministeriet utövar tillsyn över användningen av teletvångsmedel, innefattande bl.a. teleövervakningen, både enligt tvångsmedelslagen och polislagen. Ministeriet ska årligen avge en berättelse till riksdagens justitieombudsman (JO) om denna användning. Tullen ska avge en egen rapport om tullens användning av teletvångsmedel.

3.14.3 Norge

Enligt 16 a kap. 216 a–k §§ i den norska straffprocesslagen (lov om rettergangsmåten i straffesaker) får polisen inhämta uppgifter om vilka kommunikationsanläggningar som varit i förbindelse med telefon, datamaskin eller annan kommunikationsanläggning som tillhör en misstänkt person eller som denne annars kan komma att använda (kommunikasjonskontroll). Tillstånd till kommunikationskontroll får bara lämnas om inhämtningen är av väsentlig betydelse för utredningen och utredningen annars försvåras i väsentlig grad.

Tillstånd till inhämtning ges av domstol. I brådskande fall får åklagare fatta beslut om inhämtning. I dessa fall ska beslutet underställas domstolens prövning snarast, och senast 24 timmar efter att inhämtningen påbörjades. Om tidsfristen för domstolsprövning löper ut utanför domstolens kontorstid förlängs fristen till dess domstolen öppnar igen.

Den som beslutet avser ges inte tillfälle att yttra sig och underrättas inte om ansökningen eller beslutet. Innan domstolen fattar beslut ska dock en advokat utses för den som inhämtningen berör. Advokaten ska ges tillfälle att yttra sig. Advokaten har tystnadsplikt och får inte utan polisens samtycke sätta sig i förbindelse med den person vars rätt han eller hon ska bevaka. Domstolen kan besluta att advokaten i ett senare skede inte får verka som försvarare i eventuella rättegångar rörande den aktuella brottligheten.

På begäran av enskild ska det lämnas underrättelse till den enskilde om han eller hon varit föremål för kommunikationskontroll. Underrättelse får lämnas tidigast ett år efter att kontrollen avslutades. Domstolen har dock möjlighet att bestämma att underrättelse ska fördröjas eller underlåtas om det kan vara till skada för utredningen eller andra förhållanden talar för att underrättelse bör fördröjas eller underlåtas.

Enligt den norska polislagens 17 d § kan säkerhetspolisen (Politiets sikkerhetstjenste) beviljas tillstånd att använda bl.a. kommunikationskontroll i förebyggande syfte. Det ska röra sig om viss genom hänvisningar i polislagen närmare specificerad allvarlig brottslighet. Liksom vid övrig inhämtning är det domstol som fattar beslut med en interimistisk beslutandemöjlighet för säkerhetspolisen. Regleringen motsvarar den som gäller för övrig inhämtning med undantaget att någon underrättelseskyldighet gentemot enskild inte föreligger.

Dessutom kan, enligt bestämmelser i straffprocesslagens 17 b kap. 222 d §, polisen och säkerhetspolisen ges tillstånd till bl.a. inhämtning av uppgifter om elektronisk kommunikation för att avvärja vissa allvarliga förestående brottsliga handlingar.

Tillsyn över den öppna polisens och åklagarmyndighetens hantering av inhämtning genom kommunikationskontroll görs av en särskild kontrollnämnd (Kontrolludvalget for kommunikasjonskontroll). De minst tre ledamöterna i kontrollnämnden utses för fyra år. Ordföranden ska uppfylla de krav som ställs för att bli domare i högsta domstolen. Kontrollnämnden ska granska de rapporter om användningen av hemliga tvångsmedel som upprättas av Riksåklagaren (Statsadvokaten). Vidare ska kontrollnämnden undersöka klagomål från enskilda avseende rättsstridig användning av hemliga tvångsmedel och även ta egna initiativ till granskning av frågor som rör användandet av sådana åtgärder.

Med stöd av straffprocesslagen har Justitiedepartementet utfärdat föreskrifter om att Riksåklagaren ska utöva tillsyn över den öppna polisens användning av tvångsmedel. Kopior på alla ansökningar och beslut om hemliga tvångsmedel, samt rapporter om användningen av hemliga tvångsmedel inom respektive polisdistrikt, ska sändas till Riksåklagaren, som i sin tur ska lämna en årlig rapport till Justitiedepartementet med kopia till Kontrolludvalget.

Kontrollen av säkerhetspolisen (samt de norska övervakningsoch underrättelsetjänsterna) utförs av en kontrollnämnd under Stortinget, det s.k. EOS-utvalget. Nämndens ledamöter nomineras av Stortinget och de flesta är f.d. parlamentariker. Kärnan i nämndens verksamhet är regelbundna inspektioner. Nämnden behandlar även klagomål från enskilda och undersöker på eget initiativ särskilda frågor. Den har insynsrätt i arkiv och får genomföra förhör med personal från berörda myndigheter. Nämnden lämnar en årlig rapport till Stortinget.

3.14.4 Storbritannien

I Storbritannien återfinns regler om inhämtning av trafikuppgifter från tele- och Internetoperatörer i Regulation of Investigative Powers Act (RIPA) från år 2000. Polisens och andra myndigheters inhämtning av kommunikations- och trafikuppgifter från telekommunikationssystem regleras i del I kapitel II. Särskilda riktlinjer (Code of Practice) om inhämtning av trafikuppgifter har

upprättats av Inrikesdepartementet och därefter godkänts av parlamentet. Enligt dessa bestämmelser får polisen, säkerhets- och underrättelsetjänsterna (Security Service [MI5], Security Intelligence Service [MI6] och Government Communications Headquarters [GCHQ]), Serious Organised Crime Agency (SOCA), skatte- och tullmyndigheten samt ett antal andra brottsbekämpande myndigheter inhämta trafikuppgifter. Av reglerna framgår att inhämtning får ske om det är nödvändigt för t.ex. nationella säkerhetsändamål eller för att förebygga eller upptäcka brott. I syftet att upptäcka brott innefattas bl.a. inhämtning för att ta reda på vem som är gärningsman, i vilket syfte eller med vilka medel ett brott har begåtts samt andra relevanta omständigheter för brottet. Det innefattar även insamling av bevis för användning i rättegång och gripande av gärningsmän. Av den officiella rapporten från den kommissionär som har till uppgift att utöva tillsyn över inhämtningen (Interception of Communications Commissioner, se nedan) framgår att inhämtning av trafikuppgifter för underrättelseändamål sker i stor utsträckning och att syftet då är att bygga upp en bild av personer eller grupper som kan utgöra ett reellt hot mot den nationella säkerheten.

För att inhämtning ska få ske krävs att den ska vara proportionell i förhållande till vad som kan förväntas uppnås med inhämtningen.

För att få till stånd ett beslut om inhämtning, som kan ha formen av antingen en underrättelse (notice) eller ett bemyndigande (authorisation), ska sökanden (the applicant, t.ex. en förundersökningsledare eller en tjänsteman vid säkerhetstjänsten) göra en skriftlig, eller i undantagsfall muntlig, ansökan. Denna prövas av en särskilt utpekad tjänsteman inom organisationen (the designated person). Som huvudregel ska denna tjänsteman inte pröva ansökningar avseende utredningar eller underrättelseprojekt som han eller hon själv är involverad i. Vid polisen och de andra myndigheterna ska vidare finnas en kontaktperson (single point of contact). Denna person ska ha särskild utbildning för att säkerställa lagligheten och effektiviteten i inhämtningarna. Det ska även finnas en överordnad ansvarig tjänsteman (senior responsible officer).

Varje myndighet ska upprätthålla ett register över beslut om inhämtning. Registret ska normalt finnas tillgängligt för inspektion hos kontaktpersonen.

Tillsynen sköts av en särskilt utsedd kommissionär (Interception of Communications Commissioner), som till sin hjälp har ett

antal inspektörer. Kommissionären lämnar en årlig rapport över sin tillsyn till parlamentet. I rapporten för år 2007 framgår bl.a. att brittiska myndigheter under år 2007 begärde in trafikuppgifter i 519 000 fall. Det finns också en särskilt utsedd kommissionär för tillsyn över säkerhetstjänsterna (Intelligence Services Commissioner). Hans befogenheter gällande övervakningen av inhämtning av trafikuppgifter är dock inskränkt och överlämnad till Interception of Communications Commissioner. Båda kommissionärerna, som utses av regeringen, är höga domare.

Genom RIPA inrättades också en särskild nämnd (Investigatory Powers Tribunal) för att pröva klagomål från enskilda som anser sig ha blivit felaktigt utsatta för t.ex. inhämtning av trafikuppgifter. Nämnden leds av en domare från högsta domstolen.

3.14.5 Tyskland

Bestämmelser om teleövervakning har nyligen genomgått en större översyn och återfinns i den tyska straffprocesslagen (Strafprozessordnung). Inhämtning av uppgifter om kommunikation får ske vid misstanke om sådan allvarlig brottslighet som närmare anges i lagen, om inhämtningen är nödvändig för utredningen. Det är inte tillåtet med inhämtning om det inte ingår fängelse i fem år eller mer i straffskalan förutom i fall när brottet har begåtts genom användning av telekommunikation.

Ansökan görs av åklagare och åtgärden beslutas av en undersökningsdomare vid en särskild undersökningsdomstol. Vid fara i dröjsmål kan åklagaren fatta ett interimistiskt beslut om inhämtning som ska underställas undersökningsdomarens prövning inom tre arbetsdagar.

Den som har varit föremål för teleövervakning ska underrättas om åtgärden så snart det kan ske utan fara för utredningen, för den offentliga säkerheten, eller för liv eller hälsa. Om åklagare ett år efter det att åtgärden avslutades fortfarande inte anser att underrättelse bör ske måste frågan underställas domstol.

För de underrättelse- och säkerhetstjänster som har till uppgift att skydda tyska nationella säkerhetsintressen[1] gäller en annan ordning. Dessa organisationer har möjlighet att inhämta uppgifter om

[1] Bundesamt für Verfassungsschutz (BfV), Bundesnachrichtendienst (BND) och Militärischer Abschirmdienst (MAD), samt delstatliga myndigheter inom författningsskyddet.

telekommunikation enligt den s.k. G 10-lagen (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) samt enligt tidsbegränsade anti-terror lagar. Systemet har utformats utifrån att regleringen av tvångsmedel enligt dessa lagar inte är av straffprocessuell natur och att tillståndsärenden därför inte heller har ansetts böra i första hand prövas av domstol.[2]

Inhämtning av uppgifter om kommunikation enligt G 10-lagen beslutas av den för operationen ansvarige ministern efter framställning från chefen för respektive säkerhets- eller underrättelsetjänst eller dennes ställföreträdare. För att inhämtning ska få ske krävs att det rör misstanke om planerade, pågående eller begångna brott, som närmare anges i lagen, eller om det finns omständigheter som tyder på medlemskap i vissa kriminella organisationer eller sammanslutningar. Det krävs även att andra sätt att inhämta informationen bedöms som utsiktslösa eller i vart fall väsentligt svårare. Ministeriet ska varje månad underrätta den oberoende G 10-kommissonen om beslutade inhämtningar. Innan G 10-kommissionen har prövat besluten får inhämtningarna verkställas endast om det föreligger fara i dröjsmål. Om G 10-kommissionen finner att inhämtningen är otillåten eller inte är nödvändig, får beslutet inte verkställas. Om verkställighet redan har skett ska verkställigheten avbrytas. En enskild som varit föremål för inhämtning ska underrättas så snart det kan ske utan att operationens syfte äventyras. Om det efter fem år fortfarande inte är möjligt att underrätta den enskilde kan G 10-kommissionen besluta att underrättelseskyldigheten inte längre ska gälla. Ledamöterna i G 10-kommissionen är vanligen f.d. parlamentariker och kommissionen leds av en ordförande som ska uppfylla kraven på domare. G 10-kommissionen har även till uppgift att ta emot klagomål från enskilda som anser sig blivit felaktigt utsatta för övervakning.

3.14.6 Sammanfattning

Det finns ett antal faktorer som förenar flertalet av de utländska regelverk för inhämtning av uppgifter om elektronisk kommunikation. Genomgången visar att inhämtning av elektronisk kommunikation med undantag för Danmark sker både i förundersökningar och i underrättelseverksamhet. Normalt är inhämtningen både i

[2] Jfr betänkandet Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (SOU 2006:98) s. 70.

förundersökningar och i underrättelseverksamheten lagreglerad. Regleringen kan vara i ett gemensamt regelverk, som i Storbritannien, eller uppdelat på olika lagar beroende på syftet med inhämtningen, som i Tyskland och i Finland samt delvis i Norge.

En viktig likhet mellan flera av de jämförda länderna är att beslutsbefogenheten i många fall tillkommer domstol eller undersökningsdomare men att det finns möjlighet för polis eller åklagare att fatta interimistiska beslut vid fara i dröjsmål.

När det särskilt gäller underrättelseverksamheten är det oftast polisen, säkerhetspolisen eller olika underrättelsetjänster som ansöker om åtgärder och i vissa fall även kan fatta interimistiska beslut. Åklagare är inte involverade. I vissa fall, som i Norge och i Finland, fattas själva tillståndsbeslutet av domstol, medan andra beslutsformer gäller för Tyskland och Storbritannien. Särskilt i Tyskland görs också en tydlig åtskillnad mellan å ena sidan underrättelseverksamhet/förebyggande åtgärder och å andra sidan straffprocessuella åtgärder som sker inom ramen för en brottsutredning.

En annan likhet är förekomsten av underrättelseskyldighet gentemot enskild, särskilt när det gäller inhämtning under förundersökning. Likaså finns i de flesta länder ett välutvecklat tillsynsförfarande av ett fristående organ rörande inhämtningen av uppgifter om elektronisk kommunikation.

4 Myndigheternas tillgång till uppgifterna

4.1 Inledning

Så länge som telefoni och annan elektronisk kommunikation har använts har det funnits behov av att ge de brottsbekämpande myndigheterna tillgång till uppgifter om abonnemang och elektronisk kommunikation. Med den snabba utvecklingen och användningen av modern informationsteknologi har betydelsen av tillgång till uppgifterna hela tiden ökat för att brottsbekämpningen ska kunna upprätthållas. Tillgång till uppgifterna har bedömts vara av avgörande betydelse i den verksamheten (SOU 2005:38 s. 307 ff. och SOU 2007:76 s. 129 ff.).

4.2 Uppgifter om elektronisk kommunikation

Som framgått tidigare är det i dagsläget möjligt för de brottsbekämpande myndigheterna att få tillgång till historiska uppgifter om elektronisk kommunikation enligt två regelverk, bestämmelserna om hemlig teleövervakning i rättegångsbalken och utlämnande av uppgifterna från leverantörer enligt lagen om elektronisk kommunikation. Myndigheterna får i princip samma uppgifter oavsett vilka bestämmelser som tillämpas.

Förutsättningarna för *hemlig teleövervakning* enligt 27 kap. 19–21 §§ RB är följande.

1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra
   a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),

b) dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling, eller
c) försök, förberedelse eller stämpling till brott under a) och b).

3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden ska avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.

Förutsättningarna för att de brottsbekämpande myndigheterna ska få tillgång till uppgifter enligt *6 kap. 22 § första stycket 3 LEK* är följande (i jämförelse med rättegångsbalken).

1. Det ska vara fråga om misstanke om brott för vilket det inte är föreskrivet lindrigare straff än två års fängelse (även anstiftan och medhjälp omfattas men inte försöks-, förberedelse- och stämplingsbrott).
2. Det behöver inte finnas en skäligen misstänkt person.
3. Åtgärden behöver inte vara av synnerlig vikt för utredningen.
4. Åtgärden är inte begränsad till vissa teleadresser.
5. Åtgärden beslutas av den brottsbekämpande myndigheten (polis, åklagare och tull, se JO 1998/99 s. 95).

Det ska också nämnas att förutsättningarna för att få ut uppgifter i form av uppgift om abonnemang (”kataloguppgifter”) enligt *6 kap. 22 § första stycket 2 LEK* är att fängelse är föreskrivet för brottet och det kan föranleda annan påföljd än böter i det enskilda fallet, dvs. brottet ska i det enskilda fallet vara så allvarligt att det ligger på fängelsenivå.

För att hemlig teleövervakning ska få användas måste alltså det brott förundersökningen avser som utgångspunkt ha ett minimistraff på sex månaders fängelse i straffskalan. Det kan vara av värde att ge några exempel på vilka brottstyper som faller under den kategorin. Det rör sig om mord, dråp, grov misshandel, vållande till annans död (enbart grovt brott), människorov, människohandel, olaga frihetsberövande (som inte är mindre grovt), olaga tvång (enbart grovt brott), grov fridskränkning/kvinnofridskränkning, olaga hot (enbart grovt brott), våldtäkt (som inte är mindre grov),

grovt sexuellt tvång, grovt sexuellt utnyttjande av person i beroendeställning, våldtäkt mot barn, grovt sexuellt övergrepp mot barn, grovt koppleri, grov stöld, rån, tillgrepp av fortskaffningsmedel (enbart grovt brott), grovt bedrägeri, utpressning (enbart grovt brott), ocker (enbart grovt brott), häleri (enbart grovt brott), penninghäleri (enbart grovt brott), svindleri (enbart grovt brott), grov förskingring, trolöshet mot huvudman (enbart grovt brott), olovligt brukande (enbart grovt brott), grov oredlighet mot borgenärer, grovt bokföringsbrott, mordbrand, allmänfarlig ödeläggelse, grovt sabotage, sjö- eller luftfartssabotage (enbart grovt brott), grov urkundsförfalskning, penningförfalskning (enbart grovt brott), grovt barnpornografibrott, övergrepp i rättssak (enbart grovt brott), grovt tjänstefel, bestickning/mutbrott (enbart grova brott), grovt narkotikabrott, grovt skattebrott, grovt dopningsbrott, brott mot alkohollagen (enbart grovt brott), grovt vapenbrott, grovt miljöbrott, grovt artskyddsbrott, grov smuggling, grov narkotikasmuggling, grovt tullbrott, terroristbrott, grovt insiderbrott och grov människosmuggling. Hemlig teleövervakning får också användas vid dataintrång, barnpornografibrott, som inte är att anses som ringa, narkotikabrott och narkotikasmuggling.

För att de brottsbekämpande myndigheterna ska få tillgång till annat än rena kataloguppgifter enligt lagen om elektronisk kommunikation krävs, som framgick tidigare, att uppgiften gäller misstankar om brott med minst två års fängelse i straffskalan. Exempel på sådana brott är mord, dråp, människorov, människohandel, våldtäkt, våldtäkt mot barn, grovt koppleri, grovt rån, mordbrand, allmänfarlig ödeläggelse, grovt sabotage, sjö- och luftfartssabotage (enbart grovt brott), övergrepp i rättssak (enbart grovt brott), grovt narkotikabrott, grov narkotikasmuggling och terroristbrott.

Varje år lämnar regeringen en redovisning till riksdagen över tillämpningen av hemlig teleavlyssning och hemlig teleövervakning. Regeringen får uppgifterna från Åklagarmyndigheten och Rikspolisstyrelsen. Den senaste redovisningen, som avser år 2007, gjordes i regeringens skrivelse 2008/09:79. Där framkom bl.a. följande. Under året lämnades tillstånd till hemlig teleövervakning i 1 315 fall. I samtliga fall där hemlig teleavlyssning beviljades under året (966 fall) hade domstolen samtidigt gett tillstånd till hemlig teleövervakning. I 349 fall hade tillstånd meddelats till enbart hemlig teleövervakning.

Motsvarande uppgifter sammanställs inte över de fall där de brottsbekämpande myndigheterna begär ut uppgifter (”annan uppgift som angår ett särskilt elektroniskt meddelande”) med stöd av lagen om elektronisk kommunikation. I betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38 s. 185) anger BRU att polisen uppskattade antalet sådana ärenden under år 2004 till drygt 4 000 stycken. Trafikuppgiftsutredningen redovisade nya beräkningar från polisen som innebär att antalet var ca 8 000 under år 2006 (SOU 2007:76 s. 225). Polisen har gjort beräkningar över antalet fall där man har begärt att få ut uppgifter under år 2007 och uppskattat det till ca 9 500 fall. Liksom tidigare innefattar den siffran inte uppgifter rörande Säkerhetspolisens och Tullverkets ärenden.

Mot bakgrund av kravet i lagen om elektronisk kommunikation på att det ska vara fråga om misstanke om brott med ett straffminimum på två års fängelse, står det klart att utredningarna enbart rör allvarlig brottslighet och att de brottsbekämpande myndigheterna många gånger har begärt uppgifter vid flera tillfällen i samma utredning. Det förhållandet att personer som är involverade i vissa kriminella aktiviteter köper, byter och slänger mobiltelefoner eller anonyma kontantkort mycket frekvent är en av de stora anledningarna till att det i dagsläget fattas relativt många beslut om att inhämta uppgifter om elektronisk kommunikation enligt 6 kap. 22 § första stycket 3 LEK. Myndigheterna behöver få fram vilka teleadresser som används, bl.a. genom basstationstömning, för att kunna få tillstånd till hemlig teleavlyssning och hemlig teleövervakning. Företrädare för Säkerhetspolisen, Rikskriminalpolisen och länskriminalpolisen i Stockholm uttryckte 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 resultat-

löst, vilket innebär att bl.a. hemlig teleövervakning över huvud taget inte kan användas i arbetet med att utreda grova brott.

Det finns även andra anledningar till att det många gånger fattas flera beslut i samma ärende och att antalet beslut om utlämnande enligt lagen om elektronisk kommunikation vida överstiger antalet beslut om hemlig teleövervakning. Särskilt i mer akuta lägen i utredningar fattas besluten ofta med kort tids mellanrum. Det kan ibland vara fråga om minuter. Vid exempelvis ett grovt rån mot en värdetransport kan polisen på några minuter få uppgifter från en basstationstömning rörande platsen för brottet. Polisen kanske också mycket snabbt behöver få nya basstationstömningar gjorda när det t.ex. blir klarlagt vilka flyktvägar rånarna använde sig av eller på vilka platser flyktbilar har lämnats. Därefter är det troligt att ytterligare beslut om att inhämta uppgifter om elektronisk kommunikation behöver fattas för att fortsätta undersökningarna kring de uppgifter som kommit fram genom basstationstömningarna, allt i syfte att identifiera skäligen misstänkta personer och teleadresser.

4.3 Uppgifter om abonnemang

Som framgår av avsnitt 3.10.2 har den leverantör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst tystnadsplikt för bl.a. uppgifter om abonnemang som leverantören har fått del av eller tillgång till (6 kap. 20 § första stycket 1 LEK). Med uppgifter om abonnemang (kataloguppgifter) avses främst namn, titel, adress och abonnentnummer (t.ex. telefonnummer). Även IMSI-nummer och IP-nummer har ansetts falla in under kategorin uppgift om abonnemang.

Det är självfallet så att de brottsbekämpande myndigheterna liksom andra inhämtar uppgifter om abonnemang genom att utnyttja öppna källor, t.ex. telefonkatalog och Internet. För uppgifter som inte på det viset är öppna genom avtalet mellan leverantören och kunden, t.ex. hemliga telefonnummer och IP-nummer, utnyttjas i stället bestämmelserna i lagen om elektronisk kommunikation.

I 6 kap. 22 § första stycket LEK anges de fall när leverantörerna är skyldiga, och därmed behöriga, att trots sin tystnadsplikt lämna uppgifter om abonnemang till bl.a. de brottsbekämpande myndigheterna. Bestämmelserna lyder på följande sätt.

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket skall på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (1970:428), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,
2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som skall ingripa mot brottet, om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,

/---/

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,
5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),
6. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten skall kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),
7. uppgift som avses i 20 § första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten skall kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och
8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

Som framgår rör flera av punkterna möjligheten för andra myndigheter än de brottsbekämpande att få tillgång till abonnemangsuppgifter från leverantörerna. Punkterna 6 och 7 rör polis och åklagares möjligheter att få abonnemangsuppgifter utan att det kan sägas vara fråga om direkt brottsbekämpande verksamhet. Särskilt punkten 6 rör den s.k. hjälpande verksamheten, alltså verksamhet eller åtgärder som i detta fall inte rör misstankar om brott utan som i stället avser att ge allmänheten skydd, upplysningar och annan hjälp.

5 Tidigare utredningar m.m.

5.1 Upphävande av 6 kap. 22 § första stycket 3 LEK

Flera utredningsförslag har tidigare berört de regler som finns i rättegångsbalken och lagen om elektronisk kommunikation om de brottsbekämpande myndigheternas möjligheter att få tillgång till historiska uppgifter om elektronisk kommunikation. För andra uppgifter än abonnemangsuppgifter ställer lagen om elektronisk kommunikation upp strängare krav när det gäller den misstänkta brottsligheten än rättegångsbalken gör (lägst två års fängelse respektive lägst sex månaders fängelse i straffskalan). I lagen om elektronisk kommunikation saknas däremot kraven på att det ska finnas en skäligen misstänkt person, att åtgärden ska vara av synnerlig vikt för utredningen, att enbart vissa teleadresser med anknytning till en person får omfattas av åtgärden och att domstol ska fatta beslut.

Buggningsutredningen (Ju 1996:07) hade bl.a. uppdraget att se över tillämpningsområdet för hemlig teleövervakning och de regler i övrigt som gör det möjligt för brottsbekämpande myndigheter att få tillgång till uppgifter om elektronisk kommunikation. I betänkandet Om buggning och andra hemliga tvångsmedel (SOU 1998:46) lämnade Buggningsutredningen förslag på en samlad reglering av bestämmelserna i rättegångsbalken. Förslaget innebar att bestämmelsen i telelagen som i dag motsvarar 6 kap. 22 § första stycket 3 LEK och den tidigare nämnda bestämmelsen i sekretesslagen (se avsnitt 3.11) skulle upphävas.

Även BRU konstaterade att regleringen inte framstår som ändamålsenligt utformad och att det skulle bli en förstärkning av integritetsskyddet för den enskilde om det som huvudregel blir domstol som får fatta beslut om att ge brottsbekämpande myndigheter tillgång till uppgifterna. BRU föreslog därför att de nämnda bestämmelserna i lagen om elektronisk kommunikation och

sekretesslagen skulle upphävas och myndigheternas tillgång till uppgifter om elektronisk kommunikation uteslutande skulle regleras i rättegångsbalken genom hemlig teleövervakning (SOU 2005:38 s. 182 ff.).

Att det är de brottsbekämpande myndigheterna som fattar beslut i dagsläget om att använda 6 kap. 22 § första stycket 3 LEK innebär en möjlighet att få fram uppgifterna mycket snabbare än om domstol skulle fatta besluten. BRU inhämtade flera exempel på situationer där en tillgång till uppgifterna i akuta skeden under eller efter det att grova brott begås eller har blivit begångna har lett till att brotten har kunnat klaras upp. För att den brottsbekämpande verksamheten inte ska förlora i effektivitet föreslog BRU att åklagare skulle ha rätt att ge interimistiska tillstånd till hemlig teleövervakning i brådskande fall. Av rättssäkerhets- och kontrollskäl föreslog BRU även att åklagarens beslut skulle prövas av domstol i efterhand (SOU 2005:38 s. 200 ff.).

5.2 Tillgång till uppgifter om abonnemang

BRU övervägde flera frågor rörande de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang. BRU beskrev bl.a. hanteringen vid inhämtande av uppgifterna, t.ex. uppgifter om vem som är abonnent rörande ett visst telefonnummer (SOU 2005:38 s. 229). Hanteringen sker i flera steg. Eftersom förfarandet är olika beroende på vilken leverantör abonnenten använder sig av, måste först den aktuella leverantören identifieras. Först jämförs telefonnumret med de tilldelningar som framgår av den svenska nummerplanen. Därefter kontaktas den leverantör abonnenten tillhör enligt planen. Om en abonnent har valt att portera sitt nummer till en ny leverantör och den ursprungliga leverantören inte känner till vilken den nya är, kan det medföra en hel del ytterligare utredningsarbete innan saken är klarlagd och polisen har fått del av uppgifterna. Rutinerna vid utlämning av uppgifter varierar. Ofta lämnas uppgifterna ut mot ett diarienummer för den aktuella förundersökningen eller efter motringning. Rutinerna hos de mindre leverantörerna är dock enligt uppgift till BRU ibland bristfälliga. Rikspolisstyrelsen angav till BRU att det med nuvarande hantering i vissa fall är svårt att få fram upplysningar om aktuella nummer, både hemliga och öppna, särskilt från mindre leverantörer, och att uppgifterna ofta bara kan erhållas under kontorstid på vardagar,

vilket kan innebära allvarliga störningar i brottsutredningsarbetet och övrigt arbete, t.ex. när larm ska lokaliseras.

Rikspolisstyrelsen har uppgivit till den här utredningen att problemen för de brottsbekämpande myndigheterna när det gäller hanteringen har blivit värre under de sista åren, särskilt när det gäller kontakten med mindre leverantörer av Internettelefoni.

BRU menade att det fanns flera nackdelar med den gällande ordningen såväl för polisen som för leverantörerna. Enligt BRU är ordningen långsam, arbetskrävande, kostsam och otillförlitlig. Dessutom hade BRU identifierat säkerhetsrisker, sekretessbrister och stora risker för fel och misstag i hanteringen. BRU föreslog därför att brottsbekämpande myndigheter skulle få generell tillgång (en slags direktåtkomst) till abonnemangsuppgifter på samma sätt som alarmeringscentralerna har (jfr 6 kap. 22 § första stycket 8 LEK). Med en sådan ordning skulle det enligt BRU uppkomma klara effektivitetsvinster, minskade kostnader, ökad snabbhet, minskade arbetsinsatser, minskat bortfall av uppgifter, ökat skydd för sekretessbelagda uppgifter och minskade säkerhetsrisker. BRU betonade dock att de fördelarna måste vägas mot intresset hos enskilda att uppgifterna inte sprids i onödan. I den delen resonerade BRU i huvudsak så att det enbart var fråga om kataloguppgifter och inte de mer integritetskänsliga uppgifterna enligt 6 kap. 20 § första stycket 3 LEK, dvs. annan uppgift som angår ett särskilt elektroniskt meddelande, och att fördelarna med en utvidgad tillgång till uppgifter om abonnemang vägde upp den i praktiken relativt begränsade risken för ökade intrång i enskildas integritet. BRU:s förslag blev därför bl.a. att leverantörerna skulle vara skyldiga att lämna uppgift om abonnemang till brottsutredande myndigheter utan begränsning till att brottet har viss svårhetsgrad.

5.3 Tillgång till uppgifter utan att det finns en skäligen misstänkt person

BRU tog upp frågan hur ett förslag om att upphäva 6 kap. 22 § första stycket 3 LEK skulle påverka effektiviteten i det brottsbekämpande arbetet. Såväl BRU som Trafikuppgiftsutredningen konstaterade att det finns ett mycket stort behov i brottsbekämpningen av tillgång till uppgifter om elektronisk kommunikation, särskilt vid allvarlig brottslighet. Uppgifterna har ansetts vara av avgörande betydelse i det sammanhanget (SOU 2005:38 s. 322 ff. och SOU

2007:76 s. 129 ff.). Trafikuppgiftsutredningen gav följande sammanfattande exempel utifrån verkliga händelser på vilken information trafikuppgifterna kan ge i utredningarna.

Mord: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter.

Människorov: En målsägande hölls fängslad under flera dagar och kunde lokaliseras genom trafikuppgifter.

Människohandel: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter. Likaså har transportvägar, förfalskningscentraler, platser för prostitution och kontaktnät utomlands klarlagts.

Olaga hot (grovt brott): Vid en fritagning från anstalt med automatvapen gick det att med hjälp av trafikuppgifter lokalisera gärningsmännen.

Dataintrång: Gärningsmän har identifierats och knutits till varandra genom trafikuppgifter.

Våldtäkt: Gärningsmän har identifierats genom trafikuppgifter. Exempelvis kunde en underårig målsägande ange att gärningsmannen under övergreppet, som skedde i bil, hade fått två samtal till sin mobiltelefon utan att besvara dessa. Genom de uppgifterna blev det möjligt att identifiera gärningsmannen, som också kunde bindas till andra liknande brott några år tidigare.

Grov stöld: Genom trafikuppgifter kunde en stöld av en container med cigaretter klaras upp genom att kontakterna mellan fem gärningsmän blev klarlagda. Brottet var först rubricerat som rån men trafikuppgifterna gjorde klart att det var ett ”insiderjobb”.

Grov stöld/grovt häleri: Trafikuppgifter från en misstänkts telefon ledde till att ett nätverk av personer som utförde inbrott ”på beställning” kunde identifieras. Dessutom kunde ”hälericentralen” lokaliseras.

Grovt rån: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter.

Utpressning (grovt brott): Vid utredning av annat brott kunde det genom trafikuppgifter klarläggas att det pågick en utpressning, som inte var anmäld till polisen. Gärningsmannen kunde identifieras. I ett annat fall kunde gärningsmännen identifieras genom trafikuppgifter som tillkommit i samband med överlämnandet av pengar.

Mordbrand: Vid mordbränder mot flera restauranger har gärningsmän identifierats och knutits till varandra och till platser genom trafikuppgifter.

Grovt narkotikabrott: Gärningsmän har identifierats och knutits till varandra och till platser (t.ex. gömställen) genom trafikuppgifter.

Grov narkotikasmuggling: Genom trafikuppgifter kunde tullen binda telefoner till misstänkta personer och se hur dessa hade rört sig, vilka de haft kontakt med och när kommunikationen ägt rum. Uppgifterna kunde användas för att få hemlig teleavlyssning, som i sin tur användes framgångsrikt för att identifiera misstänkta personer, smugglingsvägar och tidpunkter för smugglingar. Trafikuppgifterna var också avgörande i det internationella samarbetet. – Genom trafikuppgifter rörande ett s.k. anonymt kontantkort, som användes för att ringa till en kurirs telefon, kunde sex gärningsmän och ett gömställe identifieras. Dessutom kunde nästa smugglingsparti tas i beslag och tidigare smugglingsresor klarläggas. – Vid en smugglingsresa kunde inte bara kuriren utan även personer i en följebil knytas till smugglingen med hjälp av trafikuppgifter.

Grovt skattebrott m.m.: Gärningsmän har identifierats och knutits till varandra och till platser. Följande typexempel kan nämnas vid grovt skattebrott och grova förmögenhetsbrott. En huvudman som inte vill synas utåt beordrar vissa personer att göra olika saker. Tillgången till trafikuppgifter leder till att man kan visa att huvudmannens telefon vid vissa tidpunkter haft kontakt med någon annan misstänkts telefon. Utifrån flera sådana uppgifter kan man sedan se mönster om att kontakt funnits vid intressanta tidpunkter, t.ex. vid penninguttag. Uppgifterna kan indikera att den annars osynlige huvudmannen är den som styr aktiviteten. Ett flertal samtal, som varar längre än försumbar tid, kan inte förklaras som felringningar. Det kan också vara värdefullt att få tillgång till lokaliseringsinformation för att t.ex. visa att personer träffats. Ofta kan den sortens information kombineras med fysisk spaning. Uppgifterna kan användas för att försöka påvisa att personer som påstår sig ha haft kontakt med varandra i vart fall inte har haft kontakt som visar sig genom trafikuppgifter. Trafikuppgifter visar också det motsatta, att personer har varit i kontakt med varandra och när det skedde.

Som framgår är ett viktigt användningsområde för uppgifter enligt 6 kap. 22 § första stycket 3 LEK att identifiera gärningsmän. Särskilt i de inledande skedena av utredningar rörande grova brott saknas ofta skäligen misstänkta personer. Därför är det inte möjligt att i de lägena få tillstånd till hemlig teleövervakning eftersom en förutsättning för den åtgärden är att det går att peka ut en person som skäligen misstänkt. Det kravet finns inte i lagen om elektronisk kommunikation.

BRU beskrev hur arbetet med uppgifter kunde se ut i ett inledningsskede av en utredning (SOU 2005:38 s. 323 ff.). Uppgifterna används i princip i varje utredning rörande grova brott, som mord,

människorov, grovt rån, grov mordbrand, allmänfarlig ödeläggelse (t.ex. bankboxsprängningar), grov våldtäkt, människohandel för sexuella ändamål, grovt barnpornografibrott och grovt narkotikabrott samt brott som faller inom Säkerhetspolisens område, exempelvis terroristbrott. Arbetet med att utreda grövre brottslighet inleds ofta med en kontroll av de uppgifter om elektronisk kommunikation som har genererats i anslutning till en brottsplats eller annan plats och sådana uppgifter som kan knytas till en målsägande eller en eventuell misstänkt person. Det krävs många gånger ett relativt omfattande arbete för att få fram vilka av dessa uppgifter som över huvud taget kan vara intressanta i utredningen. I utredningsarbetet kan polisen på olika sätt ”lägga pussel” med uppgifterna, kanske sammanställda med annan information, t.ex. uppgifter från vittnen och informatörer, och på så sätt få fram vilka personer som kan misstänkas för brottsligheten samt när, var och hur brottet planerades och genomfördes och vad gärningsmännen gjorde därefter. Genom kontakterna och intensiteten i kontakterna mellan särskilda mobiltelefoner, som senare kanske kan knytas till bestämda individer, blir det möjligt att klarlägga hur gärningsmännen har agerat och vilka personer som har varit inblandade i brottsligheten. Dessutom kan uppgifterna i många fall resultera i att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans.

När det gäller planeringsskedet är det genom tillgång till uppgifter om elektronisk kommunikation möjligt att ta reda på t.ex. hur gärningsmännen sammanträffade och hur de rekognoserade vid gömställen, längs flyktvägar och vid brottsplatsen samt hur de införskaffade brottsverktyg och stal flyktbilar. Uppgifterna kan som sagt också klarlägga skeenden inte enbart vid själva brottstillfället utan även vid flykten. Det sistnämnda kan bl.a. leda till att gärningsmännens kontakter med varandra blir utredda, att gömställen upptäcks, eventuellt medan gärningsmännen fortfarande befinner sig på platsen, att stulna pengar, flyktbilar eller annat gods påträffas liksom att bortförda personer eller döda kroppar hittas.

Att det saknas en skäligen misstänkt person kan enligt uppgift till BRU från Rikskriminalpolisen sägas vara det normala utgångsläget i utredningar av Internetrelaterad brottslighet. Möjligheten att uppträda anonymt och t.ex. knyta anonyma kontakter är mycket stor, exempelvis via olika chattjänster. Gärningsmän kan alltså få kontakt med tilltänkta brottsoffer utan att röja sin identitet. Ett sådant tillvägagångssätt har enligt polisen observerats bl.a. i

våldtäkts- och mordfall. Ett gott utredningsresultat vid brott där anonyma kontakter har knutits via Internet bygger till stor del på att polisen får tillgång till historiska uppgifter om elektronisk kommunikation, eftersom de uppgifterna är det enda som kan länka samman målsäganden och gärningsmannen. Möjligheten att vara anonym på Internet ger också problem vid utredning av andra typer av brott, där det i första hand inte är fråga om att knyta samman en målsägande och en gärningsman utan där Internet används som ett annat verktyg vid brottsligheten. Det har också då enligt uppgift från polisen mycket stor betydelse att de brottsbekämpande myndigheterna får tillgång till uppgifter om exempelvis det IP-nummer som var aktuellt vid ett visst tillfälle, för att kunna gå vidare i utredningarna och t.ex. identifiera en skäligen misstänkt person.

BRU framhöll också den kraftigt ökade användningen av kryptering vilket medför att betydelsen av tillgång till uppgifter om elektronisk kommunikation i brottsbekämpningen ökar, eftersom krypteringen i princip innebär att myndigheterna inte kommer åt innehållet i meddelanden genom hemlig teleavlyssning. BRU tog också upp att tillgång till uppgifter om elektronisk kommunikation i Sverige är helt nödvändig även i det internationella samarbetet mellan brottsbekämpande myndigheter.

BRU:s uppfattning var mot den bakgrunden att om bestämmelsen i 6 kap. 22 § första stycket 3 LEK upphävs måste hemlig teleövervakning enligt rättegångsbalken få användas även i fall där det saknas en skäligen misstänkt person (SOU 2005:38 s. 193 ff.). I annat fall skulle enligt BRU effektiviteten i den brottsbekämpande verksamheten försämras kraftigt. BRU föreslog därför att hemlig teleövervakning skulle få användas även om det inte finns någon som är skäligen misstänkt för brottet. Dock skulle det i sådana situationer vara möjligt att använda hemlig teleövervakning enbart vid utredning angående brott som är så allvarliga att de kan ligga till grund för hemlig teleavlyssning, dvs. som huvudregel ska det finnas föreskrivet minst två års fängelse för brottet. På så sätt skulle en bra överensstämmelse nås med den reglering som föreslogs bli upphävd i lagen om elektronisk kommunikation.

5.4 Beredningen av BRU:s förslag i SOU 2005:38

5.4.1 Upphävande av 6 kap. 22 § första stycket 3 LEK

Flertalet remissinstanser, däribland *JO*, *Domstolsverket*, *flera brottsbekämpande myndigheter och Juridiska fakultetsstyrelsen vid Lunds universitet*, tillstyrkte eller hade inte några invändningar mot förslaget om att upphäva bestämmelsen i 6 kap. 22 § första stycket 3 LEK och låta de brottsbekämpande myndigheternas tillgång till uppgifterna uteslutande regleras i rättegångsbalken.

Rikspolisstyrelsen anförde att uppgifter enligt den aktuella bestämmelsen i lagen om elektronisk kommunikation inte enbart begärs under förundersökningar utan att regeln också används inom ramen för kriminalunderrättelseverksamhet som gäller misstankar om brottslighet med minst två års fängelse i straffskalan (jfr uttrycket i 6 kap. 22 § första stycket 3 LEK). Rikspolisstyrelsen menade att polisens möjlighet att få tillgång till uppgifterna utanför en förundersökning måste bibehållas och skrev i sitt remissvar bl.a. att polisen ställer om sin verksamhet mot en underrättelsestyrd process där en bred kunskap om brottslighet förväntas ligga till grund för prioriteringar och planerade insatser inom hela polisverksamheten. Rikspolisstyrelsen angav vidare att i underrättelsearbetet inhämtas uppgifter om kriminella företeelser och personer relaterade till såväl konkreta och inträffade brottsliga handlingar som till förhållanden där en konkret misstanke ännu inte finns. Efter bearbetning och analys delges kriminalunderrättelsetjänstens produkt som underlag för strategiska och operativa beslut. Omställningen är, menade Rikspolisstyrelsen, delvis en följd av polisens resurssituation och kravet att prioritera i brottsbekämpningen men har också sin grund i att många brottstyper sällan anmäls till polisen. I stället måste brottet, för att kunna utredas och lagföras, uppdagas av polisen själv genom en fungerande kriminalunderrättelseverksamhet. Exempel på sådana brottstyper är narkotikabrott, människohandel för sexuella ändamål och till viss del även barnpornografibrott.

Flera remissinstanser hade synpunkter på BRU:s förslag om att rättegångsbalkens krav på domstolsprövning som huvudregel skulle gälla i de aktuella ärendena och möjligheten för åklagare att ge interimistiska tillstånd. *Hovrätten för Västra Sverige* menade att det är tveksamt om det är rimligt att belasta domstolarna med en så stor mängd ärenden (uppskattningen vid den tiden var drygt 4 000 ärenden årligen) och att besluten i vart fall bör kunna överlåtas till

åklagare. *Åklagarmyndigheten* menade att det, vid en avvägning mellan det förhållandevis lindriga integritetsintrånget samt den fördröjning av utredningsarbetet som domstolsförfarandet innebär och de ökade kostnader som uppstår, inte är rimligt med en domstolsprövning. Även *Rikspolisstyrelsen* var tveksam till domstolsprövning och hade uppfattningen att prövningen skulle leda till att den brottsbekämpande verksamheten blev mindre effektiv. Styrelsen angav att det inte har förekommit anledning att tro att de befintliga reglerna har lett till någon integritetsskada eller brist i rättssäkerhetshänseende och att ett domstolsförfarande skulle leda till en inte oväsentlig utökning av arbetsbördan för polis, åklagare och domstol samtidigt som polisens arbete skulle fördröjas. *Säkerhetspolisen* ansåg att polisiära förundersökningsledare borde kunna få fatta interimistiska beslut. *Justitiekanslern* ansåg att en interimistisk beslutanderätt för åklagare bör förbehållas brott med straffminimum på fyra års fängelse. *JO*, *Sveriges Advokatsamfund och Sundsvalls tingsrätt* avstyrkte förslaget om att åklagare skulle kunna fatta interimistiska beslut och förordade att man i stället organiserar domstolsverksamheten så att prövningen kan göras inom kortare tid.

5.4.2 Tillgång till uppgifter om abonnemang

De remissinstanser som yttrade sig särskilt i frågan tillstyrkte eller hade inte några invändningar mot BRU:s förslag om att de brottsbekämpande myndigheterna ska ha rätt att få del av abonnemangsuppgifter vid misstanke om brott utan den begränsning som finns i dag om att misstanken ska röra brott av viss svårhetsgrad. Flera remissinstanser, t.ex. *Svenska Antipiratbyrån*, påtalade att polisens tillgång till IP-nummer ofta är av stor betydelse i brottsutredningar som rör upphovsrättsbrott.

5.4.3 Tillgång till uppgifter utan att det finns en skäligen misstänkt person

Ingen remissinstans avstyrkte BRU:s förslag om att hemlig teleövervakning ska få användas vid kvalificerat allvarlig brottslighet, som huvudregel brott för vilket minst två års fängelse är föreskrivet, även om det inte finns någon som är skäligen misstänkt för brottet. Bland de remissinstanser som yttrade sig särskilt över förslaget hade *JO* inte några invändningar medan *Stockholms tingsrätt*

ansåg att förslaget borde analyseras mer utifrån Europakonventionens krav på förutsebarhet och klarhet. *Åklagarmyndigheten* ansåg att förslaget bör genomföras men att kravet på brottets svårhetsgrad ska vara detsamma som när det finns en skäligen misstänkt person (dvs. som huvudregel minst sex månaders fängelse i straffskalan). *Tullverket* menade att det bör övervägas en bestämmelse om att syftet med åtgärden ska vara att få fram någon som är skäligen misstänkt för brottet och att övervakningen ska avbrytas när man nått dit.

5.5 Uppdraget för den här utredningen

Frågan om de brottsbekämpande myndigheternas användning av 6 kap. 22 § första stycket 3 LEK för att få tillgång till uppgifter som angår särskilda elektroniska meddelanden inom ramen för underrättelseverksamheten behandlades inte av BRU.

Regeringen konstaterar i den här utredningens huvuddirektiv (Dir. 2007:185, se bilaga 1) att det finns ett operativt behov av att få tillgång till uppgifterna för att kartlägga brottslig verksamhet och i övrigt arbeta brottsförebyggande. Regeringen anger att bl.a. polisens och tullens underrättelseverksamhet har genomgått stora förändringar under senare år och att det mot den bakgrunden kan ifrågasättas om den aktuella bestämmelsen numera är ändamålsenligt utformad samtidigt som det inte är tillfyllest att ersätta bestämmelsen med en reglering i rättegångsbalken (eftersom en sådan enbart skulle träffa förundersökningssituationer). Utredningen har därför enligt regeringen att utgå från att 6 kap. 22 § första stycket 3 LEK ska ersättas med en annan lagreglering. I samband med ett sådant förslag blir det också nödvändigt att ersätta den nuvarande möjligheten att hämta in uppgifterna under förundersökningar innan det finns en skäligen misstänkt person med annan reglering.

Regeringen konstaterar i huvuddirektiven även att det i underrättelseverksamheten kan finnas behov av att få tillgång till uppgifter om abonnemang (6 kap. 22 § första stycket 2 LEK) och att utredningen i den delen ska utgå från att det ska vara möjligt för de brottsbekämpande myndigheterna att få tillgång till sådana uppgifter, inklusive uppgift om vem som har haft ett visst IP-nummer vid ett visst tillfälle, även vid misstanke om brott som i det konkreta fallet bör föranleda ett bötesstraff. Enligt regeringen ska med andra ord den begränsning som finns i dag om att brottet i det enskilda fallet kan föranleda annan påföljd än böter tas bort.

6 Överväganden och förslag

6.1 Allmänna utgångspunkter

Bedömning: Det bör göras skillnad mellan inhämtning av uppgifter om elektronisk kommunikation i förundersökning respektive underrättelseverksamhet, eftersom de principer och mål som styr respektive verksamhet är olika. Även behovet av att skydda integriteten gör sig gällande på olika sätt.

6.1.1 Allmänt

Inhämtning och bearbetning av uppgifter om elektronisk kommunikation är ett allt viktigare verktyg för de brottsbekämpande myndigheterna såväl i underrättelseverksamhet som i det brottsutredande arbetet. Samtidigt har elektronisk kommunikation ett starkt skydd i både regeringsformen och Europakonventionen. Den omfattas av skyddet rörande privat- och familjeliv och korrespondens i artikel 8 i Europakonventionen och skyddet mot undersökning av förtroligt meddelande i 2 kap. 6 § regeringsformen.

En grundläggande utgångspunkt för de förslag som lämnas i det följande är att de inte bara ska syfta till att upprätthålla en effektiv brottsbekämpande verksamhet utan även till att förstärka och bygga ut rättssäkerheten och integritetsskyddet vid inhämtning av uppgifter om elektronisk kommunikation.

6.1.2 Förundersökning

De principer som styr och de målsättningar som gäller för underrättelseverksamhet respektive förundersökning ser olika ut.

Under förundersökningen är syftet främst att utreda ett redan begånget brott och i det sammanhanget klarlägga vem eller vilka som skäligen kan misstänkas för brottet. Förundersökningen syftar således redan i inledningsskedet till att utreda vem som är gärningsman. De som berörs av ett beslut om inhämtning av uppgifter om elektronisk kommunikation under en förundersökning kan således komma att misstänkas för delaktighet i brottet och, åtminstone så småningom, som misstänkta och åtalade inta partsställning och få rätt till partsinsyn i det material som åberopas mot dem. Inhämtningen av uppgifter sker mot denna bakgrund mera riktat mot personer som kan vara aktörer i samband med brottet. Det är partsintresset som här är styrande för vilka principer som bör bära upp regelsystemet. Det innebär att också integritetsaspekten under förundersökningen främst tar sikte på den övervakade personen som potentiell part. De principer som styr inhämtningen bör därför så långt det är möjligt anknyta till de rättssäkerhetsprinciper som gäller för den som är skäligen misstänkt. Utgångspunkten bör därför vara att tillämpa det ordinära regelsystemet för hemlig teleövervakning enligt rättegångsbalken så långt detta är möjligt och för förundersökningar i första hand överväga vilka ändringar som bör göras i detta regelsystem. Karakteristiskt för detta kan sägas vara tvåpartsförhållandet, insyn i det material som åberopas mot personen och relativt vittgående möjligheter till rättslig prövning av olika beslut. Den rättsliga prövningen är ofta inriktad på frågan om tillräckliga skäl föreligger för att vidta en integritetskänslig åtgärd. Det är en riktad inhämtning som lämpar sig väl för att prövas av ordinära rättsliga organ.

6.1.3 Underrättelseverksamhet

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 verksamhet för att förebygga eller förhindra att brottsligheten genomförs.

Inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpningen utgör ett 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. Den som berörs av ett beslut om inhämtning är en del av ett större sammanhang, men så länge som informationen inte används riktat mot honom eller henne och förs över till en förundersökning finns det inte skäl att behandla denne som en potentiell part, utan som en medborgare som i och för sig blir föremål för integritetskänsliga åtgärder. Därmed är inte sagt att integritetsaspekten skulle vara mindre framträdande. Från vissa utgångspunkter är integritetsskyddet i stället snarare viktigare i en situation som denna, där den som utsätts för en integritetskänslig åtgärd saknar de rättssäkerhetsgarantier som normalt är förknippade med en partsställning. Men det är den utsatte personen som medborgare som är i fokus när det gäller att bedöma hur integritetsintresset ska kunna tillgodoses. Det framåtblickande perspektivet i underrättelseverksamheten gör att domstolsprövning inte är lika naturligt som vid en tillbakablickande bedömning när ett brott redan har begåtts och där prövningen kan knytas till en historisk händelse. Av det skälet måste frågor om parlamentarisk insyn och kontroll samt tillsynsverksamhet av oberoende organ ges en helt annan betydelse i det sammanhanget. Det blir också styrande för vilka principer som bör gälla för underrättelseverksamheten. En informationsinhämtning i underrättelseverksamheten ställer särskilda krav på kontinuerlig kontroll och uppföljning av verksamhetens lagenlighet och lämplighet.

Det som sagts innebär att underrättelseverksamheten bör behandlas separat och regleras i särskild ordning. Om information förs över från underrättelseverksamhet till förundersökning finns det däremot skäl att låta partsintresset få genomslag. Användningen av en sådan överförd information bör behandlas inom samma regelsystem som gäller för förundersökningar i övrigt, dvs. prövas inom ramen för ett reformerat förfarande med hemlig teleövervakning.

6.2 Tydliga och rättssäkra befogenheter för utfående av uppgifter om elektronisk kommunikation

Förslag: Bestämmelsen om tillgång till uppgifter om elektronisk kommunikation i 6 kap. 22 § första stycket 3 LEK ska upphävas.

I förundersökningar ska uppgifter om elektronisk kommunikation kunna inhämtas från leverantörerna enbart efter beslut om hemlig teleövervakning.

I underrättelseverksamhet ska befogenheter att inhämta uppgifter från leverantörerna tas in i en ny lag om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

6.2.1 Upphävande av regleringen i lagen om elektronisk kommunikation

Det är möjligt för de brottsbekämpande myndigheterna att få tillgång till uppgifter om elektronisk kommunikation enligt såväl rättegångsbalken som lagen om elektronisk kommunikation. Det ska för tydlighetens skull nämnas att de uppgifter utredningen behandlar inte rör uppgifter som kan inhämtas från trådlös kommunikation, som radio- och satellitkommunikation, eftersom etern under lång tid har ansetts vara fri (jfr 6 kap. 17 § andra stycket 3 LEK).

Bestämmelsen i 6 kap. 22 § första stycket 3 LEK ställer som enda krav för att uppgifterna ska få hämtas in, att misstanken rör brottslighet av viss svårhetsgrad. Vid en jämförelse med hemlig teleövervakning enligt rättegångsbalken, som ger de brottsbekämpande myndigheterna tillgång till i stort sett samma uppgifter, saknas det i lagen om elektronisk kommunikation bestämmelser t.ex. om formerna för tillståndsgivningen, om krav på synnerlig vikt för utredningen, om hur överskottsinformation får användas, om underrättelseskyldighet till enskild och om särskild tillsyn av Säkerhets- och integritetsskyddsnämnden.

Utredningen menar mot den bakgrunden att den nu gällande regleringen i 6 kap. 22 § första stycket 3 LEK inte i tillräcklig grad uppfyller de krav på rättssäkerhet och integritetsskydd som måste finnas vid det här slaget av integritetskänsliga åtgärder och att den därför ska upphävas.

En utgångspunkt för utredningens arbete är att de förslag som läggs ska bibehålla en effektiv brottsbekämpande verksamhet. När bestämmelsen i 6 kap. 22 § första stycket 3 LEK upphävs måste den därför ersättas med befogenhetsbestämmelser i annan lagstiftning som samtidigt uppfyller de utökade kraven på rättssäkerhet och integritetsskydd.

6.2.2 Förundersökning

Utredningens uppdrag är att föreslå en reglering som ersätter den aktuella bestämmelsen i lagen om elektronisk kommunikation och som är tillämplig dels under förundersökning innan det finns någon skäligen misstänkt person, dels i underrättelseverksamhet.

Rättegångsbalkens regler om straffprocessuella tvångsmedel, däribland hemlig teleövervakning, är uteslutande begränsade till brottsutredningsverksamhet. Det är därför inte lämpligt att i rättegångsbalken föra in bestämmelser som ska tillämpas i underrättelseverksamheten. Detta framgår också av direktiven till utredningen och är dessutom i linje med de allmänna utgångspunkterna (se avsnitt 6.1).

Frågan blir då om den reglering som ska ersätta bestämmelsen i 6 kap. 22 § första stycket 3 LEK under förundersökning innan det finns någon skäligen misstänkt person passar att föra in i rättegångsbalken. I dag är det möjligt att använda vissa av rättegångsbalkens straffprocessuella tvångsmedel under en förundersökning, även om det saknas en skäligen misstänkt person. Det som framför allt är av betydelse att nämna här är husrannsakan och kroppsvisitation. Det faktum att det i en förundersökning saknas en skäligen misstänkt person är alltså inte i sig något som principiellt hindrar att bestämmelserna placeras i rättegångsbalken. Det som då bör övervägas är förändringar i de nuvarande reglerna om hemlig teleövervakning.

För att hemlig teleövervakning ska få användas krävs att det finns en skäligen misstänkt person mot vilken åtgärden riktas. I det avseendet skulle bestämmelserna om hemlig teleövervakning behöva förändras. Hemlig teleövervakning får enbart avse vissa teleadresser med särskild anknytning till den skäligen misstänkte. Det är med andra ord inte möjligt enligt rättegångsbalken att använda basstationstömning, något som också skulle behöva förändras. Beslut om hemlig teleövervakning fattas av domstol. För att

kunna möta de behov som finns i brottsbekämpningen av att bl.a. snabbt få tillgång till uppgifter om elektronisk kommunikation skulle rättegångsbalkens bestämmelser om att enbart domstol fattar beslut också behöva förändras. I dag krävs misstanke om brott med minst två års fängelse i straffskalan för att de brottsbekämpande myndigheterna ska få tillgång till uppgifter enligt 6 kap. 22 § första stycket 3 LEK, medan det som huvudregel krävs minst sex månaders fängelse i straffskalan vid hemlig teleövervakning. Även i den delen kan det behövas en särskild reglering i rättegångsbalken för situationer när det saknas en skäligen misstänkt person.

Att det behöver ske förändringar i bestämmelserna om hemlig teleövervakning i förhållande till vad som gäller i dag när tvångsmedlet enbart reglerar situationer när det finns en skäligen misstänkt person är inte en nackdel. Det framstår som mer lämpligt än att lägga bestämmelserna utanför rättegångsbalken, något som skulle kunna innebära att karaktären av dubbelreglering i förhållande till balken består.

Utredningen har kommit fram till att i förundersökningar ska uppgifter om elektronisk kommunikation kunna inhämtas från leverantörerna enbart genom en tillämpning av rättegångsbalkens regler om hemlig teleövervakning. Det behöver därför övervägas hur bestämmelserna om det tvångsmedlet behöver kompletteras.

6.2.3 Underrättelseverksamhet

Frågan blir därefter var den reglering som avser underrättelseverksamhet ska finnas.

Enligt 20 § lagen om särskild utlänningskontroll får domstol ge tillstånd till hemlig teleövervakning, om det är av betydelse för att utröna om en viss utlänning eller en organisation eller grupp som han tillhör eller verkar för planlägger eller förbereder terroristbrott. Att förutsättningarna för lagens tillämpning på det sättet är knutna till en viss utlänning gör att den reglering utredningen har i uppdrag att föreslå inte passar att föra in i lagen om särskild utlänningskontroll.

Lagen om åtgärder för att förhindra vissa särskilt allvarliga brott innehåller också regler om hemlig teleövervakning i ett skede innan en förundersökning har inletts. Syftet med lagen är att förebygga och förhindra att allmänfarliga brott, brott mot rikets säkerhet och terroristbrott begås. Lagen gäller även vissa andra brott, som mord

och människorov, om det finns särskild anledning att anta att avsikten med brottet är att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd. Framför allt med hänsyn till att den aktuella lagen har kommit att tillämpas i situationer mycket nära inpå att en förundersökning kan inledas, att den enbart rör vissa särskilt uppräknade brott, som främst faller under Säkerhetspolisens ansvarsområde, och att det enligt lagen krävs särskild anledning anta att en viss person kommer att utöva den brottsliga verksamheten, är det inte ändamålsenligt att föra in bestämmelserna som ska ersätta 6 kap. 22 § första stycket 3 LEK i den lagen.

Ett annat alternativ skulle kunna vara att föra in regleringen i polislagen. Där finns bestämmelser om bl.a. polisverksamhetens ändamål och uppgifter samt om principer vid polisingripanden, rapporteringsskyldighet och vissa befogenheter (t.ex. våldsanvändning, omhändertaganden, avlägsnanden, kroppsvisitation av säkerhetsskäl och husrannsakan för att söka personer som ska omhändertas). Många bestämmelser rör ordningspolisverksamheten, att ge service, skydd och verka brottsförebyggande. Vid lagens tillkomst var en av utgångspunkterna att bestämmelserna i rättegångsbalken om förundersökningsförfarandet och särskilda befogenheter under detta, t.ex. tvångsmedelanvändning i brottsutredande syfte, inte skulle finnas i polislagen. Den reglering utredningen har i uppdrag att föreslå rör en åtgärd som ger tillgång till i princip samma uppgifter som vid hemlig teleövervakning enligt rättegångsbalken. Regleringen hör inte hemma i polislagen.

Utredningen bedömer mot denna bakgrund att det är mest lämpligt att befogenheterna att inhämta uppgifter från leverantörerna regleras särskilt och tas in i en ny lag om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

6.3 Hemlig teleövervakning i förundersökningar

6.3.1 När ska inhämtning få ske?

Förslag: Hemlig teleövervakning avseende historiska uppgifter ska få användas när det saknas en skäligen misstänkt person. Det ska krävas att åtgärden är av synnerlig vikt för utredningen och

att syftet är att fastställa vem som skäligen kan misstänkas för brottet eller utröna annan omständighet av väsentlig betydelse för utredningen.

Ett strängare krav ska gälla än när det finns en skäligen misstänkt person för att tvångsmedlet ska få användas i ett sådant tidigt skede i en förundersökning. Misstanken ska röra brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff, eller annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Syfte och krav på åtgärden

Nuvarande reglering

Hemlig teleövervakning får enligt 27 kap. 20 § RB användas endast när det i en förundersökning finns en skäligen misstänkt person. När bestämmelsen i 6 kap. 22 § första stycket 3 LEK upphävs ska uppgifter om elektronisk kommunikation i förundersökningar kunna inhämtas enbart med tillämpning av regelsystemet för hemlig teleövervakning. Det finns inget krav i 6 kap. 22 § första stycket 3 LEK att det ska finnas en skäligen misstänkt person i utredningen. Tvärtom saknas det ofta en skäligen misstänkt person när uppgifter om elektronisk kommunikation inhämtas enligt den bestämmelsen (se avsnitt 4.2).

Utredningens bedömning

När regeln i 6 kap. 22 § första stycket 3 LEK upphävs blir det, för att kunna upprätthålla en effektiv brottsbekämpning, nödvändigt att möjliggöra att hemlig teleövervakning avseende historiska uppgifter får användas även när det ännu inte finns en skäligen misstänkt person. Utredningen föreslår därför en sådan reglering.

Med uttryckssättet att det ännu inte finns en skäligen misstänkt person menas att åtgärden inte omfattar teleadresser med sådan koppling till en skäligen misstänkt som avses i 27 kap. 20 § första stycket RB. Om det finns en skäligen misstänkt person ska det inte

finnas något hinder mot hemlig teleövervakning för att t.ex. utreda även andra personers eventuella brottsliga verksamhet.

Hemlig kameraövervakning kan i visst fall få ske även om det saknas en skäligen misstänkt person. Syftet ska då enligt 27 kap. 20 c § RB vara att fastställa vem som skäligen kan misstänkas för brottet.

Utredningen föreslår att hemlig teleövervakning som används när det inte finns en skäligen misstänkt person på samma sätt ska syfta till att fastställa vem som är skäligen misstänkt. Även andra syften med åtgärden bör dock finnas. Det ska uttryckas så att syftet är att utröna annan omständighet av väsentlig betydelse för utredningen. Det kan t.ex. handla om att fastställa var en målsägande eller ett vittne har befunnit sig eller var en brottsplats är belägen. Åtgärder kan behöva vidtas med dessa syften oavsett om det finns någon som skäligen kan misstänkas för brottet eller inte och kan, liksom i andra fall, bl.a. leda till att misstankarna mot någon person stärks eller att en tidigare misstänkt person avförs från utredningen.

Oavsett om syftet är att fastställa vem som skäligen kan misstänkas för brottet eller att utröna annan omständighet av väsentlig betydelse för utredningen, ska det krävas att åtgärden som sådan är av synnerlig vikt för utredningen. Med det avses att situationen ska göra användningen av åtgärden nödvändig. Uppgifterna ska i princip inte kunna inhämtas med andra medel och det ska finnas skäl att räkna med att tvångsmedelsanvändningen ensam eller i förening med andra åtgärder verkligen kan få effekt.

Vid beslut om och användning av tvångsmedel gäller proportionalitetsprincipen. Den brukar i korthet beskrivas så att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med den. Principen har, när det gäller hemlig teleövervakning, uttryckts i 27 kap. 1 § RB och kommer att gälla även för situationer där åtgärden vidtas med de syften som nyss har angetts.

Det förhållandet att de situationer som nyss har nämnts kommer att omfattas av hemlig teleövervakning medför ökade rättssäkerhetsgarantier för den enskilde. Omständigheterna i det enskilda fallet måste konstateras vara sådana att kravet på synnerlig vikt är uppfyllt och att ett genomförande av åtgärden är proportionerlig. Till detta kommer de förslag på förstärkning av rättssäkerheten som utredningen presenterar nedan särskilt vad gäller beslutande-

rätt, underrättelse till enskild och tillsynen över de brottsbekämpande myndigheternas verksamhet.

Brottslighetens svårhetsgrad

Nuvarande reglering

Frågan blir därefter vad en misstanke om brott ska röra för att hemlig teleövervakning ska få användas i en förundersökning med syfte att fastställa vem som skäligen kan misstänkas för brottet m.m.

Enligt 27 kap. 19 och 20 §§ RB får hemlig teleövervakning användas när det finns en skäligen misstänkt person och förundersökningen avser ett brott för vilket det inte är förskrivet lindrigare straff än sex månaders fängelse eller avser dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling eller försök, förberedelse eller stämpling till sådant brott. För att de brottsbekämpande myndigheterna ska få inhämta motsvarande uppgifter enligt 6 kap. 22 § första stycket 3 LEK krävs att det finns misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Detta innebär bl.a. att inga försöks-, förberedelse- eller stämplingsbrott omfattas av bestämmelsen i lagen om elektronisk kommunikation. Det betyder t.ex. att ett grovt rån mot en bank eller en värdetransport som misslyckas i den meningen att gärningsmännen inte får med sig något av värde, inte omfattas av regleringen. Detsamma gäller t.ex. fall av oprovocerat gatuvåld som är så allvarligt att det bedöms som försök till mord. Myndigheterna kan i ett sådant läge inte få uppgifter om elektronisk kommunikation förrän man har identifierat en skäligen misstänkt person och genomfört hemlig teleövervakning enligt rättegångsbalken.

Utredningens bedömning

Under utredningens arbete har det framkommit att det finns ett stort behov i den brottsbekämpande verksamheten av att få del av uppgifter om elektronisk kommunikation i förundersökningar rörande mindre allvarlig brottslighet, t.ex. olaga hot som har skett via mobiltelefon av okänd gärningsman. Myndigheterna har bl.a. mot den bakgrunden menat att de brott som skulle ge rätt till hem-

lig teleövervakning i syfte att fastställa vem som skäligen kan misstänkas för brottet m.m. borde vara desamma som i de fall när en skäligen misstänkt person finns, dvs. som utgångspunkt brott med minst sex månaders fängelse i straffskalan (jfr olaga hot, grovt brott enligt 4 kap. 5 § andra stycket brottsbalken).

Utredningen kan konstatera att det finns en mängd brott, i vissa fall till och med grova sådana, som skulle ges mycket större förutsättningar att bli uppklarade om de brottsbekämpande myndigheterna gavs möjlighet att få del av uppgifter om elektronisk kommunikation i utredningarna. Det är dock enligt utredningens uppfattning påkallat av integritetsskäl att begränsa myndigheternas tillgång till de aktuella uppgifterna i förhållande till vad som gäller för samma tvångsmedel när det finns en skäligen misstänkt person. En rimlig nivå i det sammanhanget är att tillåta hemlig teleövervakning vid brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, dvs. brott som ger möjlighet att använda det klart mer integritetskänsliga tvångsmedlet hemlig teleavlyssning mot en skäligen misstänkt person. Dessa brott omfattas i dag av regleringen i 6 kap. 22 § första stycket 3 LEK. Det bör dock ske en viss utvidgning i förhållande till hur den sistnämnda bestämmelsen är utformad. Det finns ett stort behov i brottsbekämpningen av tillgång till uppgifter även om brottet inte har kommit till fullbordan. Det kan t.ex. röra sig om förberedelse till grova rån av värdetransporter där åtgärden kan innebära att myndigheterna får möjlighet att förhindra att brotten fullbordas. Även vid brott vars straffvärde överstiger fängelse i två år bör möjligheten till hemlig teleövervakning finnas. Det sistnämnda rör exempelvis rån som inte kan kvalificeras som grova. Intresset av att skydda integriteten hindrar inte en sådan reglering, särskilt som brottslighetens svårhetsgrad vid hemlig teleövervakning i dessa fall kommer att bli densamma som för hemlig teleavlyssning (jfr SOU 2005:38).

6.3.2 Vem ska fatta beslut?

Förslag: Åklagare ska få ge interimistiskt tillstånd till hemlig teleövervakning, om det kan befaras att inhämtande av rättens tillstånd skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen.

Har åklagaren gett ett interimistiskt tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I

anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har ett interimistiskt tillstånd till hemlig teleövervakning upphört att gälla innan rätten har prövat ärendet, ska åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Om åtgärden inte kan antas bli av stor omfattning eller av särskilt ingripande slag, ska frågor om hemlig teleövervakning i syfte att fastställa vem som skäligen kan misstänkas för brottet m.m. vid sidan av domstol även få prövas av undersökningsledaren eller åklagaren.

Interimistiskt tillstånd av åklagare

Nuvarande reglering m.m.

Tillstånd till hemlig teleövervakning ges i dag av domstol på ansökan av åklagaren (27 kap. 21 § RB). När åtgärden riktas mot en skäligen misstänkt person ska även fortsättningsvis tillstånd ges av rätten. Främst mot bakgrund av att den nuvarande möjligheten för brottsbekämpande myndigheter att snabbt få tillgång till uppgifter genom lagen om elektronisk kommunikation upphävs är frågan om det finns anledning att införa en rätt för åklagare att ge interimistiskt tillstånd till tvångsmedlet.

I lagen om åtgärder för att utreda vissa samhällsfarliga brott finns ett undantag från regeln om domstolsbeslut (4 §). Där anges att tillstånd till hemlig teleövervakning i de fall som omfattas av lagen får ges av åklagaren om det kan befaras att inhämtande av rättens tillstånd till hemlig teleövervakning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. Det anges också att åklagaren genast ska göra anmälan om åtgärden hos rätten, som skyndsamt ska pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden ska den upphäva beslutet. Skulle däremot åtgärden ha upphört att gälla innan rätten har prövat ärendet, ska åklagaren anmäla ärendet till Säkerhets- och integritetsskyddsnämnden (6 §).

BRU föreslog att en möjlighet för åklagare att ge interimistiskt tillstånd till hemlig teleövervakning skulle införas i rättegångsbalken och motiverade det främst med behovet av snabba avgöranden (SOU 2005:38 s. 200 ff.). Tidigare föreslog även Buggningsutred-

ningen samma sak (SOU 1998:46 s. 414 ff.). Som framgår av avsnitt 5.4.1 rörande beredningen av BRU:s förslag tog bl.a. JO upp frågan om det, som ett alternativ till åklagares interimistiska beslutanderätt, finns anledning att organisera domstolsväsendet så att domstolsprövning kan ske inom kortare tid.

Genom en ändring i 19 kap. 12 § RB, som trädde i kraft den 1 juli 2000, utvidgades de s.k. jourdomstolarnas behörighet till att omfatta beslut om användande av tvångsmedel i brådskande fall (prop. 1999/2000:26, bet. 1999/2000:JuU10). Den nämnda regleringen i rättegångsbalken kompletteras av föreskrifter i förordningen (1988:31) om tingsrätternas beredskap för prövning av häktningsfrågor m.m., där det anges att tingsrätten ska ha beredskap för prövning av frågor som rör bl.a. användning av tvångsmedel under söndag, annan allmän helgdag, lördag och vissa aftnar. Det anges också att beredskap företrädesvis bör fullgöras av ordinarie domare. Ytterligare bestämmelser finns i Domstolsverkets föreskrifter om beredskap vid tingsrätterna för prövning av häktningsfrågor m.m. (DVFS 2007:1). Beredskapen fullgörs genom att domstolen är tillgänglig för beslut vissa tider under dagtid.

Utredningens bedömning

Det är av stor vikt i det brottsbekämpande arbetet att det finns möjlighet att mycket snabbt få tillgång till uppgifter om elektronisk kommunikation. Detta gäller oavsett om det finns en skäligen misstänkt person i förundersökningen eller inte. Snabbheten i förfarandet är en avgörande framgångsfaktor för brottsbekämpningen. Ofta är möjligheten till ”minutoperativa” beslut avgörande för att säkra ett lyckat utredningsresultat. Det gäller särskilt som de personer som sysslar med grov brottslighet många gånger aktivt vidtar åtgärder i syfte att försvåra ett framgångsrikt arbete från myndigheternas sida.

Det är nödvändigt för en framgångsrik brottsbekämpning att tillstånd till hemlig teleövervakning kan ges snabbare än vad som är möjligt vid en domstolsprövning, även med beaktande av domstolarnas beredskapsorganisation. Domstolarna har i och för sig möjlighet att ta om hand brådskande frågor om tvångsmedel, men någon beredskap för omedelbara beslut dygnet runt finns inte. Det är inte heller rimligt att föreslå att en sådan organisation ska byggas

upp för att tillstånd ska kunna ges mycket snabbt under dygnets alla timmar.

Utredningen menar därför att det i rättegångsbalken ska införas en rätt för åklagare att ge interimistiska tillstånd till hemlig teleövervakning mot en skäligen misstänkt person. Hos åklagare finns inte bara kompetensen för uppgiften utan även den tillgänglighet dygnet runt som behövs för att kunna tillgodose brottsbekämpningens behov. Det är mest lämpligt att den ordningen utformas i enlighet med bestämmelserna i lagen om åtgärder för att utreda vissa samhällsfarliga brott. Rätten för åklagare bör därför gälla enbart om det kan befaras att inhämtande av rättens tillstånd skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. Dessutom bör åklagaren genast göra en skriftlig anmälan om åtgärden till rätten och samtidigt ange skälen för åtgärden. Rätten bör ha skyldighet att skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har ett interimistiskt tillstånd till hemlig teleövervakning upphört att gälla innan rätten har prövat ärendet, bör åklagaren vara skyldig att anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Beslutanderätt när syftet är att fastställa vem som skäligen kan misstänkas för brottet m.m.

Behovet av att mycket snabbt få tillgång till uppgifter om elektronisk kommunikation framträder kanske tydligast i de situationer där det saknas en skäligen misstänkt person, vilket ofta är fallet i inledningsskedena av utredningar om grövre brott. Då fattas många gånger flera beslut om inhämtning enligt 6 kap. 22 § första stycket 3 LEK i samma ärende. Det kan ibland vara fråga om minuter mellan besluten. Vid exempelvis ett grovt rån mot en värdetransport kan polisen på mycket kort tid få uppgifter från en basstationstömning rörande platsen för brottet. Polisen kanske också mycket snabbt behöver få nya basstationstömningar gjorda när det t.ex. blir klarlagt vilka flyktvägar rånarna använde sig av eller på vilka platser flyktbilar har lämnats. Därefter är det troligt att ytterligare beslut om att inhämta uppgifter om elektronisk kommunikation behöver fattas för att fortsätta undersökningarna kring de uppgifter som kommit fram genom basstationstömningarna, allt i syfte att identifiera skäligen misstänkta personer.

Det saknas bestämmelser i lag eller förordning om vem som inom polis och tull får fatta beslut om inhämtning enligt 6 kap. 22 § första stycket 3 LEK. JO har dock uttalat att besluten bör underställas förundersökningsledare, som kan vara polisman, tulltjänsteman eller åklagare.

Enligt utredningens mening ska det på samma sätt som i övrigt vid tvångsmedel enligt rättegångsbalken finnas utsagt i lag vem som ska ha behörighet att besluta om hemlig teleövervakning i syfte att fastställa vem som skäligen kan misstänkas för brottet m.m.

Det är naturligt att det är allmän domstol som har rätt att besluta om hemlig teleövervakning även i de nu nämnda fallen. Frågan är om även undersökningsledare och åklagare ska ha den behörigheten, vilket skulle motsvara den rätt som brottsbekämpande myndigheter i dag har att besluta om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 3 LEK. Det som med styrka talar för att undersökningsledare och åklagare bör ha beslutanderätt även i fortsättningen är effektivitetsskälen, dvs. det faktum att det ofta är mycket bråttom att få fram de aktuella uppgifterna och att utredningarnas effektivitet allvarligt skulle försämras med en annan ordning. Åtgärden kommer ofta att sättas in i tidigt skede när det saknas en skäligen misstänkt person. Utredningarna kommer också att avse brottslighet med betydligt högre minimistraff än vad som annars gäller vid hemlig teleövervakning. Utredningen menar att det är en fullt tillräcklig rättssäkerhetsgaranti i de flesta fall att prövningen görs av undersökningsledare eller åklagare.

Till detta kommer att Säkerhets- och integritetsskyddsnämnden i dag har tillsyn över användningen av hemlig teleövervakning men inte direkt över hur myndigheterna inhämtar uppgifter enligt lagen om elektronisk kommunikation. Med utredningens förslag kommer dock nämnden att ha tillsyn över all sådan inhämtning som sker i en förundersökning. En uttrycklig lagreglering om att det är undersökningsledare och åklagare som ska besluta om att hämta in uppgifterna innebär dessutom en klar skärpning i förhållande till dagens regelverk, där befogenheten tillkommer den enskilde polismannen eller tulltjänstemannen.

Sammanfattningsvis innebär detta att utredningens förslag i flera avseenden medför förstärkningar av rättssäkerheten för den enskilde.

En delad beslutanderätt mellan domstol, undersökningsledare och åklagare i fråga om tvångsmedel finns i dag i 28 kap. 4 § RB beträffande husrannsakan. Om den åtgärden kan antas bli av stor

omfattning eller medföra synnerlig olägenhet för den hos vilken åtgärden företas, bör, om det inte är fara i dröjsmål, husrannsakan inte vidtas utan rättens förordnande.

En liknande ordning ska finnas även i nu aktuella fall av hemlig teleövervakning. Det är enbart i de fall där det saknas tunga integritetsintressen som står emot de intressen som åtgärden ska tillgodose som frågor om hemlig teleövervakning ska kunna prövas av annan än domstol. Det bör uttryckas så att när åtgärden inte kan antas bli av stor omfattning eller av särskilt ingripande slag, t.ex. vid känsliga uppgifter, ska beslut få fattas av undersökningsledaren eller åklagaren. Den interimistiska rätt för åklagare att ge tillstånd till hemlig teleövervakning som utredningen föreslår ovan, ska dock gälla även i dessa fall där normalt domstol ska ge tillstånd. Någon fara för effektivitetsförlust i de fallen finns därför inte.

Det är av stor vikt att de beslut som fattas av undersökningsledare och åklagare dokumenteras noggrant för att det ska finnas ett fullgott underlag för den skärpta tillsynsverksamhet som utredningens förslag innebär (se avsnitt 6.9).

6.4 Tillgång till uppgifter om elektronisk kommunikation i underrättelseverksamhet

6.4.1 Inledning

De brottsbekämpande myndigheternas underrättelseverksamhet är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad allvarlig brottslighet har ägt rum, pågår eller kan antas komma att begås. I underrättelseverksamheten samlar myndigheterna in, bearbetar och analyserar uppgifter. Det framtagna underrättelsematerialet kan läggas till grund för t.ex. beslut om att vidta särskilda åtgärder för att förhindra eller upptäcka brott och beslut om att inleda förundersökning. Det finns således behov att i underrättelseverksamheten inhämta och hantera stora mängder information. En bred inhämtning ställer dock stora krav på att det också finns en fungerande kontroll av informationsinhämtningen.

6.4.2 När ska inhämtning få ske?

Förslag: I de brottsbekämpande myndigheternas underrättelseverksamhet ska uppgifter om viss elektronisk kommunikation få hämtas in i en undersökning om det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 4, 5 a första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. olovlig kårverksamhet eller brott mot medborgerlig frihet enligt 18 kap. 4 eller 5 § brottsbalken,
4. spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig under rättelseverksamhet enligt 19 kap. 5, 7, 8 eller 10 § brottsbalken,
5. företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning, eller
6. brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

Inhämtning ska få beslutas och genomföras endast om 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.

Vilken betydelse ska uppgifterna förväntas ha för att de ska få hämtas in?

Nuvarande reglering m.m.

Enligt 19 och 20 §§ lagen om särskild utlänningskontroll får vissa tvångsmedel användas om det är av betydelse för att utröna om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott. Lagen ställer inte upp något krav på brottsmisstanke för att tvångsmedel ska få tillgripas och inte heller något krav på att förundersökning har inletts. Det saknar enligt lagen också betydelse om det finns någon misstanke mot just den person som drabbas av tvångsmedlet, eftersom användningen av detta syftar till att utröna om organisationen eller gruppen som sådan planlägger eller förbereder ett terroristbrott. Med den regleringen som utgångspunkt föreslogs i den promemoria som låg till grund för regeringens proposition om åtgärder för att förhindra vissa särskilt allvarliga brott (Ds 2005:21, prop. 2005/06:177) att tillstånd till tvångsmedel i preventivt syfte skulle få användas, om det med hänsyn till omständigheterna kan antas att någon person, organisation eller grupp som personen tillhör eller verkar för kommer att utöva viss brottslig verksamhet.

I den nyss nämnda propositionen diskuterade regeringen vilken grad av misstanke som borde införas i det som senare blev lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177 s. 54 ff.). Regeringen menade att reglerna som övervägdes behövde snävas in ytterligare jämfört med hur lagen om särskild utlänningskontroll är utformad. Bland annat var det enligt regeringen inte lämpligt att som enda förutsättning för tvångsmedelsanvändningen ställa upp ett krav att tvångsmedlet ska vara av betydelse för att utröna om brottsligheten förbereds. Regeringen uttalade att ett sådant rekvisit skulle göra möjligheten till tvångsmedelsanvändning allt för omfattande. För att snäva in tillämpningsområdet var det enligt regeringen lämpligt att föreskriva någon grad av misstanke. Regeringen bedömde att misstankegraden borde uttryckas på samma sätt som i 23 kap. 1 § RB som reglerar när förundersökning ska inledas, dvs. att det ska finnas ”anledning att anta". Vid riksdagsbehandlingen av propositionen skärptes graden av misstanke så att det i 1 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott numera anges att det ska finnas ”särskild anledning att anta” att en viss person kommer att utöva viss

angiven brottslig verksamhet. Justitieutskottet underströk vikten av att misstanken inte får bygga enbart på spekulationer eller allmänna bedömningar, utan att den ska vara grundad på faktiska omständigheter inom ramen för ett enskilt fall eller händelseförlopp. Enligt utskottet riskerade den av regeringen föreslagna misstankegraden att ge utrymme för en alltför extensiv tillämpning (bet. 2007/08:JuU3 s. 19).

Som nyss nämndes krävs enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott att det finns misstanke om att en *viss person* kommer att utöva brottslig verksamhet.

I den tidigare nämnda promemorian (Ds 2005:21) rörande åtgärder för att förhindra vissa särskilt allvarliga brott föreslogs att det inte skulle krävas att någon misstanke kan riktas mot en viss person för att tvångsmedelsanvändning ska aktualiseras. I stället skulle det vara tillräckligt att en person tillhör eller verkar för en organisation eller grupp som kan misstänkas för att komma att utöva brottslig verksamhet. Förslaget innebar att den preventiva tvångsmedelsanvändningen skulle kunna riktas mot alla medlemmar i en organisation och alla som utan att vara medlemmar verkar för den, utan att någon viss person kan misstänkas för något, bara det kan antas att organisationen kommer att utöva viss brottslighet. Regeringen bedömde dock i propositionen (prop. 2005/06:177 s. 56 f.) att det förslaget var allt för långtgående. Det är, menade regeringen, inte rimligt att t.ex. alla medlemmar i en organisation kan utsättas för den föreslagna tvångsmedelsanvändningen endast på grund av sitt medlemskap. Enligt regeringen talade integritetsintresset för att personkretsen som kan bli föremål för tvångsmedelsanvändningen avgränsas så att det krävs att någon form av misstanke kan riktas mot en person.

I dag gäller att i stort sett samma uppgifter om elektronisk kommunikation kan inhämtas av de brottsbekämpande myndigheterna med stöd av såväl rättegångsbalkens bestämmelser om hemlig teleövervakning som enligt 6 kap. 22 § första stycket 3 LEK. När det gäller förutsättningarna för åtgärderna skiljer de sig åt bl.a. genom att det saknas krav på att det ska finnas en skäligen misstänkt person i lagen om elektronisk kommunikation. Det är mycket på grund av detta som antalet sådana ärenden årligen enligt lagen om elektronisk kommunikation är så mycket högre än för hemlig teleövervakning (ca 9 500 jämfört med ca 1 300). Vid förundersökningar rörande allvarlig brottslighet, t.ex. mord, grova rån, våldtäkter eller grova narkotikabrott, är det många gånger så att det

i vart fall i utredningarnas inledning saknas en skäligen misstänkt person. Uppgifterna som inhämtas om elektronisk kommunikation blir ett hjälpmedel för att komma framåt i utredningen och identifiera misstänkta gärningsmän.

Utredningens bedömning

Frågan blir då om det i den lag utredningen föreslår för inhämtning av uppgifter i underrättelseverksamhet är lämpligt att kräva en anknytning till en viss persons brottsliga verksamhet, såsom är fallet i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Enligt utredningens mening ska syftet med att inhämta uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet uttryckas så att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka viss allvarlig brottslig verksamhet. I ett sådant tidigt skede i brottsbekämpningen och med hänsyn till de syften som underrättelseverksamheten ska tillgodose är det inte möjligt att knyta misstanken till en viss person. Utredningen föreslår därför inte något sådant krav.

Det bör däremot för att inhämtning ska få ske finnas ett krav på att uppgifterna kan antas ha en påtaglig betydelse för den undersökning som anger de ramar som gäller för underrättelseinhämtningen. Det ska uttryckas så att det ska finnas särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet. Det kan därmed inte vara fråga om en allt för extensiv bedömning av värdet av uppgifterna i undersökningen. Bedömningarna får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter, t.ex. källinformation. Begreppet undersökning innefattar olika former av ”ärenden” i underrättelseverksamheten, t.ex. särskild undersökning i kriminalunderrättelseverksamheten, underrättelseprojekt, operationsplan, aktionsgrupp eller insats. Genom att inhämtningen knyts till en undersökning tydliggörs att det inte är fråga om en ”fri inhämtning” utan att det finns en ram utifrån vilken rekvisiten för inhämtning ska bedömas.

Den befarade brottslighetens svårhetsgrad

Bestämmelsen i 6 kap. 22 § första stycket 3 LEK ger de brottsbekämpande myndigheterna rätt att inhämta uppgifter om elektronisk kommunikation i förundersökningar och används även i underrättelseverksamhet, om misstankarna rör brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. För underrättelseverksamhetens del, med den breda informations- och kunskapsinsamlingen och det framåtblickande perspektivet, är det av integritetsskäl i huvudfallet lämpligt att behålla en lika hög tröskel även i fortsättningen. Eftersom det är fråga om just underrättelseverksamhet finns det inte behov av att i detta sammanhang föra in osjälvständiga brottsformer (försöks-, förberedelse- och stämplingsbrott).

Säkerhetspolisen arbetar med brott mot rikets inre och yttre säkerhet och terroristbrott. Lagen om åtgärder för att utreda vissa samhällsfarliga brott innehåller en uppräkning av brott som lagen får tillämpas vid och som faller inom Säkerhetspolisens ansvarsområde. I den uppräkningen ingår vissa brott som inte har minst två års fängelse i straffskalan trots att de måste bedömas som i hög grad samhällsfarliga. Säkerhetspolisen behöver ha möjlighet att bedriva en effektiv underrättelseverksamhet vid samtliga de brott som omfattas av den nämnda lagen. Därför ska Säkerhetspolisen få inhämta uppgifter om elektronisk kommunikation i sin underrättelseverksamhet vid bekämpning av all sådan brottslig verksamhet som omfattas av lagen.

Proportionalitet

För samtliga tvångsmedel gäller proportionalitetsprincipen. Principen brukar i korthet beskrivas så att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Principen finns uttryckt i bl.a. 24 kap. 1 §, 25 kap. 1 §, 26 kap. 1 §, 27 kap. 1 § och 28 kap. 3 a § RB samt i 3 § lagen om hemlig rumsavlyssning och 5 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Att proportionalitetsprincipen ska tillämpas ska uttryckligen anges i den lag utredningen föreslår om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Inhämtning ska få

beslutas och genomföras endast om 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.

6.4.3 Vem ska fatta beslut?

Förslag: Beslut i underrättelseverksamheten om inhämtning av uppgifter om elektronisk kommunikation ska få fattas av chefen för den aktuella brottsbekämpande myndigheten. Myndighetschefen ska i viss utsträckning få delegera beslutanderätten. Det ska få ske till annan person på ledningsnivå.

Inledning

Bestämmelsen i 6 kap. 22 § första stycket 3 LEK anger att leverantören vid misstanke om vissa brott på begäran av den brottsbekämpande myndigheten ska lämna ut uppgifter om elektronisk kommunikation. Utredningen föreslår i avsnitt 6.3.2 att beslut om hemlig teleövervakning avseende historiska uppgifter i syfte att fastställa vem som skäligen kan misstänkas för brottet m.m. ska få fattas av domstol, undersökningsledaren eller åklagaren. Frågan blir vem som ska fatta beslut om inhämtning i underrättelseverksamhet.

Den principiella frågan om allmän domstols och åklagares medverkan i underrättelseverksamhet

Allmän domstol

Att allmän domstol fattar beslut om hemliga tvångsmedel under en förundersökning är naturligt och väl förenligt med det tvåpartsförfarande och de möjligheter till rättslig prövning som gäller där. Däremot är det annorlunda i underrättelseverksamhet. Som framgår av utredningens allmänna utgångspunkter i avsnitt 6.1 gör sig andra intressen gällande där. Integritetsaspekten präglas mera av ett medborgarperspektiv än av ett sådant tvåpartsförfarande som särskilt lämpar sig för rättslig prövning i allmän domstol. Det får också anses vara principiellt tveksamt om de allmänna domstolarna,

inom ramen för nuvarande domstolsorganisation och rättegångsordning, på förhand ska rättsligt pröva olika åtgärder som vidtas inom ramen för underrättelseverksamhet. Den verksamheten är till sin natur operativ, kunskapssökande och undersökande men inte primärt inriktad mot någon viss inträffad gärning eller någon viss misstänkt person. För det fall allmän domstol generellt skulle rättsligt pröva olika åtgärder som vidtas i underrättelseverksamheten och därmed i många fall skulle ge klartecken till olika operativa spaningsåtgärder, kan det finnas risk för 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. I andra rättsordningar fattas integritetsinskränkande beslut i underrättelseverksamhet ibland av särskilda undersökningsdomare eller specialiserade domstolar eller domstolsliknande nämnder utanför den vanliga domstolsorganisationen vilka inte själva har någon del i en eventuell senare brottmålsprocess och rättegång. Den ordningen finns inte i Sverige, men de principer som bär upp kravet på oberoende och självständiga domstolar, fristående från polisen, tullen och underrättelseverksamheten, gäller naturligtvis även i vårt land. Det krävs därför mycket starka skäl för att allmän domstol ska få en roll i prövningen enligt den nya lagen.

Frågan om allmän domstol som beslutandeinstans utanför en förundersökning diskuterades i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177 s. 64 f.). Frågan var där om det i stället för allmän domstol var lämpligt att tillskapa en särskild nämnd som skulle kunna fatta beslut i frågorna. Regeringen bedömde dock att ett system med en särskild nämnd har nackdelar och att det torde vara svårt att inom ramen för en nämndprövning skapa en ordning som på samma påtagliga sätt kan ta till vara integritetsintresset. Ett system med en nämnd skulle också enligt regeringen kunna bli sårbart genom att det skulle kunna uppstå svårigheter att med kort varsel samla nämnden för föredragning och beslut. Regeringen menade därför att övervägande skäl talade mot ett införande av en nämnd som fattar beslut i dessa frågor och föreslog att prövningen i stället skulle göras av allmän domstol (se 6 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott). Det bör emellertid i detta sammanhang betonas att det rör sig om en tidsbegränsad lag och att lagen som den enligt uppgift har kommit att tillämpas närmast tar sikte på

situationer när det beslutas om tvångsmedel mycket nära inpå att en förundersökning kan inledas, dvs. inom ramen för vad som brukar benämnas förutredning.

Åklagare

Åklagarna deltar i regel inte i polisens eller tullens underrättelseverksamhet. I stället sker åklagarinträde först i samband med att förundersökning rörande ett brott har inletts och någon är skäligen misstänkt för brottet.

Frågor om tillstånd till tvångsmedelsanvändning enligt lagen om särskild utlänningskontroll prövas av Stockholms tingsrätt på ansökan av Rikspolisstyrelsen eller en polismyndighet. Åklagarinträde i dessa ärenden sker i regel först i samband med att förundersökning för ett konkret brott har inletts och någon är skäligen misstänkt för brottet.

I propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177 s. 67 f.) angav regeringen att det som talar för att polisen skulle kunna ansöka om tillstånd till de aktuella tvångsmedlen är att ärendena befinner sig på ett spaningsstadium och att det därför skulle innebär ett avsteg från den rådande ansvarsfördelningen mellan polis och åklagare om åklagare tilldelas en roll i polisens underrättelsearbete. Det skulle därför, menade regeringen, krävas starka skäl för att införa en sådan ordning. Efter att ha konstaterat att jämförelsen med lagen om särskild utlänningskontroll av flera skäl inte var helt relevant, uppgav regeringen att polis och åklagare redan i dag i samråd bedömer om det finns tillräckliga skäl för att inleda förundersökning i ärenden om allvarlig brottslighet eller om det krävs ytterligare underrättelse- eller spaningsåtgärder. Regeringen nämnde också att i de större utredningar om allvarlig brottslighet som utförts med framgång har regelmässigt åklagare, spanings- och underrättelseavdelning samt utredningsenheter samarbetat på ett mycket tidigt stadium. Mot bakgrund av detta och det faktum att det rör sig om komplicerade juridiska överväganden vid tvångsmedel för att förhindra brott, bedömde regeringen det, trots de starka skäl som angavs, som mest lämpligt att det är åklagare som ansöker om tillstånd till tvångsmedelsanvändning även i de fallen (se 6 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott).

Som utredningen tidigare har konstaterat har de preventiva tvångsmedlen kommit att användas främst i situationer när en förundersökning är nära förestående och där det därför ligger närmare till hands än annars att åklagaren är involverad. Det ter sig betydligt mera tveksamt om åklagaren ska ha en beslutsfunktion i ”den löpande” underrättelseverksamheten. Det rör sig i dessa fall om inhämtning av uppgifter om elektronisk kommunikation på ett betydligt tidigare stadium där det inte finns någon anknytning till ett särskilt brott eller en särskild brottsutredning. Åklagaren skulle därmed behöva ta ansvar för åtgärder långt innan det finns förutsättningar för att inleda förundersökning och där utredningen typiskt sett inte ens ska leda till en sådan. Enligt 23 kap. 3 § andra stycket RB och 19 § tredje stycket lagen om straff för smuggling är det polis och tull som biträder åklagaren vid förundersökningen. En åklagarmedverkan i underrättelseverksamhet skulle närmast ge det omvända förhållandet, att åklagaren blir ett biträde åt polis och tull i den verksamheten.

Utgångspunkter för bedömningen

Det finns som framgått tungt vägande skäl som talar mot att allmän domstol ges en roll i underrättelseverksamheten. Dessa skäl gör sig gällande med minst samma styrka vad gäller åklagare. 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 åklagarens 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 således mycket tungt vägande skäl att vidmakthålla den ansvarsfördelning som normalt gäller mellan polis och tull respektive åklagare.

Bör allmän domstol eller annat organ fatta besluten?

Säkerhets- och integritetsskyddsnämnden har i sitt remissvar över Trafikuppgiftsutredningens betänkande (SOU 2007:76) angivit att det bör övervägas att, såsom i många andra länder, ge de brottbekämpande myndigheterna befogenheter i underrättelsearbetet som motsvarar de hemliga tvångsmedlen och att sådana befogenheter

kan förhandsprövas av domstol eller annat rättsligt organ som utformas särskilt för den uppgiften. Det bör framhållas att nämnden här anger att det ska vara fråga om en specialdomstol eller annat rättsligt organ som utformas särskilt för uppgiften och inte allmän domstol.

Utredningens arbete vid sidan av frågorna i detta delbetänkande rör relativt stora frågor om de brottsbekämpande myndigheternas befogenheter såväl i underrättelseverksamheten som under förundersökning. Utredningen kommer i det sammanhanget också att behöva göra överväganden om vilket beslutsorgan som bör finnas för t.ex. infiltrationsverksamhet, provokativa åtgärder, tvångsmedelsliknande situationer och tekniska spaningsmetoder. Utredningens uppdrag i den delen ska redovisas senast den 1 oktober 2009.

Det arbete som bedrivs i underrättelseverksamheten, där man t.ex. på ett mycket tidigt stadium kartlägger och analyserar företeelser som senare kan komma att utvecklas till brottslighet, skiljer sig många gånger till sin karaktär från förundersökningsverksamheten. Som utredningen konstaterat finns tungt vägande skäl av principiell natur mot att allmänna domstolar ges beslutanderätt i underrättelseverksamheten.

Det finns också en del praktiska hinder. Ett sådant problem är frågan i vilken utsträckning jourdomstolar skulle kunna tillgodose behovet av snabba beslut utanför kontorstid. Att införa en ordning med dygnet-runt-beredskap för de allmänna domstolarna för att pröva frågor om inhämtande av uppgifter i underrättelseverksamheten framstår inte som ändamålsenligt. Som utredningen återkommer till är det inte heller någon framkomlig väg att i det här sammanhanget lägga den interimistiska beslutanderätten på åklagare.

Med hänsyn till såväl principiella skäl som de praktiska hinder som finns gör utredningen bedömningen att det varken är lämpligt eller ändamålsenligt att, inom ramen för nuvarande domstolsorganisation, låta allmänna domstolar få beslutanderätten vid inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

När det sedan gäller frågan om befogenheterna bör ges av en specialdomstol, nämnd eller liknande organ gör utredningen bedömningen att prövningens i många fall brådskande natur i kombination med en spridd geografisk förekomst och ett förhållandevis stort antal ärenden gör att det inte framstår som realistiskt att inrätta ett sådant organ på en plats i landet. Att i stället inrätta

flera nämnder eller liknande organ på olika platser för att kunna tillgodose behovet av närhet till lokala brottsbekämpande myndigheter framstår ur verksamhets- och effektivitetsperspektiv inte heller som särskilt lämpligt när det enbart är fråga om det ändamål som nu övervägs. Utredningen föreslår därför inte heller att det i detta sammanhang ska inrättas någon specialdomstol eller annat särskilt rättsligt organ för att fatta beslut om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamheten.

Bör åklagare fatta besluten?

Nästa fråga blir då om åklagare bör ha beslutanderätt i fråga om åtgärden att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet.

Åklagare har som huvudsakliga uppgifter att leda förundersökningar, väcka åtal och föra talan i domstol. Som utredningen nyss har betonat har åklagare alltså inte i dagsläget någon egentlig roll i underrättelseverksamheten. Tvärtom finns det som utredningen tidigare anfört starka principiella och verksamhetsanknutna invändningar mot att åklagare ges en sådan roll. Däremot förekommer det ibland samråd mellan polis, tull och åklagare i frågan om det finns tillräckliga skäl att inleda förundersökning eller om det krävs ytterligare underrättelse- eller spaningsåtgärder. Även om åklagare således till viss del och i vissa skeden kan vara delaktiga i underrättelseverksamheten är det som regel begränsat till konkreta ärenden och situationer när en förundersökning är nära förestående. Med hänsyn härtill bör det, som också konstateras i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177 s. 67), krävas starka skäl för att utvidga åklagarens roll i underrättelseverksamhet och därigenom frångå den rådande ansvarsfördelningen mellan polis och tull respektive åklagare. När det gäller inhämtande av uppgifter om elektronisk kommunikation gör utredningen bedömningen, särskilt i ljuset av de principiella och verksamhetsanknutna invändningarna mot en sådan ordning, att sådana tungt vägande skäl inte finns och att beslutanderätten därför inte bör ligga hos åklagare.

Bör polis och tull själva få fatta beslut om att inhämta uppgifterna?

Beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 3 LEK fattas enligt nuvarande ordning av polisen respektive tullen. Det är inte närmare reglerat på vilken nivå inom myndigheterna besluten ska fattas. Visserligen har JO uttalat att en fråga om inhämtning bör underställas förundersökningsledaren, men när det gäller inhämtning i underrättelseverksamhet saknas den funktionen.

Utredningen menar att beslutanderätten ska ligga kvar hos de brottsbekämpande myndigheterna, men föreslår samtidigt att beslutsordningen inom myndigheterna preciseras och att det införs en kontinuerlig kontroll inom ramen för Säkerhets- och integritetsskyddsnämndens oberoende tillsynsverksamhet (se avsnitt 6.9).

Utredningen anser således att det inte bör göras något avsteg från ordningen att polisen och tullen själva fattar beslut om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Däremot är det nödvändigt att det etableras en fastlagd ordning för vem som inom myndigheterna ska vara behörig att besluta om inhämtning. Med hänsyn till de överväganden som bör göras innan ett beslut om inhämtning fattas, bör beslutanderätten inte tillkomma varje polisman respektive tulltjänsteman. Tvärtom ser utredningen skäl att precisera vem som får fatta besluten och tillskapa en ordning som innebär att beslutet om inhämtning fattas av någon som inte handlägger det aktuella ärendet i övrigt. Utredningen föreslår därför att beslutanderätten ska tillkomma myndigheten som sådan, dvs. myndighetschefen. Denne ska dock ha möjlighet att delegera beslutanderätten till andra personer på myndighetsledningsnivå. Utredningen återkommer nedan i avsnitt 6.9 till frågan om utformningen av en löpande och mera kontinuerlig tillsynsverksamhet, som, i avsaknad av andra oberoende beslutsorgan och utöver den föreslagna uppstramningen av beslutsfunktionen, framstår som nödvändig från rättssäkerhets- och integritetsskyddssynpunkt.

6.4.4 I vilken omfattning ska uppgifterna få användas?

Förslag: Om det i de brottsbekämpande myndigheternas underrättelseverksamhet har inhämtats information av betydelse för att förhindra brott, ska informationen få användas för att förhindra brottet.

Om det i de brottsbekämpande myndigheternas underrättelseverksamhet har inhämtats information som är av betydelse för utredningen av ett brott, ska informationen få användas för att utreda brottet endast om beslut om hemlig teleövervakning har fattats.

Allmänt

Utredningen föreslår att de brottsbekämpande myndigheternas användning av de uppgifter som inhämtats enligt den föreslagna lagen ska regleras. Regleringen ska omfatta inte bara vad som skulle kunna benämnas överskottsinformation (jfr 27 kap. 23 a § RB och 12 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott), dvs. information som inte har samband med den brottsliga verksamhet som är kopplad till beslutet att inhämta uppgifterna, utan även uppgifter som har sådan koppling.

Användning i syfte att förhindra brott

Intresset av att förhindra brott är mycket starkt. Därför finns det inte föreskrivet några begränsningar i de nuvarande regleringarna i fråga om de brottsbekämpande myndigheternas möjlighet att använda inhämtad information i det syftet. Det gäller i teorin även bötesbrott. Det finns enligt utredningens mening inte skäl att ha andra bestämmelser för uppgifter om elektronisk kommunikation som har inhämtats enligt den föreslagna lagen. Det bör dock påpekas att bestämmelserna i t.ex. polisdatalagen och sekretesslagen kan begränsa möjligheterna att använda informationen.

Användning i syfte att utreda brott

När information har inhämtats i underrättelseverksamheten kan det ifrågasättas om sådan information ska få användas för att utreda brott. Som påpekades i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/2006:177 s. 70) kan det i praktiken innebära en ny brottsutredningsmetod. Bl.a. mot den bakgrunden bedömde regeringen att om information som inhämtas enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott ger uppgifter om redan begångna brott, så bör den informationen inte få användas i samma utsträckning som om informationen erhålls inom ramen för en förundersökning. Däremot talade enligt regeringen starka skäl för att i vart fall den allra allvarligaste brottsligheten utreds och lagförs, oavsett hur informationen om brottet kommit till de brottsbekämpande myndigheternas kännedom. En annan ordning skulle, menade regeringen, kunna leda till stötande resultat. Det föreskrivs därför i den nämnda lagen att om det har kommit fram uppgifter om brott får uppgifterna användas för att utreda det brottet endast om det är fråga om brott som avses i lagen. Information om andra brott får därför inte på något sätt användas för att utreda sådana brott, dvs. den får varken läggas till grund för ett beslut att inleda en förundersökning om brottet eller användas för att berika materialet i en pågående förundersökning.

En lämplig ordning för de brottsbekämpande myndigheternas underrättelseverksamhet är att om den information som inhämtas enligt lagen är av betydelse för att utreda ett begånget brott, ska uppgifterna få användas för att utreda brottet endast om det är fråga om brott av så kvalificerat slag att det skulle ge myndigheterna möjlighet att använda hemlig teleövervakning för att inhämta uppgifterna. Utredningen menar dock att det utifrån de allmänna utgångspunkterna (se avsnitt 6.1) finns skäl att gå ytterligare ett steg och kräva att det faktiskt fattas ett beslut om hemlig teleövervakning för att sådana uppgifter ska få användas i en förundersökning.

De brottsbekämpande myndigheterna behöver därför med hjälp av underrättelseinformation och eventuellt ytterligare utredningsåtgärder bygga upp de skäl som krävs för att tillstånd till hemlig teleövervakning kan ges enligt rättegångsbalken. Med den ordningen säkerställs att det sker samma prövning oberoende av om uppgifterna inhämtas i underrättelseverksamheten eller under en

förundersökning. Det ska med andra ord inte vara möjligt att ”gå runt” rättegångsbalkens bestämmelser.

Praktiskt innebär detta att om det i underrättelseverksamheten inhämtas uppgifter om elektronisk kommunikation, som ensamma eller tillsammans med annan underrättelseinformation visar sig ha betydelse för en förundersökning, krävs det att domstol, åklagare eller undersökningsledare fattar beslut om hemlig teleövervakning enligt rättegångsbalken för att de uppgifterna ska få användas i den fortsatta utredningen. En särskild fråga, framför allt vid avslagsbeslut, är vilket material som kommer att omfattas av partsinsyn från den misstänktes sida. Det kan nämnas att Insynsutredningen för närvarande arbetar med att se över frågan om hur långtgående en misstänkts, en tilltalads respektive en dömd persons rätt till insyn i förundersökningsmaterial och annat utredningsmaterial bör vara (Dir. 2007:120, Ju 2007:13).

6.4.5 Behandling av upptecknin gar av uppgifter om elektronisk kommunikation

Förslag: Upptecknin gar av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska granskas snarast möjligt.

Upptecknin gar ska, i de delar de är av betydelse för att förebygga eller förhindra brott, bevaras så länge det behövs för att förebygga eller förhindra brott. De ska därefter förstöras.

De brottsbekämpande myndigheterna ska dock alltid få behandla uppgifter från upptecknin gar om förestående brott i enlighet med vad som är särskilt föreskrivet i lag.

Nuvarande reglering

En upptagning eller upptecknin g som görs vid hemlig teleavlyssning, hemlig teleövervakning eller hemlig rumsavlyssning eller en upptagning som görs vid hemlig kameraövervakning ska enligt bestämmelserna i 27 kap. 12 och 24 §§ RB samt 13 § lagen om hemlig rumsavlyssning granskas så snart det är möjligt. Granskningen får utföras endast av rätten, förundersökningsledaren, åklagaren eller en sakkunnig. I de delar upptagningen eller upptecknin gen är av betydelse från brottsutredningssynpunkt ska de bevaras till dess

förundersökningen lagts ned eller avslutats eller målet har avgjorts slutligt. Har upptagningen eller uppteckningen betydelse för att förhindra brott, ska den bevaras så länge det behövs för det syftet för att därefter förstöras. Liknande bestämmelser finns även i 13 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Utredningens bedömning

Även i den föreslagna lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska det finnas bestämmelser om behandling av uppteckningar av uppgifter. Regleringen bör utformas med förebild i de bestämmelser som gäller vid hemlig teleövervakning. Granskning av uppteckning ska ske snarast möjligt. Det saknas dock anledning att för underrättelseverksamheten föreskriva vem som får genomföra granskningen. Utredningen föreslår också att uppteckningarna, i de delar de är av betydelse för att förebygga eller förhindra brott, ska få bevaras så länge det behövs för att förebygga eller förhindra brott. De ska därefter förstöras.

När användningen av överskottsinformation reglerades föreskrevs i bl.a. 27 kap. 24 § tredje stycket RB att bestämmelserna om bevarande respektive förstörande av upptagningar eller uppteckningar från hemlig teleavlyssning inte hindrar att de brottsutredande myndigheterna behandlar uppgifter från upptagningarna eller uppteckningarna i enlighet med vad som är särskilt föreskrivet i lag. Numera gäller bestämmelsen även för hemlig teleövervakning. Det är alltså fråga om undantag från vad som annars föreskrivs om förstörande av upptagningar och uppteckningar i bestämmelsen. Om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen eller lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, utgör alltså regleringen inte hinder för att nämnda uppgifter behandlas enligt dessa lagar. I fråga om gallring m.m. av uppgifterna gäller då vad som föreskrivs i de särskilda lagarna. En motsvarande ordning ska finnas även för myndigheternas underrättelseverksamhet.

6.5 Tillgång till lokaliseringsuppgifter

Förslag: De brottsbekämpande myndigheterna ska under samma förutsättningar som gäller för hemlig teleövervakning få inhämta lokaliseringsuppgifter. Med det avses

1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, eller
2. uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.

Lokaliseringsuppgifter ska också få inhämtas enligt lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottbekämpande myndigheternas underrättelseverksamhet.

6.5.1 Nuvarande reglering m.m.

Genom hemlig teleövervakning har de brottsbekämpande myndigheterna möjlighet att få tillgång till vissa lokaliseringsuppgifter för bl.a. mobiltelefoner. Det rör uppgifter om vilken basstation en telefon eller annan mobil elektronisk kommunikationsutrustning varit uppkopplad mot i samband med en kommunikation (t.ex. ett samtal eller ett SMS-meddelande). Sådana historiska uppgifter har myndigheterna möjlighet att få ut även enligt 6 kap. 22 § första stycket 3 LEK i den utsträckning det finns en elektronisk kommunikation, eftersom det är frågan om uppgifter som angår särskilda elektroniska meddelanden.

En basstationstömning innebär att de brottsbekämpande myndigheterna får uppgifter t.ex. om samtliga de mobiltelefoner som vid en viss tid har varit uppkopplade för kommunikation (t.ex. samtal eller SMS-meddelande) och som då haft kontakt med en viss basstation och då befunnit sig inom ett avgränsat geografiskt område. Sådana uppgifter anses vara uppgifter som angår särskilda elektroniska meddelanden och kan därför lämnas ut till myndigheterna om förutsättningarna för det finns enligt 6 kap. 22 § första stycket 3 LEK. Däremot medger inte de nuvarande bestämmelserna om hemlig teleövervakning att en basstationstömning sker, eftersom övervakningen enbart får avse uppgifter om telemeddelanden

till eller från vissa teleadresser med viss koppling till en skäligen misstänkt person.

Både med stöd av bestämmelserna om hemlig teleövervakning och regeln i 6 kap. 22 § första stycket 3 LEK kan alltså de brottsbekämpande myndigheterna få del av lokaliseringsuppgifter enbart när sådana uppgifter har genererats i samband med att mobiltelefonen har varit uppkopplad för kommunikation. Lokaliseringsuppgifter som finns hos leverantören och som genereras av utrustningens kontakt med en basstation utan att det varit fråga om en kommunikation, t.ex. en enbart påslagen mobiltelefon, omfattas inte av de uppgifter som ska lämnas ut enligt de aktuella bestämmelserna. Sådana uppgifter omfattas inte heller av leverantörernas tystnadsplikt enligt lagen om elektronisk kommunikation, eftersom det inte är fråga om uppgifter som angår något särskilt elektroniskt meddelande. Det innebär också att det inte finns någon skyldighet för leverantörerna enligt 6 kap. 22 § LEK att lämna ut sådana uppgifter. Som framgår nedan har Justitiekanslern i ett beslut ansett att leverantörerna inte heller får lämna ut uppgifterna, om inte uppgifterna avidentifieras eller att samtycke ges från den berörde.

Buggningsutredningen föreslog att hemlig teleövervakning uttryckligen skulle omfatta lokalisering av teleadress, även utan att det samtidigt t.ex. rings ett samtal. Utredningen anförde att det tveklöst finns ett stort behov av sådana uppgifter i brottsbekämpningen och att det inte möter några hinder från integritetssynpunkt (SOU 1998:46 s. 365 f. och 477 f.).

Även BRU föreslog att hemlig teleövervakning uttryckligen ska få användas för att inhämta uppgifter om lokalisering, oavsett om en mobiltelefon eller något annat tekniskt hjälpmedel har använts för kommunikation eller inte. BRU konstaterade att uppgifterna många gånger är värdefulla i brottsbekämpningen, att uppgifterna kan ha mycket stor betydelse i effektivitetshänseende, att det tveklöst finns ett mycket stort behov av att få tillgång till sådana uppgifter och att det inte möter några avgörande hinder från integritetssynpunkt med en ordning där sådana uppgifter lämnas ut vid hemlig teleövervakning (SOU 2005:38 s. 202 ff.).

Flera remissinstanser uttalade sig särskilt om BRU:s förslag om att lokaliseringsuppgifter som inte har samband med en kommunikation ska lämnas ut vid hemlig teleövervakning. Bland annat JO sade sig inte har någon invändning mot förslaget. Till samma slut kom Skövde tingsrätt, Åklagarmyndigheten, Säkerhetspolisen och Kriminalvårdsstyrelsen medan IT-Företagen efterlyste bättre

underlag vad gäller brottsbekämpningens behov av sådana uppgifter.

6.5.2 JK:s beslut

Enligt 6 kap. 9 § LEK får lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer behandlas av leverantörerna endast sedan de har avidentifierats eller användaren eller abonnenten har gett sitt samtycke till behandlingen. Justitiekanslern har i ett beslut den 15 augusti 2008 (dnr 6545-06-21) konstaterat att den nuvarande regleringen i 6 kap. 9 § LEK innebär att leverantörerna inte till polisen får lämna ut uppgifter om lokalisering av en mobiltelefon som är påslagen men som inte använts för en kommunikation utan att de berörda fysiska personerna först har avidentifierats eller gett sitt samtycke.

Samtidigt kan de brottsbekämpande myndigheterna få åtkomst till uppgifterna genom beslag, eventuellt i kombination med husrannsakan, eller editionsföreläggande. Justitiekanslern har dock i ovannämnda beslut konstaterat att de lokaliseringsuppgifter som polis och åklagare skulle kunna få tillgång till genom t.ex. beslag eller editionsföreläggande inte torde vara tillräckligt för att tillgodose det legitima behov som ofta finns att komma över dessa uppgifter. Det framstår enligt Justitiekanslern som givet, trots integritetsriskerna, att polis och åklagare bör ges en sådan möjlighet.

6.5.3 Utredningens bedömning

På flera ställen i det här betänkandet (se bl.a. avsnitt 4.2) framgår att basstationstömningar ofta sker med avseende på platsen för grova brott. För de brottsbekämpande myndigheterna är basstationstömning ofta en inledande åtgärd för att så snabbt som möjligt kunna identifiera skäligen misstänkta personer i utredningen. När bestämmelsen i 6 kap. 22 § första stycket 3 LEK upphävs är det nödvändigt för effektiviteten i den brottsbekämpande verksamheten att möjligheten att genomföra basstationstömning finns kvar. Det är av samma skäl viktigt att det i brottsbekämpningen ges tillgång till uppgifter avseende t.ex. mobiltelefoner som är påslagna men som inte används för en kommunikation. Genom dessa uppgifter kan myndigheterna t.ex. följa en viss mobiltelefon längs en

flyktväg eller lokalisera ett gömställe eller den plats där målsäganden befinner sig. Utredningen föreslår att båda dessa typer av uppgifter ska benämnas lokaliseringsuppgifter, som därmed blir ett vidare begrepp än lokaliseringsuppgifter enligt 6 kap. 9 § LEK.

De uppgifter som nu har nämnts är inte uppgifter om telemeddelanden (jfr 4 kap. 8 § brottsbalken) och bör därför inte regleras som en del av tvångsmedlet hemlig teleövervakning. Uppgifterna bör dock få inhämtas enligt rättegångsbalken under samma förutsättningar som gäller för hemlig teleövervakning. Uppgifterna bör också få inhämtas enligt lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottbekämpande myndigheternas underrättelseverksamhet. En sådan reglering ger de rättssäkerhetsgarantier som erfordras.

Det ska sägas att Trafikuppgiftsutredningens förslag om vilka uppgifter som ska lagras av leverantörerna för brottsbekämpande syften enbart omfattar vissa lokaliseringsuppgifter som har samband med en kommunikation (se SOU 2007:76). Förutsättningen för en effektiv ordning vad gäller lokaliseringsuppgifter är att sådana uppgifter åtminstone i viss utsträckning lagras så att de finns tillgängliga för de brottsbekämpande myndigheterna. Det ligger dock inte i utredningens uppdrag att föreslå någon ytterligare lagringsskyldighet.

6.6 Inhämtning av uppgifter om abonnemang

Förslag: Skyldigheten för leverantörerna att lämna ut uppgifter om abonnemang till brottsbekämpande myndigheter ska i motsats till vad som nu gäller inte vara begränsad till misstanke om brott av viss svårhetsgrad.

6.6.1 Nuvarande reglering m.m.

Som framgått i avsnitt 4.3 har samtliga brottsbekämpande myndigheter i dag möjlighet att få tillgång till uppgifter om abonnemang genom att söka uppgifterna på vanligt sätt i öppna källor eller genom att kontakta leverantörerna och begära att få tillgång till uppgifterna med stöd av 6 kap. 22 § första stycket 2 LEK. Leverantörerna är enligt den bestämmelsen skyldiga att på begäran lämna ut abonnemangsuppgifterna till myndigheterna vid

misstanke om brott för vilket fängelse är föreskrivet, om brottet bedöms föranleda annan påföljd än böter i det enskilda fallet.

Den dubbelreglering som finns i dag för de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (6 kap. 22 § första stycket 3 LEK och hemlig teleövervakning enligt rättegångsbalken) finns inte för tillgång till uppgifter om abonnemang. Hemlig teleövervakning ger inte myndigheterna tillgång till abonnemangsuppgifter, t.ex. uppgift om vem som innehar en teleadress som haft kontakt med en teleadress som den hemliga teleövervakningen avser. I stället måste myndigheterna använda öppna källor alternativt 6 kap. 22 § första stycket 2 LEK för att få sådana uppgifter, alltså även under en pågående hemlig teleövervakning.

Regeringen har nyligen lämnat propositionen Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG till riksdagen (prop. 2008/09:67). En effekt av förslaget i propositionen är att rättighetshavare ges en civilrättslig möjlighet att få ut information från en Internetleverantör om vem som har ett abonnemang (ett IP-nummer) som har använts vid ett immaterialrättsintrång via Internet. För att informationen ska lämnas ut krävs dels en domstolsprövning, dels att det finns sannolika skäl för intrånget. En Internetleverantör som har lämnat ut information ska efter viss tid underrätta abonnenten om detta.

6.6.2 Utredningens bedömning

För brottsbekämpningen finns det ett stort behov av uppgifter om abonnemang såväl i förundersökningar som i underrättelseverksamhet. Många gånger behöver uppgifterna hämtas in mycket snabbt. Framför allt mot bakgrund av att det är fråga om uppgifter som inte avslöjar användningen av elektronisk kommunikation hindrar enligt utredningen inte integritetsskyddsskäl en ordning där brottsbekämpande myndigheter även i fortsättningen själva beslutar om inhämtningen. Det gäller under förutsättning att uppgifterna inskränker sig till vad som kan betecknas som identifieringsuppgifter. Som framgår av avsnitt 3.10.2 har uppgifter om vem som innehar ett visst IP-nummer vid en viss tidpunkt ansetts vara en abonnemangsuppgift. Utredningen föreslår inte någon förändring av detta.

Det förtjänar dock att påpekas att uppgifter som i det sammanhanget går utöver vad som kan anses som identifieringsuppgifter, t.ex. med vilka andra IP-nummer som innehavaren har kommunicerat, vilka hemsidor som ett visst IP-nummer har besökt och liknande uppgifter måste bedömas vara uppgifter som angår ett särskilt elektronisk meddelande. Enligt utredningens mening innebär ett utfående av dessa uppgifter från leverantören ett ingrepp i telehemligheten och kräver därför beslut om hemlig teleövervakning eller beslut enligt den föreslagna lagen om inhämtning av uppgifter i underrättelseverksamhet.

BRU föreslog att de brottsbekämpande myndigheterna ska kunna få del av abonnemangsuppgifter utan begränsning till att misstanken ska röra brott av viss svårhetsgrad. Flera remissinstanser instämde i BRU:s förslag och framhöll att det är av stor vikt att myndigheterna får del av uppgifterna även vid mindre allvarliga brott som var för sig inte når upp till fängelsenivå, t.ex. immaterialrättsliga brott. Även utredningen har konstaterat ett sådant behov. Det kan som exempel röra sig om olika former av trakasserier på Internet, som ofta bedöms som ofredande eller förtal på bötesnivå. Men även upphovsrättbrott hör hit. När det gäller det immaterialrättsliga området är det värt att notera att ett genomförande av förslagen i prop. 2008/09:67 med nuvarande reglering skulle innebära att rättighetshavare, om än efter domstolsprövning, i några fall skulle ha mer vittgående befogenheter att få ut IP-nummer från Internetleverantörerna än vad de brottsbekämpande myndigheterna för närvarande har. I en rättsstat måste dock det huvudsakliga brottsbekämpande arbetet åvila polisen och andra myndigheter, även när det gäller bötesbrottslighet av det slag som upphovsrättsbrott utgör exempel på. Det finns således flera starka skäl till varför möjligheterna till inhämtande av abonnemangsuppgifter bör utvidgas till att avse även brott på bötesnivå.

Utredningen föreslår därför att de brottsbekämpande myndigheterna ska ha rätt att få del av uppgifterna vid misstankar om brott, dvs. den nuvarande begränsningen till misstankar om brott av viss svårhetsgrad ska tas bort.

6.7 Överprövning m.m.

Förslag: Har hemlig teleövervakning avseende en viss teleadress beslutats av undersökningsledaren eller åklagaren ska den som innehar teleadressen kunna begära rättens prövning av beslutet.

Brottsbekämpande myndighets beslut om inhämtning av uppgifter i underrättelseverksamhet ska inte kunna bli föremål för överprövning av domstol. I stället ska Säkerhets- och integritetsskyddsnämndens tillsyn i efterhand förstärkas.

6.7.1 Nuvarande reglering

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, däribland hemlig teleövervakning, får beslutet överklagas särskilt, dvs. utan samband med överklagande av dom eller slutligt beslut (se även 54 kap. 4 § RB). Några nya bestämmelser om detta behövs inte.

När syftet med hemlig teleövervakning är att fastställa vem som skäligen kan misstänkas för brottet m.m. ska beslut om åtgärden enligt utredningens förslag få fattas även av undersökningsledare eller åklagare. Frågan blir om det finns tillräckliga skäl att införa en överklagandemöjlighet rörande sådana beslut.

En polismans beslut om tvångsmedel under en förundersökning kan inte överklagas till 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 beslag, reseförbud och anmälningsskyldighet).

6.7.2 Utredningens bedömning

Mot att införa in rätt att överklaga undersökningsledarens och åklagarens beslut om hemlig teleövervakning talar att en sådan möjlighet närmast torde bli av teoretiskt intresse med hänsyn till att den som är föremål för åtgärden genom att inneha den teleadress som omfattas av tvångsmedlet normalt saknar kännedom om

att tvångsmedlet 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 prövning 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.

Att inhämta lokaliseringsuppgifter genom basstationstömning är i och för sig en integritetskänslig åtgärd. Integritetsintrånget för den enskilde är dock klart begränsat så länge uppgiften inte bearbetas vidare i utredningen. Enligt utredningens mening ska rätten att begära domstolens prövning av beslut om hemlig teleövervakning som har fattats av undersökningsledaren eller åklagaren finnas endast när övervakningen har avsett en viss teleadress. Den som innehar teleadressen bör vara den som har rätt att få en sådan prövning. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har beslutet upphört att gälla innan rätten har prövat ärendet, ska undersökningsledaren eller åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Som framgår i avsnittet om allmänna utgångspunkter (avsnitt 6.1) är det först vid en förundersökning som partsintressena gör sig så pass påtagligt gällande att det finns skäl att möjliggöra en rättslig prövning av beslut om inhämtande av uppgifter. Det finns alltså enligt utredningens mening inte tillräckliga skäl att tillskapa en sådan ordning i underrättelseskedet. Däremot finns det anledning att betona den noggrannhet och de grannlaga bedömningar som krävs från de brottsbekämpande myndigheternas sida när beslut ska fattas och att den tillsyn som ska finnas över myndigheternas verksamhet är robust och effektiv. Den förstärkning av Säkerhets- och integritetsskyddsnämndens tillsyn som föreslås i avsnitt 6.9 innebär att kontrollen av beslutens lagenlighet blir kontinuerlig och frekvent.

6.7.3 Offentliga ombud

När det gäller hemliga tvångsmedel eller liknande hemliga åtgärder får den som utsatts 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. Däremot ska offentliga ombud medverka vid prövningen av om hemlig teleövervakning, liksom övriga tvångsmedel, ska tillåtas enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (6 §). Mot bakgrund av att möjligheten att inhämta uppgifter om elektronisk kommunikation direkt från leverantörerna var under översyn, ansåg regeringen att ett slutligt ställningstagande i frågan om medverkan av offentligt ombud i ärenden om hemlig teleövervakning borde anstå till dess att översynen var slutförd (prop. 2002/03:74 s. 24).

I dagsläget medverkar offentliga ombud inte vid beslut om hemlig teleövervakning enligt rättegångsbalken eller vid utlämnanden av uppgifter enligt lagen om elektronisk kommunikation. Regeringen har inte tagit slutlig ställning i frågan om ombudens medverkan. Det finns både för- och nackdelar med att införa en ordning med offentliga ombud i samtliga de fall som enligt utredningens förslag i fortsättningen ska kräva beslut om hemlig teleövervakning. Frågan om medverkan av offentliga ombud måste avgöras i hela dess vidd, dvs. för samtliga fall där hemlig teleövervakning kan bli aktuell enligt rättegångsbalken. Det får därför anses ligga utanför den här utredningens uppdrag att överväga en sådan ordning.

6.8 Underrättelse till enskild

Förslag: Underrättelse ska ske i efterhand till enskild som innehar en teleadress som hemlig teleövervakning har avsett även när syftet med tvångsmedlet har varit att fastställa vem som skäligen kan misstänkas för brottet m.m. Förundersökningsledaren ska ansvara för att underrättelse sker.

En underrättelseskyldighet ska inte finnas när

1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område har inhämtats,
2. integritetsintrånget för den enskilde annars kan antas vara ringa, eller
3. uppgift om vem som innehar teleadressen inte fastställts.

Det ska inte finnas någon underrättelseskyldighet i de brottsbekämpande myndigheternas underrättelseverksamhet.

Underrättelseskyldighet ska inte heller finnas vid inhämtning av uppgifter om abonnemang.

6.8.1 I vilka fall ska underrättelse ske?

Nuvarande reglering m.m.

Den som är eller har varit brottsmisstänkt ska enligt 27 kap. 31 § RB som huvudregel underrättas om hemlig teleövervakning. Om åtgärden har avsett en teleadress som innehas av någon annan än den misstänkte, ska även innehavaren underrättas. 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 vilken teleadress den har avsett och när den verkställdes. Dessutom ska personen underrättas om vilken brottsmisstanke som legat till grund för teleövervakningen. 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.

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. Underrättelseskyldigheten kan även ha en återhållande verkan på använd-

ningen av metoderna och bidra till att prövningen inför ett beslut sker på ett än mer noggrant sätt (prop. 2006/07:133 s. 30).

Utredningens bedömning

Förundersökning

I dag finns alltså en underrättelseskyldighet vid bl.a. hemlig teleövervakning enligt rättegångsbalken och enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Underrättelseskyldighet finns dock inte när de brottsbekämpande myndigheterna har hämtat in motsvarande uppgifter enligt 6 kap. 22 § första stycket 3 LEK. Av integritetsskyddsskäl menar utredningen att det ska finnas en underrättelseskyldighet vid hemlig teleövervakning som genomförs även när syftet med åtgärden är att fastställa vem som skäligen kan misstänkas för brottet m.m. Det är den som innehar en teleadress som åtgärden har avsett som ska underrättas. I praktiken innebär det en stor utvidgning av antalet ärenden där underrättelseskyldighet finns.

I vissa fall behöver, enligt utredningens bedömning, underrättelseskyldighet inte finnas, eftersom integritetsintrånget för den enskilde kan bedömas vara så ringa att det inte är motiverat att bygga upp en sådan ordning. Det rör sig för det första om basstationstömningar, alltså inhämtande av lokaliseringsuppgifter om vilka mobila elektroniska kommunikationsutrustningar, framför allt mobiltelefoner, som har funnits inom ett visst avgränsat geografiskt område. Det är inte motiverat att alla som har använt sin mobiltelefon inom ett avgränsat geografiskt område i tidsmässig anslutning till att exempelvis ett grovt rån har begåtts ska behöva underrättas om den åtgärden. En enda sådan basstationstömning kan föranleda att de brottsbekämpande myndigheterna behöver underrätta hundratals personer. För det andra rör det bl.a. den bearbetning som sker i steget efter en basstationstömning, när myndigheterna hämtar in ytterligare uppgifter rörande de t.ex. 100 teleadresser som befann sig på platsen i syfte att sortera ut de teleadresser som kan vara intressanta för den fortsatta utredningen. I praktiken kan den åtgärden närmast ses som en del av basstationstömningen och är så löst kopplad till och föga inriktad mot den enskilde att integritetsintrånget inte kan bedömas vara av så ingripande slag att det kan motivera en underrättelseskyldighet.

Underrättelseskyldighet bör inte heller finnas i situationer där det inte fastställs vem som innehar den teleadress som en hemlig teleövervakning har avsett, t.ex. när det är fråga om ett anonymt kontantkort i mobiltelefon.

Underrättelseverksamhet

I underrättelseverksamheten saknas det i dag en underrättelseskyldighet när de brottsbekämpande myndigheterna har inhämtat uppgifter enligt 6 kap. 22 § första stycket 3 LEK. Som framgår av bl.a. de allmänna utgångspunkterna (se avsnitt 6.1) är underrättelseverksamhet inte inriktad mot en viss person och partsintresset 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 partintressena 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. Däremot är det av största vikt att den tillsynsverksamhet som utredningen föreslår att Säkerhets- och integritetsskyddsnämnden ska bedriva genom att granska inhämtningens lagenlighet och måttet av integritetsintrång, blir effektiv, kontinuerlig och av tillräckligt robust slag (se avsnitt 6.9).

Uppgift om abonnemang

När myndigheterna inhämtar uppgifter om abonnemang sker inget intrång i telehemligheten. Underrättelse till enskild är inte motiverad i de fallen.

6.8.2 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. Enligt förordningen (2007:1144) om fullgörande av underrättelseskyldighet enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, är det åklagaren som fullgör underrättelseskyldighet. Även i dessa fall ska åklagaren underrätta Säkerhets- och integritetsskyddsnämnden när en underrättelse inte har kunnat lämnas under ett år på grund av sekretess.

Utredningens förslag innebär att förundersökningsledare vid polisen och tullen, liksom åklagare, i fortsättningen kommer att kunna besluta om hemlig teleövervakning (se avsnitt 6.3.2). Det kommer i de flesta fall att vara fråga om situationer när det inledningsvis saknas en skäligen misstänkt person i utredningen. Om förundersökningsledarskapet vid beslutet finns hos polis eller tull, kan det givetvis senare övergå till åklagare, t.ex. när en skäligen misstänkt person har identifierats. Likaså kan en åklagare som en gång har varit förundersökningsledare i ett ärende föra över förundersökningsledningen till polis eller tull, om förutsättningar för det finns enligt 23 kap. 3 § RB respektive 19 § lagen om straff för smuggling.

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. Den som har förundersökningsledaransvaret i varje läge ska därför också 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. Den åklagare, polisman eller tulltjänsteman som var förundersökningsledare när förundersökningen avslutades ska vara ansvarig för underrättelsen. I avsnitt 7.1 återkommer utredningen med en bedömning av de ekonomiska konsekvenserna av förslagen.

6.9 Särskild tillsyn av Säkerhets- och integritetsskyddsnämnden

Förslag: Säkerhets- och integritetsskyddsnämnden ska utöva löpande tillsyn även över användningen av de nya befogenheterna att inhämta uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. För att uppväga att de brottsbekämpande myndigheterna själva ska få fatta beslut om inhämtning ska nämndens kapacitet förstärkas med ett eller flera granskningsombud som hos myndigheterna kontrollerar hur befogenheterna har beslutats och använts.

Granskningsombud ska utses av nämnden för en bestämd tid, högst fyra år. Ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Ett granskningsombud får inte vara ledamot av nämnden.

Säkerhets- och integritetsskyddsnämnden ska även vara skyldig att på begäran av en enskild person kontrollera om han eller hon har utsatts för inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och om användningen av tvångsmedel och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning.

6.9.1 Nuvarande reglering

Genom lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet inrättades Säkerhets- och integritetsskyddsnämnden den 1 januari 2008 som ett tillsynsorgan för en rättssäker brottsbekämpning. I propositionen Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (prop. 2006/07:133 s. 31 f.) angav regeringen att även om en underrättelse lämnas till den enskilde i efterhand vid användning av hemliga tvångsmedel så är möjligheterna för honom eller henne att bedöma om åtgärden har varit rättsenlig eller inte mycket små. Regeringen föreslog därför att bestämmelserna om att den enskilde ska underrättas om tvångsmedelsanvändningen skulle förenas med en möjlighet för den enskilde att begära en kontroll av ett fristående och självständigt organ i frågan om tvångsmedelsanvändningen har varit lagen-

lig. Det var också, enligt regeringen, angeläget för allmänhetens förtroende för de brottsbekämpande myndigheterna att enskilda, när de inte har fått någon underrättelse, ska kunna få prövat om de har utsatts för en felaktig användning av hemliga tvångsmedel.

Säkerhets- och integritetsskyddsnämnden ska ha högst tio ledamöter. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Övriga ledamöter ska av regeringen utses bland personer som föreslås av partigrupperna i riksdagen.

Säkerhets- och integritetsskyddsnämnden har till uppgift att utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. Uttrycket ”sammanhängande verksamhet” innebär, t.ex. när det gäller hemlig teleövervakning, att både själva övervakningen och den vidare hanteringen av uppteckningarna omfattas av tillsynen, såsom hur överskottsinformation används eller förstörs och hur underrättelseskyldigheten fullgörs. Även den brottsbekämpande verksamhet som föregår och ligger till grund för ansökan om tvångsmedlet omfattas.

Säkerhets- och integritetsskyddsnämnden utövar sin tillsyn genom inspektioner och andra undersökningar. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps.

Säkerhets- och integritetsskyddsnämnden är skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för tvångsmedel eller därmed sammanhängande verksamhet och om detta har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde 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 nämnden de uppgifter som den begär.

6.9.2 Utredningens bedömning

Som framgår har Säkerhets- och integritetsskyddsnämnden i dag tillsyn över användningen av hemlig teleövervakning enligt rättegångsbalken och enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

För närvarande har dock Säkerhets- och integritetsskyddsnämnden inte tillsyn över de brottsbekämpande myndigheternas inhämtning av uppgifter med stöd av 6 kap. 22 § första stycket 3 LEK.

Utredningen har tidigare på flera ställen i betänkandet behandlat frågan om att den föreslagna möjligheten för de brottsbekämpande myndigheterna att inhämta uppgifter om viss elektronisk kommunikation i underrättelseverksamhet ger anledning att överväga att införa en extern och oberoende tillsyn på det området. Den uppgiften bör enligt utredningen läggas på det organ som redan inrättats för sådan tillsyn, nämligen Säkerhets- och integritetsskyddsnämnden. Utredningen föreslår därför att nämnden även ska utöva tillsyn över användningen av de nya befogenheterna i underrättelseverksamheten.

För att Säkerhets- och integritetsskyddsnämnden ska ges möjlighet att bedriva en effektiv tillsyn krävs enligt utredningen att den, utöver sina nuvarande uppgifter, löpande följer den aktuella underrättelseverksamheten hos de brottsbekämpande myndigheterna.

Det finns fördelar med att utöka Säkerhets- och integritetsskyddsnämndens organisation med egen personal för den uppgiften. Utredningen har dock kommit fram till att det är mer lämpligt att nämnden i stället ger denna tillsynsuppgift på uppdragsbasis åt lämpliga personer, t.ex. pensionerade chefsdomare. Nämndens nuvarande organisation bör därför tillföras ett eller flera s.k. granskningsombud, som för nämndens räkning följer hur de nya befogenheterna hos de brottsbekämpande myndigheterna beslutas och används i underrättelseverksamheten. Granskningsombud ska inom ramen för sitt uppdrag ha motsvarande rätt till uppgifter och biträde från de granskade myndigheterna som nämnden har. För det fall granskningsombuden finner förhållanden som är av betydelse för nämndens tillsyn ska ombuden anmäla förhållandena till nämnden. Det är alltså nämnden som även fortsättningsvis ska ta slutlig ställning i ett tillsynsärende och som uttalar sig om bland

annat konstaterade förhållanden och behov av förändringar i myndigheternas underrättelseverksamhet.

Granskningsombuden ska utses av Säkerhets- och integritetsskyddsnämnden för en bestämd tid, lämpligen högst fyra år. Uppgiften fordrar att granskningsombud fyller högt ställda krav. Utredningen föreslår därför att ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Det är självklart att ett granskningsombud inte samtidigt får vara ledamot av nämnden, men detta bör ändå uttryckligen framgå av författning.

Utredningens återkommer i avsnitt 7.1 med en bedömning av vilka resurstillskott som krävs till Säkerhets- och integritetsskyddsnämnden.

6.10 Regeringens redovisning till riksdagen

Bedömning: Regeringen redovisar i en årlig skrivelse till riksdagen användningen av hemlig teleövervakning i brottsbekämpningen. Skrivelsen bör också redovisa inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. På motsvarande sätt som i dag bör uppgifter som rör Säkerhetspolisens användning av tvångsmedel inte redovisas.

6.10.1 Nuvarande ordning

En parlamentarisk kontroll av tillämpningen av reglerna om hemlig teleavlyssning och hemlig teleövervakning utövas av riksdagen bl.a. på grundval av en skrivelse från regeringen. Regeringen får uppgifterna från Åklagarmyndigheten och Rikspolisstyrelsen, som årligen lämnar en gemensam redovisning för användningen av tvångsmedlen under föregående år. I den senaste skrivelsen, som avser användningen under år 2007 (skr. 2008/09:79), framgår att antalet fall av hemlig teleövervakning uppgick till 1 315 under året. I skrivelsen redovisas vilka brott som besluten avsett, den genomsnittliga tiden som besluten gällt, antalet fall där tvångsmedlet haft betydelse för förundersökningen, antalet fall då förundersökningen lagts ned på grund av att brott inte kunde styrkas, antalet fall då verkställighet inte kunnat ske i önskad omfattning, t.ex. på grund av tekniska problem, antalet fall då ansökan om tvångsmedlet

avslagits och antalet fall där tillstånd till tvångsmedlet meddelats efter begäran om rättslig hjälp från annat land. De fall av hemlig teleövervakning som avser Säkerhetspolisens ärenden redovisas i särskild ordning och inte i den skrivelse som lämnas till riksdagen. Säkerhetspolisens uppgifter omfattas nämligen av sekretess enligt 2 kap. 2 § och 5 kap. 1 § sekretesslagen och anses vara av synnerlig betydelse för rikets säkerhet (se 7 § sekretessförordningen [1980:657]). Tillämpningen av lagen om särskild utlänningskontroll redovisas också i skrivelse till riksdagen (senast genom skr. 2008/09:89).

Någon motsvarande redovisning till riksdagen av de fall där brottsbekämpande myndigheter har beslutat att inhämta uppgifter om elektronisk kommunikation med stöd av 6 kap. 22 § första stycket 3 LEK har inte gjorts. Trafikuppgiftsutredningens betänkande behandlade frågan om hur EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter ska genomföras i svensk rätt. Enligt artikel 10 i direktivet ska det föras statistik över antalet verkställda beslut om hemlig teleövervakning och utlämnanden enligt 6 kap. 22 § första stycket 3 LEK samt vilka typer av brott som ärendena har avsett, hur lång tid som har förlöpt från det att respektive trafikuppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften, antalet ärenden där myndigheternas begäran om att få tillgång till trafikuppgifter inte har kunnat tillgodoses av leverantörerna och vilka typer av brott ärendena har avsett (SOU 2007:76 s. 281 ff.).

6.10.2 Utredningens bedömning

I den årliga skrivelsen till riksdagen redovisar regeringen användningen av hemlig teleövervakning i brottsbekämpningen. Skrivelsen bör enligt utredningens mening också redovisa inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. På motsvarande sätt som i dag bör uppgifter som rör Säkerhetspolisens användning av tvångsmedel inte redovisas i skrivelsen.

6.11 Sekretess och tystnadsplikt

Förslag: I sekretesslagen ska det införas undantag från meddelarfriheten såvitt avser uppgifter om användning av befogenheten att inhämta uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

I lagen om elektronisk kommunikation ska det införas en tystnadsplikt för leverantörer såvitt avser uppgifter som hänför sig till användning av befogenheten att inhämta uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. En tystnadsplikt ska även införas i den lagen med avseende på åtgärd att begära in uppgift om abonnemang.

6.11.1 Nuvarande reglering

I 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 5 kap. 1 § första stycket sekretesslagen gäller sekretess för bl.a. uppgift som hänför sig till förundersökning i brottmål, 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 5 kap. 1 § andra stycket sekretesslagen 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 också att sekretess även 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. Detsamma gäller enligt bestämmelsen 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, dvs. där det behövs för att förhindra eller upptäcka brottslig verksamhet.

Det råder meddelarfrihet för de flesta uppgifter som omfattas av sekretess till skydd för brottsbeivrande verksamhet. Även uppgifter om tvångsmedel omfattas många gånger av meddelarfrihet. Dock gäller enligt 16 kap. 1 § sekretesslagen att uppgifter som omfattas av sekretess enligt 5 kap. 1 § sekretesslagen och som avser användning av hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning, postkontroll och hemlig rumsavlyssning inte omfattas av meddelarfrihet. Detsamma gäller för uppgifter som omfattas av sekretess hos leverantörerna enligt 6 kap. 20 § LEK och som avser annan uppgift som angår ett särskilt elektroniskt meddelande, dvs. uppgifter som omfattas av regleringen i 6 kap. 22 § första stycket 3 LEK. Inte heller uppgifter som omfattas av sekretess hos leverantörerna enligt 6 kap. 21 § LEK och som avser uppgift om bl.a. hemlig teleövervakning omfattas av meddelarfrihet.

Enligt 9 kap. 17 § första stycket sekretesslagen 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 9 kap. 17 § sekretesslagen 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 9 kap. 18 § sekretesslagen finns bestämmelser om att sekretessen enligt 9 kap. 17 § sekretesslagen i vissa fall inte gäller. Så är bl.a. som huvudregel fallet för uppgifter som lämnas till domstol med anledning av åtal.

Det bör nämnas att en ny offentlighets- och sekretesslag är föreslagen och avses träda i kraft den 30 juni 2009. Syftet med den nya lagen är att göra regleringen mer lättförståelig och lättillämpad.

När det gäller leverantörers tystnadsplikt för bl.a. uppgifter om elektronisk kommunikation hänvisas till avsnitt 3.10.2.

6.11.2 Utredningens bedömning

Uppgifter som på olika sätt hänför sig till förundersökning och underrättelseverksamhet är i dag föremål för sekretesskydd genom bestämmelserna i 5 kap. 1 § första och andra styckena sekretesslagen. Sekretesskyddet i dessa bestämmelser får anses vara så starkt att det inte finns skäl att föreslå någon särskild bestämmelse med anledning av förslagen. Även sekretesskyddet till förmån för enskildas personliga och ekonomiska förhållanden enligt 9 kap. 17 § sekretesslagen bedömer utredningen som tillräckligt omfattande.

När det gäller uppgifter som omfattas av sekretess enligt 5 kap. 1 § sekretesslagen och som avser användning av bl.a. hemlig teleövervakning gäller som nämndes tidigare inte någon meddelarfrihet. Likaså gäller inte meddelarfrihet för leverantörer när det gäller uppgifter som omfattas av sekretess enligt 6 kap. 21 § LEK och som avser uppgifter om bl.a. hemlig teleövervakning. En inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet kan i detta avseende jämställas med användningen av hemliga tvångsmedel i förundersökning. Utredningen menar därför att det ska finnas undantag från meddelarfriheten även för sådana uppgifter. Det gäller oavsett om sekretessen följer av 5 kap. 1 § sekretesslagen eller 6 kap. 21 § LEK. Leverantörerna har i dag tystnadsplikt enligt 6 kap. 21 § LEK för uppgift som hänför sig till angelägenhet som avser användning av bl.a. hemlig teleövervakning. Den bestämmelsen behöver kompletteras så att tystnadsplikten även avser uppgifter som hänför sig till användning av befogenheten att inhämta uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Tystnadsplikt ska även finnas i den bestämmelsen med avseende på myndigheternas åtgärd att begära in uppgift om abonnemang.

7 Konsekvenser och genomförande

7.1 Konsekvenser

Bedömning: Förslagen innebär ökade kostnader för de brottsbekämpande myndigheterna, domstolarna och Säkerhets- och integritetsskyddsnämnden. Kostnadsökningarna kan finansieras inom de befintliga ramarna för rättsväsendet.

Om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska enligt 14 § kommittéförordningen (1998:1474) en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, ska en finansiering föreslås.

Utredningens förslag innebär en förstärkt rättsäkerhet vid inhämtningen av uppgifter om elektronisk kommunikation, bl.a. genom att det införs en underrättelseskyldighet i efterhand i betydligt fler fall än i dag och genom att tillsynen över de brottsbekämpande myndigheternas verksamhet förstärks.

Som framgått tidigare föreslog BRU i betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. bl.a. att bestämmelsen i 6 kap. 22 § första stycket 3 LEK skulle upphävas och ersättas av en reglering i rättegångsbalken inom tvångsmedlet hemlig teleövervakning. Som en följd av det skulle samtliga beslut som innefattar tillgång till uppgifter om elektronisk kommunikation komma att fattas av domstol och inte av de brottsbekämpande myndigheterna själva. Enligt förslaget skulle åklagare ansöka om åtgärden hos domstolen. BRU föreslog även att åklagare skulle ha möjlighet

att i brådskande fall ge interimistiska tillstånd som rätten skyndsamt hade att pröva (SOU 2005:38 s. 182 och 200).

I kostnadsfrågan utgick BRU från att 5 000 ärenden om hemlig teleövervakning skulle prövas av domstol årligen. BRU konstaterade att det var svårt att bedöma hur ärendena skulle fördelas rent geografiskt men utgick från att den största andelen, kanske 3 000 ärenden, skulle komma att beröra storstadsregionerna. Även den genomsnittliga tidsåtgången för varje ärende var enligt BRU svår att uppskatta, men 30 minuters arbete beräknades för såväl åklagare som domare. Mot den bakgrunden menade BRU att det framför allt i de tre storstadsregionerna kunde komma att krävas ett resurstillskott i form av någon åklagar- och domartjänst i varje region och att den totala kostnaden kunde beräknas till högst tre miljoner kronor vardera för åklagar- respektive domstolsväsendet (SOU 2005:38 s. 402).

Den här utredningens förslag om en mer rättssäker inhämtning av uppgifter om elektronisk kommunikation och särskilt förslaget att utvidga underrättelseskyldigheten till enskild innebär ökade kostnader för de brottsbekämpande myndigheterna. Eftersom det inte är möjligt att redovisa statistik över hur många inhämtningar enligt lagen om elektronisk kommunikation som avser situationer som med utredningens förslag kommer att omfattas av underrättelseskyldigheten måste en uppskattning av kostnaderna göras. För polisens del kan det sammanlagda förstärkningsbehovet uppskattningsvis handla om 10–12 tjänster och en kostnad på fem miljoner kr. För Åklagarmyndigheten och Ekobrottsmyndigheten kan det röra sig om fem åklagartjänster till en kostnad på cirka fem miljoner kr. För Tullverkets del bedöms förslagen inte medföra några ökade kostnader. De ökade kostnaderna för de brottsbekämpande myndigheterna i detta avseende bedöms kunna finansieras inom de befintliga ramarna för rättsväsendet även om vissa omprioriteringar kan behöva göras.

En annan följd av utredningens förslag är att uppgifter om elektronisk kommunikation till skillnad från vad som nu gäller kommer att kunna hämtas in i förundersökningar där det inte finns någon skäligen misstänkt även i fall där brottet inte har ett straffminimum på fängelse i två år, men där det på grund av omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år. Ökade möjligheter att hämta in uppgifter om elektronisk kommunikation i förundersökningar kommer sannolikt att leda till att antalet inhämtade uppgifter kommer att öka och därmed även till

en ökning av de brottsbekämpande myndigheternas kostnader. Vidare kan inhämtningen av sådana uppgifter förväntas öka något även inom underrättelseverksamheten. En ökad inhämtning leder till ökade kostnader för att bearbeta, dokumentera och analysera den inhämtade informationen. Därtill kommer även ökade kostnader för att administrera verkställigheten av uppgiftsinhämtningen. Å andra sidan kan förslagen förväntas leda till en effektivare underrättelse och utredningsverksamhet, som i sin tur bör leda till ökade möjligheter att förebygga och förhindra brottslighet och därigenom även på sikt minskade kostnader för rättsväsendet. Sammantaget gör utredningen bedömningen att kostnadsökningarna i dessa avseenden bör kunna rymmas inom befintliga anslag.

För domstolarnas del kommer utredningens förslag om att domstolarna i vissa fall ska pröva ärenden om tillstånd till hemlig teleövervakning innan det finns en skäligen misstänkt person att leda till att något fler ärenden behöver prövas. Ökningen av antalet ärenden per år kan rimligtvis uppskattas till omkring 500, något som skulle motsvara en kostnad för domstolarna på femhundratusen kr. Denna kostnad bedöms kunna rymmas inom domstolarnas befintliga anslag.

Utredningen föreslår också en förstärkning av Säkerhets- och integritetsskyddsnämndens tillsyn av Säkerhetspolisens, den öppna polisens och Tullverkets underrättelseverksamhet med särskilda av nämnden utsedda granskningsombud. Detta medför kostnader för ersättning till ombuden, resekostnader, kostnader för lokaler, tekniskt handläggningsstöd och säkerhetsskydd. Vid bedömningen av vilken kostnad som kan uppstå har utredningen utgått från att det utses två eller flera granskningsombud som sammantaget är verksamma motsvarande två heltidstjänster. Utredningen har vidare beaktat behovet av att granskningsombud är verksamma inte bara i Stockholm utan även på några andra orter där det behöver ordnas särskilda lokaler för ombuden, som dock kan utgöras av avskilda rum inom exempelvis Säkerhetspolisens lokaler. Den årliga kostnadsökningen för Säkerhets- och integritetsskyddsnämnden kan beräknas till tre miljoner kronor. Denna kostnad ryms inte inom nämndens nuvarande anslag. Särskilda medel måste därför anvisas till nämnden. Denna kostnadsökning bedöms av utredningen kunna finansieras genom omprioriteringar inom rättsväsendets befintliga anslag. De initiala kostnader som kan uppkomma för Säkerhets och integritetsskyddsnämnden för att avskilja lokaler på nämnt sätt, inklusive att utrusta dem med eget säkerhetsskydd, bör dock kunna hanteras inom ramen för de totala resurser som nämnden kommer

att ha tillgång till. De brottsbekämpande myndigheternas arbete för att möjliggöra nämndens tillsyn bedöms också kunna rymmas inom dessa myndigheters befintliga anslag.

Förslagen har inte betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen. Förslagens betydelse för brottsligheten och det brottsförebyggande arbetet har utöver vad som tidigare angetts i detta avsnitt redovisats på andra ställen i betänkandet. I övrigt bedöms förslagen inte få några konsekvenser av de slag som anges i kommittéförordningen.

7.2 Genomförande

Förslag: Förslagen i betänkandet ska träda i kraft senast den 1 januari 2010.

Trafikuppgiftsutredningens förslag i betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76) genomför EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter i svensk rätt. Förslagen innebär bl.a. att leverantörerna får en skyldighet att lagra vissa uppgifter om elektronisk kommunikation och abonnemangsuppgifter för brottsbekämpande ändamål under ett år. Syftet är att uppgifterna ska finnas tillgängliga och kunna lämnas ut av leverantörerna till de brottsbekämpande myndigheterna när förutsättningar för det finns enligt bestämmelserna om hemlig teleövervakning i rättegångsbalken eller enligt 6 kap. 22 § första stycket 2 och 3 LEK. Utredningen föreslog inga förändringar i de nämnda bestämmelserna om myndigheternas tillgång till uppgifterna. Vissa delar av EG-direktivet ska vara genomförda i svensk rätt senast den 15 september 2007 och övriga delar senast den 15 mars 2009. Trafikuppgiftsutredningens förslag bereds för närvarande inom Regeringskansliet.

Det kan visserligen anses lämpligt att utredningens förslag träder i kraft samtidigt eller i nära anslutning till de bestämmelser som genomför EG-direktivet. Samtidigt är utredningens förslag i och för sig inte beroende av genomförandet av EG-direktivet. Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, beredning inom Regeringskansliet och riksdagsbehandling, bör de författningsändringar som utredningen föreslår kunna träda i kraft den 1 januari 2010.

8 Författningskommentar

8.1 Förslaget till lag om ändring i rättegångsbalken

27 kap. 19 §

Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram. Vad som sägs om hemlig teleövervakning ska även gälla inhämtning i hemlighet av lokaliseringsuppgifter. Med sådana uppgifter avses

1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, och
2. uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.

Hemlig teleövervakning får användas vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader,
2. brott enligt 4 kap. 9 c § brottsbalken, brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, brott enligt 1 § narkotikastrafflagen (1968:64), brott enligt 6 § första stycket lagen (2000:1225) om straff för smuggling, eller
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om sådan gärning är belagd med straff.

I fall som avses i 20 d § får hemlig teleövervakning dock användas endast vid förundersökning angående brott som kan föranleda hemlig teleavlyssning enligt 18 § andra stycket.

Paragrafen innehåller grundläggande bestämmelser om hemlig teleövervakning. Tvångsmedlet innebär enligt *första stycket* att uppgifter om telemeddelanden, både historiska uppgifter och realtidsuppgifter, hämtas in. Till uppgifter om telemeddelanden hör lokaliseringsuppgifter avseende mobil elektronisk kommunikationsutrustning när det har pågått en kommunikation. I det första stycket har den sista meningen lagts till. Vad som sägs om hemlig teleövervakning ska enligt den gälla även inhämtning i hemlighet av andra

typer av lokaliseringsuppgifter. Det är fråga om uppgifter (telefonnummer, koder och andra teleadresser) om vilka mobila elektroniska kommunikationsutrustningar, t.ex. mobiltelefoner och mobil datautrustning, som har funnits inom ett visst avgränsat geografiskt område. Sådana historiska uppgifter har de brottsbekämpande myndigheterna tidigare erhållit med stöd av lagen om elektronisk kommunikation genom vad som brukar benämnas basstationstömning (jfr 6 kap. 22 § första stycket 3 LEK). Det är också fråga om uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits, alltså lokaliseringsuppgifter (historiska uppgifter och realtidsuppgifter) som inte har samband med att utrustningen har använts för kommunikation. När de nu nämnda typerna av lokaliseringsuppgifter inhämtas är det formellt inte frågan om en hemlig teleövervakning men vad som anges om hemlig teleövervakning i författningar ska gälla även inhämtning av dessa uppgifter. Frågan har behandlats i avsnitt 6.5.

Tredje stycket i paragrafen är nytt och anger vilka brott som kan föranleda att hemlig teleövervakning kommer till stånd i de fall som anges i den föreslagna 27 kap. 20 d § RB. Det rör situationer där syftet med åtgärden är att fastställa vem som skäligen kan misstänkas för brottet eller att utröna annan omständighet av väsentlig betydelse för utredningen (se vidare kommentaren till den bestämmelsen). Hemlig teleövervakning i sådana fall får användas vid samma brott som hemlig teleavlyssning enligt 27 kap. 18 § RB, dvs. vid avsevärt färre brottstyper än vad som normalt är fallet för hemlig teleövervakning enligt paragrafens andra stycke. Bestämmelsen har motiverats i avsnitt 6.3.1.

27 kap. 20 §

Hemlig teleavlyssning och hemlig teleövervakning får, om inte annat följer av 20 d §, endast ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

1. en teleadress 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, eller
2. en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.

> Avlyssning eller övervakning får inte avse telemeddelanden som endast befordras eller har befordrats inom ett telenät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt.

Paragrafen innehåller de närmare förutsättningar som ska vara uppfyllda för att hemlig teleavlyssning och hemlig teleövervakning ska få användas. Bl.a. anges i *första stycket* att det ska finnas någon som är skäligen misstänkt för brottet för att åtgärderna ska få vidtas. Mot bakgrund av den föreslagna 27 kap. 20 d § RB, som tillåter att hemlig teleövervakning används även i fall där det saknas en skäligen misstänkt person, har det i första stycket införts en hänvisning till den nämnda bestämmelsen.

27 kap. 20 d §

> Utöver vad som anges i 20 § får hemlig teleövervakning avseende uppgifter om telemeddelanden som har befordrats eller inhämtning av lokaliseringsuppgifter ske, om åtgärden är av synnerlig vikt för utredningen och syftet är att fastställa vem som skäligen kan misstänkas för brottet eller utröna annan omständighet av väsentlig betydelse för utredningen.

Paragrafen, som har motiverats i avsnitt 6.3.1 och 6.5, är ny och ger bestämmelser om när hemlig teleövervakning får ske utöver vad som följer av 27 kap. 20 § RB. Det rör sig om inhämtning av historiska uppgifter om telemeddelanden. Det rör sig också om inhämtning av lokaliseringsuppgifter (se den föreslagna lydelsen av 27 kap. 19 § första stycket RB), dvs. uppgifter från basstationstömning och uppgifter som inte har samband med att en mobil elektronisk kommunikationsutrustning används eller har använts för kommunikation. Eftersom de sistnämnda uppgifterna kan vara både historiska uppgifter och realtidsuppgifter anges lokaliseringsuppgifter uttryckligen i lagtexten vid sidan av historiska uppgifter om telemeddelanden.

Det första kravet enligt paragrafen är att åtgärden ska vara av synnerlig vikt för utredningen. Innebörden av rekvisitet 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 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 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 skall 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 åtgärden nödvändig. Nödvändiga uppgifter ska i princip inte kunna inhämtas med andra medel och det ska finnas skäl att räkna med att tvångsmedelsanvändningen ensam eller i förening med andra åtgärder verkligen kan få effekt.

Vid sidan om kravet på synnerlig vikt och att utredningsläget ska göra inhämtningen nödvändig, finns enligt paragrafen krav även på vilket syfte åtgärden ska ha i förundersökningen.

Ett av de tillåtna syftena är att åtgärden genomförs för att fastställa vem som skäligen kan misstänkas för brottet. Så kan vara fallet när det helt saknas en skäligen misstänkt person i utredningen. Det syftet kan också finnas när någon eller några personer redan bedöms som skäligen misstänkta och de brottsbekämpande myndigheterna söker utreda andra personers inblandning i den brottsliga verksamheten. Åtgärden kan i dessa fall inte avse teleadresser med sådan koppling till en skäligen misstänkt som avses i 27 kap. 20 § första stycket RB.

Det andra tillåtna syftet uttrycks i paragrafen så att den brottsbekämpande myndigheten söker utröna annan omständighet av väsentlig betydelse för utredningen. Så kan t.ex. vara fallet när man genom uppgifterna kan få fram var en målsägande eller ett vittne befinner sig eller har befunnit sig, eller var en brottsplats är belägen.

Till skillnad från bestämmelsen i 27 kap. 20 § RB anges inte i förevarande bestämmelse vilka teleadresser åtgärden får avse. Kravet på synnerlig vikt för att den hemliga teleövervakningen ska få genomföras och det syfte åtgärden får ha enligt paragrafen sätter dock, tillsammans med proportionalitetsprincipen (se 27 kap. 1 § tredje stycket RB), i det enskilda fallet en gräns för vilka teleadresser som kan bli aktuella att övervaka.

27 kap. 21 §

> Frågor om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning prövas av rätten på ansökan av åklagaren. Om hemlig teleövervakning inte kan antas bli av stor omfattning eller av särskilt ingripande slag, får frågor enligt 20 d § även prövas av undersökningsledaren eller åklagaren.
>
> I ett beslut att tillåta åtgärder enligt första stycket ska det anges vilken tid tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.
>
> I ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning ska det anges vilken teleadress som tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga telenät. I ett beslut att tillåta inhämtning av lokaliseringsuppgifter ska det anges vilken teleadress eller vilket avgränsat geografiskt område tillståndet avser.
>
> I ett tillstånd till hemlig kameraövervakning ska det anges vilken plats tillståndet gäller.

Paragrafen innehåller bestämmelser om hur en fråga om hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning ska prövas och vad som ska anges i ett beslut om tillstånd.

Enligt *första stycket* första meningen är det rätten som prövar frågorna om hemlig teleavlyssning, hemlig teleövervakning respektive hemlig kameraövervakning. I de situationerna är åklagare förundersökningsledare. Andra meningen i stycket är ny och föreskriver att om hemlig teleövervakning inte kan antas bli av stor omfattning eller av särskilt ingripande slag, får frågor enligt 27 kap.

20 d § RB även prövas av undersökningsledaren eller åklagaren. Det rör fall när syftet är att fastställa vem som är skäligen misstänkt eller att utröna annan omständighet av väsentlig betydelse för utredningen. Frågan har behandlats i avsnitt 6.3.2. Det är undersökningsledaren eller åklagaren som i första hand ska pröva frågorna i de situationerna. Besluten ska dokumenteras noggrant. Kan åtgärden antas bli av stor omfattning, t.ex. när den avser totalt sett långa historiska tidsperioder eller ett stort antal personer, ska frågan om tillstånd som regel prövas av rätten. Även fast en basstationstömning oftast omfattar många personer, är den normalt inte av sådan omfattning att det krävs domstolsbeslut. Som regel ska åtgärden också prövas av rätten när uppgifterna kan antas bli av särskilt ingripande slag. Det kan t.ex. vara fråga om uppgifter som avser någon som arbetar med källskyddad information på ett medieföretag eller någon offentlig befattningshavare. Bedömningen får göras utifrån den information den brottsbekämpande myndigheten har tillgänglig före beslutet.

Bestämmelsen innebär att det kan förekomma att såväl domstol som åklagare och annan förundersökningsledare, beroende på omständigheterna, fattar beslut om hemlig teleövervakning i samma förundersökning. Om det i samband med att domstol prövar om tillstånd ska ges till hemlig teleövervakning mot en skäligen misstänkt person, finns skäl att genomföra åtgärden även i syfte att fastställa om andra personer är skäligen misstänkta, kan det, även om det inte formellt krävs, finnas praktiska skäl till att domstol, på åklagares begäran, samtidigt ger tillstånd i fall som avses i 27 kap. 20 d § RB, även om åtgärden inte kan antas bli av stor omfattning eller av särskilt ingripande slag. Om det i ett fall där domstolen bör besluta om åtgärden är bråttom att få frågan prövad, har åklagaren möjlighet, enligt den föreslagna 27 kap. 21 a § RB, att ge interimistiskt tillstånd till åtgärden.

I *tredje stycket* har den tredje meningen lagts till. I ett beslut om att tillåta inhämtning av lokaliseringsuppgifter ska det, förutom vad som anges i bestämmelsens andra stycke om tillståndstiden, även anges vilken teleadress eller vilket avgränsat geografiskt område tillståndet avser. Teleadress kan inte finnas i tillståndet vid inhämtning av lokaliseringsuppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, alltså vid basstationstömning. Det avgränsade geografiska området kan anges med t.ex. en viss bestämd gatuadress,

men kan också anges med större områden, t.ex. färdvägar och liknande.

27 kap. 21 a §

> Kan det befaras att inhämtande av rättens tillstånd till hemlig teleövervakning skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden, i avvaktan på rättens beslut, ges av åklagaren.
>
> Har åklagaren gett ett sådant interimistiskt tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har ett interimistiskt beslut om övervakning upphört att gälla innan rätten har prövat ärendet ska åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Paragrafen är ny och ger åklagaren rätt att ge interimistiska tillstånd till hemlig teleövervakning när annars domstol skulle ha fattat beslutet enligt 27 kap. 21 § första stycket första meningen RB. Tillståndet får ha samma omfattning som det domstolsbeslut som inte kan inväntas. Det får därmed avse såväl uppgifter om telemeddelanden som lokaliseringsuppgifter. Uppgifterna kan i förekommande fall vara både historiska och inhämtas i realtid. Det kan också vara fråga om såväl den situation när det finns en skäligen misstänkt person som när en sådan person saknas (jfr 27 kap. 20 d § RB).

Förutsättningen för att åklagaren ska få ge tillstånd är enligt *första stycket* att det kan befaras att inhämtande av rättens tillstånd skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. I detta ligger att paragrafen ska kunna tillämpas endast i situationer där ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle avvaktas. Så kan exempelvis vara fallet när en hemlig teleövervakning verkställs samtidigt som de brottsbekämpande myndigheterna upptäcker att en misstänkt person använder en teleadress som inte omfattas av tillståndet. Ett annat exempel är att någon under en pågående hemlig teleövervakning har identifierats som skäligen misstänkt och att de förutsättningar för tvångsmedlet som ställs upp i 27 kap. 20 d § RB därmed inte längre finns och att beslutet därmed måste hävas (jfr 27 kap. 23 § RB), samtidigt som det i och för sig finns

förutsättningar att besluta om tvångsmedlet enligt 27 kap. 20 § RB mot den skäligen misstänkte.

I paragrafens *andra stycke* föreskrivs att åklagaren, om han eller hon har gett tillstånd till hemlig teleövervakning, genast ska göra en skriftlig anmälan om åtgärden hos rätten. Med "genast" avses att ett beslut respektive en anmälan ska göras i ett sammanhang. 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 (jfr 27 kap. 28 § RB). Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva åklagarens tillstånd.

I andra stycket föreskrivs också att om åklagarens beslut om tillstånd till hemlig teleövervakning har upphört att gälla innan rätten har prövat ärendet ska åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden. Med uttrycket att beslutet har upphört avses att några ytterligare uppgifter inte kan inhämtas från leverantören med stöd av detsamma.

Rätten får i dessa fall avskriva ärendet från vidare handläggning, eftersom frågan har fallit.

Motiven till bestämmelsen har redovisats i avsnitt 6.3.2.

27 kap. 21 b §

> Har hemlig teleövervakning avseende en viss teleadress beslutats utan rättens prövning enligt 21 § får den som innehar teleadressen begära rättens prövning av beslutet. Rätten ska skyndsamt pröva ärendet. Finner rätten att det inte finns skäl för åtgärden, ska den upphäva beslutet. Har beslutet om övervakning upphört att gälla innan rätten har prövat ärendet ska undersökningsledaren eller åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

I paragrafen, som är ny, finns bestämmelser om rätt att i vissa fall begära rättens prövning av beslut om hemlig teleövervakning. Frågan har behandlats i avsnitt 6.7. Tingsrättens beslut om hemlig teleövervakning får överklagas enligt 49 kap. 5 § första stycket 6 RB (se även 52 kap. 7 § tredje stycket RB rörande bl.a. inhibition). Möjligheten att överklaga tillkommer i praktiken endast åklagaren och det offentliga ombudet (se 27 kap. 26 § RB), eftersom den misstänkte i normalfallet inte har kännedom om beslutet om det hemliga tvångsmedlet. Skulle det bli klarlagt att den misstänkte har sådan kännedom, kommer åklagaren säkerligen att behöva häva beslutet eftersom det inte längre finns skäl för det (27 kap. 23 §

RB). Den som innehar en viss teleadress som hemlig teleövervakning har avsett ska ändå ha möjlighet enligt den föreslagna paragrafen att få rättens prövning av de beslut som fattats av undersökningsledaren eller åklagaren. Det är då fråga om beslut enligt 27 kap. 21 § RB och inte åklagarens interimistiska tillstånd enligt den föreslagna 27 kap. 21 a § RB. Att rättens prövning får begäras av den som innehar den teleadress som beslutet om hemlig teleövervakning har avsett innebär att rätt till domstolsprövning inte finns när åtgärden är en basstationstömning, eftersom den då inte har avsett en viss teleadress. Rätten ska skyndsamt ta upp ärendet till prövning. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet. Skulle beslutet om hemlig teleövervakning ha upphört att gälla innan rätten har prövat ärendet, ska undersökningsledaren eller åklagaren anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden. Med uttrycket att beslutet har upphört avses att några ytterligare uppgifter inte kan inhämtas från leverantören med stöd av detsamma.

Rätten får i dessa fall avskriva ärendet från vidare handläggning, eftersom frågan har fallit.

27 kap. 23 §

> Om det inte längre finns skäl för ett beslut om hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning, ska undersökningsledaren, åklagaren eller rätten omedelbart häva beslutet.

Paragrafen innebär att ett beslut om hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning ska hävas när det inte längre finns skäl för beslutet. I bestämmelsen har undersökningsledare lagts till vid sidan av åklagaren och rätten som behöriga att fatta beslut om ett sådant hävande. Ändringen har skett mot bakgrund av att undersökningsledaren respektive åklagaren har fått rätt enligt 27 kap. 21 § första stycket andra meningen RB att fatta beslut om hemlig teleövervakning i de fall syftet är att fastställa vem som skäligen kan misstänkas för brottet eller utröna annan omständighet av väsentlig betydelse för utredningen (den föreslagna 27 kap. 20 d § RB). Skulle syftet i ett sådant fall har blivit uppfyllt så att de brottsbekämpande myndigheterna kan konstatera t.ex. att en viss person är skäligen misstänkt, måste beslutet hävas enligt den nu aktuella bestämmelsen. Om myndigheterna anser att det finns tillräckliga

skäl för en fortsatt hemlig teleövervakning, behöver åklagaren begära rättens prövning av den frågan enligt 27 kap. 21 § första stycket första meningen RB. För att utredningsresultatet inte ska äventyras kan åklagaren, om förutsättningarna är uppfyllda enligt den föreslagna 27 kap. 21 a § RB, ge ett interimistiskt tillstånd till åtgärden i avvaktan på rättens tillstånd.

27 kap. 33 §

Om det gäller sekretess enligt 2 kap. 1 eller 2 §, 5 kap. 1 § eller 9 kap. 17 § sekretesslagen (1980:100) för uppgifter som avses i 32 §, ska en underrättelse enligt 31 § skjutas upp till dess att sekretess inte längre gäller.

Har det på grund av sekretess enligt första stycket inte kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, får underrättelsen underlåtas.

En underrättelse enligt 31 § ska inte lämnas, om förundersökningen angår

1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
2. brott som avses i 13 kap. 4 eller 5 § brottsbalken,
3. brott som avses i 18 kap. 1, 3, 4, 5 eller 6 § eller 19 kap. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 eller 13 § brottsbalken,
4. brott som avses i 3 eller 4 kap. brottsbalken, om brottet är av det slag som anges i 18 kap. 2 § eller 19 kap. 11 § samma balk,
5. brott som avses i 2 § lagen (2003:148) om straff för terroristbrott eller 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., eller
6. försök, förberedelse eller stämpling till brott som anges i 1–5 eller underlåtenhet att avslöja sådant brott, om gärningen är belagd med straff.

En underrättelse enligt 31 § ska inte heller lämnas när

1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område har inhämtats,
2. integritetsintrånget för den enskilde annars kan antas vara ringa, eller
3. uppgift om vem som innehar teleadressen inte fastställs.

Paragrafen reglerar de situationer när en underrättelse till enskild enligt 27 kap. 31 § RB ska skjutas på framtiden eller helt underlåtas. *Sista stycket* är nytt och har motiverats i avsnitt 6.8. Tillägget innebär att en underrättelse inte ska lämnas när uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område har inhämtats, dvs. när

en basstationstömning har genomförts. Tillägget innebär också att underrättelse inte ska lämnas när integritetsintrånget för den enskilde annars kan bedömas som ringa. Det tar bl.a. sikte på den bearbetning som sker i steget efter en basstationstömning när de brottsbekämpande myndigheterna hämtar in ytterligare uppgifter rörande de teleadresser som basstationstömningen givit uppgift om. Det kan också vara frågan om att uppgifter hämtas in i ett inledande spaningsskede om vissa intressanta teleadresser utan att det dessförinnan har genomförts en basstationstömning men med det främsta syftet att avföra personer från den vidare utredningen. Tillägget innebär dessutom att underrättelse inte ska lämnas när uppgift om vem som innehar den teleadress som hemlig teleövervakning har avsett inte fastställs. Att det inte fastställs vem som innehar en viss teleadress innebär inte att myndigheterna får en utredningsbörda i det avseendet. Myndigheten behöver inte lägga ner resurser på att identifiera personer som finns bakom t.ex. anonyma kontantkort i mobiltelefon.

8.2 Förslaget till lag (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

1 §

> Denna lag innehåller bestämmelser om brottsbekämpande myndigheters rätt att i underrättelseverksamhet i hemlighet hämta in uppgifter om viss elektronisk kommunikation från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Om det i annan lag finns bestämmelser som avviker från denna lag ska de bestämmelserna gälla.

Paragrafen upplyser i korthet om vad lagens bestämmelser ger de brottsbekämpande myndigheterna för befogenhet i underrättelseverksamhet. Det är fråga om att hämta in uppgifter om viss elektronisk kommunikation. Vilka typer av uppgifter det rör framgår av 2 §. Lagen omfattar inte uppgifter från trådlös kommunikation, som radio- och satellitkommunikation, eftersom etern under lång tid har ansetts vara fri (se 6 kap. 17 och 24 §§ LEK och prop. 2002/03:110 s. 396). Uppgifterna inhämtas från den som enligt

lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Det är fråga om samma krets av leverantörer som omfattas av tystnadsplikten enligt 6 kap. 20 och 21 §§ LEK. Paragrafens sista mening uttrycker att om det i lag finns andra bestämmelser som avviker från lagen ska de bestämmelserna gälla. Genom bestämmelserna i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott ges myndigheterna befogenhet att använda vissa tvångsmedel, bl.a. hemlig teleövervakning, i myndigheternas förebyggande verksamhet. Tillstånd till tvångsmedlen kan meddelas om det finns särskild anledning att anta att en viss person kommer att utöva brottslig verksamhet som innefattar brott som hör till Säkerhetspolisens ansvarsområde och vissa andra angivna brott. Skulle förutsättningarna vara uppfyllda för att använda hemlig teleövervakning enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott ska den lagen tillämpas i stället för den här aktuella lagen. Ett ytterligare exempel på en sådan reglering är lagen om särskild utlänningskontroll.

2 §

Inhämtning får avse

1. uppgifter om telemeddelanden som har befordrats till eller från en viss teleadress,
2. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, eller
3. uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.

Paragrafen reglerar vilka typer av uppgifter som får inhämtas enligt lagen. Det rör historiska uppgifter om telemeddelanden samt lokaliseringsuppgifter. I kommentaren till ändringen i bestämmelsen i 27 kap. 19 § första stycket RB framgår närmare vad som avses med uppgifter om telemeddelanden respektive lokaliseringsuppgifter.

3 §

Inhämtning av uppgifter får ske i en undersökning om det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 4, 5 a första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. olovlig kårverksamhet eller brott mot medborgerlig frihet enligt 18 kap. 4 eller 5 § brottsbalken,
4. spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet enligt 19 kap. 5, 7, 8 eller 10 § brottsbalken,
5. företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning, eller
6. brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

Paragrafen innehåller förutsättningarna för att de uppgifter som anges i 2 § ska få hämtas in. Motiven till regleringen har redovisats i avsnitt 6.4.2.

Inhämtning av uppgifter får ske i en undersökning om det finns särskild anledning att anta att uppgifterna kan bidra till 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 de brottsbekämpande 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, operationsplan, aktionsgrupp och insats. Att inhämtningen på detta sätt knyts till en viss undersökning är också av värde för den tillsyn som ska ske över myndigheternas verksamhet.

Begreppen förebygga, förhindra och upptäcka används för att beskriva underrättelseverksamheten på samma sätt som i exempelvis 7 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och 2 kap. 5 § förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet (Ds 2007:43).

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 upptäcka 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.

Genom rekvisitet ”brottslig verksamhet” framgår att regleringen inte ställer upp något krav på att det ska finnas en misstanke om ett specifikt brott. Det föreligger därför en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt bl.a. rättegångsbalken som i princip förutsätter att ett specifikt brott har begåtts. Däremot måste den befarade brottsliga verksamheten innefatta någon av de gärningar som räknas upp i punkterna 1–6. Uppgifterna får alltså hämtas in om någon del av den brottsliga verksamhet som t.ex. en viss gruppering antas syssla med innefattar vissa uppräknade gärningar.

Punkten 1 i uppräkningen innefattar de brott som tidigare angavs i 6 kap. 22 § första stycket 3 LEK, dvs. brott med minst två års fängelse i straffskalan. Eftersom det är fråga om underrättelseverksamhet saknas det anledning att på samma sätt som vid förundersökning rörande ett redan begånget brott, föreskriva att uppgifter får inhämtas vid osjälvständiga brottsformer (jfr t.ex. 27 kap. 18 och 19 §§ RB). Genom punkterna 1–6 kommer all brottslighet som omfattas av lagen om åtgärder för att utreda vissa samhällsfarliga brott att omfattas även av denna lag.

4 §

Inhämtning av uppgifter beslutas av chefen för den brottsbekämpande myndigheten. Myndighetschefen får delegera beslutanderätten.

Enligt paragrafen, som har motiverats i avsnitt 6.4.3, är det chefen för den brottsbekämpande myndigheten som beslutar om inhämtning av uppgifter enligt lagen. Beslutanderätten ligger därmed för polisens del på rikspolischefen och länspolismästarna och för tullens del på generaltulldirektören. Med myndighetschef avses även säkerhetspolischefen.

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 mer aktivt deltar i den underrättelseverksamhet där uppgifterna ska användas. I stället är det fråga om personer på myndighetsledningsnivå, t.ex. myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen, biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet.

Ekobrottsmyndigheten är en åklagarmyndighet. Den brottsliga verksamhet som finns angiven i 3 § är så allvarlig att den inte omfattar de brott som i dag faller under Ekobrottsmyndighetens ansvarsområde. Om det blir aktuellt i framtiden så bör det för Ekobrottsmyndighetens underrättelseverksamhet vara rikspolischefen som delegerar beslutanderätten till den som leder polisverksamheten vid Ekobrottsmyndigheten.

5 §

> I ett beslut om inhämtning av uppgifter ska det anges vilken tid och, i förekommande fall, vilken teleadress och vilket avgränsat geografiskt område tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.
>
> Inhämtning av uppgifter får beslutas och genomföras endast om 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.

Paragrafens *första stycke* reglerar vilka uppgifter ett beslut om inhämtning av uppgifter ska innehålla och motsvarar i princip vad som gäller vid hemlig teleövervakning enligt 27 kap. 21 § andra stycket RB. Den tid som ska anges får inte bestämmas längre än nödvändigt. Det gäller för såväl historiska uppgifter som realtidsuppgifter (uppgifter om i vilket avgränsat geografiskt område en

viss mobil elektronisk kommunikationsutrustning finns). När det gäller de sistnämnda uppgifterna finns den ytterligare begräsningen att tiden inte får överstiga en månad från dagen för beslutet. I förekommande fall ska även teleadress och det avgränsade geografiska område som tillståndet avser anges i beslutet. Teleadress kan inte anges när uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område hämtas in, dvs. vid basstationstömning. När det gäller lokaliseringsuppgifterna blir det oftast aktuellt att ange t.ex. en viss bestämd gatuadress men också större områden, exempelvis färdvägar och liknande.

Den för samtliga tvångsmedel gällande proportionalitetsprincipen utrycks i *andra stycket* i paragrafen. Principen brukar i korthet beskrivas på det sättet att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Bestämmelsen innebär att den brottsbekämpande myndigheten alltid måste beakta principen när den prövar om inhämtning av uppgifter ska få ske enligt denna lag. Proportionalitetsprincipen får betydelse också för hur beslutet ska utformas och vilka villkor som eventuellt ska förenas med det. Den gäller vidare under hela verkställighetsförfarandet och ska alltså, även sedan beslut om inhämtning har fattas, beaktas självmant av myndigheten. Man kan alltså tänka sig en situation när integritetsintrånget under verkställigheten blir så stort att åtgärden att hämta in uppgifter inte längre kan anses tillåten, trots att det fortfarande enligt 3 § finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

6 §

Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter ska beslutet omedelbart hävas.

Paragrafen överensstämmer i princip med vad som gäller för hemlig teleavlyssning och hemlig teleövervakning enligt 27 kap. 23 § RB. Om det under den tid som inhämtning av uppgifter får ske t.ex. har kommit fram att förutsättningar för beslutet har fallit bort genom att den brottsliga verksamhet som avsågs förhindras har genomförts, ska den brottsbekämpande myndigheten häva beslutet. Finns

det i sådant fall fortfarande tillräckliga skäl för att inhämta uppgifter kan det bli aktuellt att besluta om hemlig teleövervakning enligt rättegångsbalkens regler.

7 §

Om det genom inhämtningen av uppgifter har kommit fram information om förestående brott, får uppgifterna användas för att förhindra brott.

Om det genom inhämtningen av uppgifter har kommit fram information som är av betydelse för utredningen av ett brott, får uppgifterna användas i utredningen endast om beslut om hemlig teleövervakning har fattats.

Paragrafen reglerar de brottsbekämpande myndigheternas användning av uppgifterna som har hämtats in enligt lagen. Motiven till bestämmelsen har redovisats i avsnitt 6.4.4.

Om det genom inhämtningen av uppgifter har kommit fram information om förestående brott, får enligt *första stycket* uppgifterna i enlighet med underrättelseverksamhetens syfte användas för att förhindra brott.

I paragrafens *andra stycke* finns av integritetsskäl begränsningar när det gäller de brottsbekämpande myndigheternas användning i förundersökning av de uppgifter som hämtats in enligt lagen. Det kan t.ex. vara fråga om att ett förestående brott inte kunde förhindras utan genomfördes eller att uppgifterna är av betydelse för utredningen av något annat brott. De uppgifter som har inhämtats får användas i en förundersökning endast om beslut om hemlig teleövervakning har fattats. När den åtgärden har beslutats får myndigheten välja efter operativa, ekonomiska och andra överväganden om uppgifterna återigen ska inhämtats via leverantören eller lämnas över till brottsutredningsverksamheten från den undersökning i underrättelseverksamheten i vilken de hämtades in.

8 §

Uppteckningar av uppgifter ska granskas snarast möjligt.

Uppteckningar ska, i de delar de är av betydelse för att förebygga eller förhindra brott, bevaras så länge det behövs för att förebygga eller förhindra brott. De ska därefter förstöras.

Trots vad som sägs i andra stycket får brottsbekämpande myndigheter behandla uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag.

I paragrafen regleras de brottsbekämpande myndigheternas hantering och behandling av uppteckningar av uppgifter som inhämtats enligt denna lag. Motiven till bestämmelsen har redovisats i avsnitt 6.4.5.

Enligt *första stycket* ska en uppteckning av uppgifter, på samma sätt som vid hemlig teleövervakning (jfr 27 kap. 24 § RB), granskas snarast möjligt. Den brottsbekämpande myndigheten utför granskningen.

Enligt *andra stycket* ska de delar av uppteckningen som är av betydelse för att förebygga eller förhindra brott bevaras så länge det behövs för det syftet. När uppteckningen inte längre ska bevaras, ska den förstöras. Med det avses att uppgifterna utplånas, inte enbart att uppgifterna görs oåtkomliga för den operativa verksamheten.

Finns det delar av uppteckningen som är av betydelse från brottsutredningssynpunkt och har beslut om hemlig teleövervakning fattats (se 7 §), blir de bestämmelser som reglerar hanteringen och behandlingen av uppteckningen vid det tvångsmedlet tillämpliga (jfr 27 kap. 24 § RB).

Tredje stycket innehåller ett undantag från vad som föreskrivs om förstörande av uppteckningar enligt andra stycket. Enligt undantagsregeln får de brottsbekämpande myndigheterna behandla uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag. Om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen eller lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, utgör alltså regleringen i andra stycket inte hinder för att nämnda uppgifter behandlas enligt dessa lagar. I fråga om gallring m.m. av uppgifterna gäller då vad som föreskrivs i de lagarna.

9 §

I lagen (2007:908) 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 när det gäller att inhämta uppgifter enligt lagen. Bestämmelsen har införts mot bakgrund av att den enskilde som innehar den teleadress som omfattas av beslutet om inhämtning inte har möjlighet att överklaga ett sådant beslut (jfr 49 kap. 5 § första stycket 6 RB) eller begära rättens prövning av det (jfr den föreslagna 27 kap. 21 b § RB). Enligt lagen om tillsyn över viss brottsbekämpande verksamhet har den enskilde dock alltid rätt att begära att nämnden kontrollerar om han eller hon har utsatts för en sådan åtgärd och om detta har skett i enlighet med lag eller annan författning. För närmare uppgifter om nämndens tillsyn hänvisas till avsnitt 6.9.

8.3 Förslaget till lag om ändring i sekretesslagen (1980:100)

16 kap. 1 §

Att friheten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter i vissa fall är begränsad framgår av 7 kap. 3 § första stycket 1 och 2, 4 § 1–8 samt 5 § 1 och 3 tryckfrihetsförordningen och av 5 kap. 1 § första stycket samt 3 § första stycket 1 och 2 yttrandefrihetsgrundlagen. De fall av uppsåtligt åsidosättande av tystnadsplikt, i vilka nämnda frihet enligt 7 kap. 3 § första stycket 3 och 5 § 2 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 3 yttrandefrihetsgrundlagen i övrigt är begränsad, är de där tystnadsplikten följer av

---

3. denna lag enligt

---

5 kap. 1 §	såvitt avser 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, eller inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättel-

	severksamhet
9. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation	
6 kap. 21 § lagen (2003:389) om elektronisk kommunikation	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag eller om hemlig teleavlyssning och hemlig teleövervakning på grund av beslut av domstol, undersökningsledare eller åklagare, eller inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

I paragrafen anges i vilka fall tystnadsplikt har företräde framför meddelarfrihet.

Sekretessen enligt 5 kap. 1 § sekretesslagen, som skyddar brottsutredningar och annan brottsbekämpande verksamhet, innebär endast ett fåtal begränsningar i meddelarfriheten. De begränsningar som finns rör uppgifter om hemliga tvångsmedel, dvs. tvångsmedel som verkställs utan att den som blir utsatt för åtgärden har vetskap om den. För närvarande är meddelarfriheten begränsad i fråga om uppgift om s.k. postkontroll, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och hemlig rumsavlyssning, s.k. buggning.

Åtgärden att hämta in uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet enligt den föreslagna lagen därom, är till sin karaktär sådan att den måste hållas hemlig. Av förevarande paragraf följer därför att samma begränsningar i meddelarfriheten som gäller för befintliga hemliga tvångsmedel när tystnadsplikten följer av 5 kap. 1 § sekretesslagen ska gälla även för sådan inhämtning.

I 6 kap. 21 § LEK föreskrivs en tystnadsplikt för den som i samband med ett tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till uppgifter som hänför sig till postkontroll, hemlig teleavlyssning eller hemlig teleövervakning. Sådana uppgifter omfattas även av begränsningar i meddelarfriheten. Av samma skäl som nyss angavs har förevarande paragraf ändrats så att begränsningar i meddelarfriheten ska gälla för åtgärden att hämta in upp-

gifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet enligt den angivna lagen när tystnadsplikten följer av 6 kap. 21 § LEK (se även avsnitt 8.4).

8.4 Förslaget till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap. 8 §

Bestämmelserna i 5–7 §§ gäller inte

1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 5 § för att lösa tvister,
2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning, inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

I 6 kap. 5–7 §§ LEK finns bestämmelser om hur leverantörerna får behandla vissa trafikuppgifter. De ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Uppgifterna får dock sparas för vissa ändamål, exempelvis abonnentfakturering. I paragrafen görs undantag från de nämnda reglerna, bl.a. vid beslut om hemlig teleövervakning. I punkten 2 har en hänvisning till lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet lagts till.

6 kap. 10 a §

Bestämmelserna i 9 och 10 §§ gäller inte när lokaliseringsuppgifter omfattas av beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Paragrafen är ny.

I 6 kap. 9 och 10 §§ LEK finns bestämmelser om hur leverantörer får behandla lokaliseringsuppgifter som inte är trafikuppgifter, exempelvis uppgifter som avser en enbart påslagen mobiltelefon, alltså lokaliseringsuppgifter som inte har samband med befordran av ett elektroniskt meddelande. Uppgifter som rör fysiska personer eller abonnenter får behandlas endast sedan de har avidentifierats eller abonnenten gett sitt samtycke till behandlingen. Det finns också begränsningar i fråga om vilka personer som får ta befattning med uppgifterna.

De angivna bestämmelserna om behandling av lokaliseringsuppgifter som inte är trafikuppgifter kan inte tillämpas när sådana uppgifter omfattas av beslut om inhämtning enligt 27 kap. rättegångsbalken eller enligt den föreslagna lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Paragrafen föreskriver därför undantag i det avseendet (jfr 6 kap. 8 § LEK).

6 kap. 21 §

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,
2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18, 19 eller 20 d § rättegångsbalken eller tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,
3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
4. inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, och
5. begäran om utlämnande enligt 22 § första stycket 2.

Paragrafen innehåller vissa bestämmelser om tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till uppgifter som hänför sig till vissa hemliga tvångsmedel, dvs. tvångsmedel som verkställs utan att den som blir utsatt för åtgärden har vetskap om den.

Även hemlig teleövervakning enligt 27 kap. 20 d § RB, inhämtning enligt lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet liksom begäran från myndigheterna att få tillgång till uppgifter om abonnemang är till sin karaktär sådana åtgärder som måste hållas hemliga. Punkten 2 i paragrafen har därför ändrats och punkterna 4 och 5 har lagts till. Frågan har behandlats i avsnitt 6.11.

6 kap. 22 §

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (1970:428), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,
2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet,
3. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,
4. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),
5. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),
6. uppgift som avses i 20 § första stycket 1 till polismyndighet eller åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och
7. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

Ersättning för att lämna ut uppgifter enligt första stycket 7 ska vara skälig med hänsyn till kostnaderna för utlämnandet.

I bestämmelsen föreskrivs skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst att utan hinder av tystnadsplikt lämna ut vissa uppgifter till bl.a. brottsbekämpande myndigheter.

Enligt *första stycket punkten 2* har de brottsbekämpande myndigheterna rätt att få tillgång till uppgifter om abonnemang. Det gäller såväl i underrättelseverksamhet som under förundersökning. Den tidigare begränsningen, som innebar dels att fängelse skulle vara föreskrivet för brottet, dels att brottet skulle kunna föranleda annan påföljd än böter i det enskilda fallet, för att myndigheterna skulle ha rätt att begära uppgifterna har tagits bort. Frågan har behandlats i avsnitt 6.6.

I *första stycket punkten 3* föreskrevs tidigare en skyldighet att lämna uppgifter som angår ett särskilt elektroniskt meddelande till de brottsbekämpande myndigheter som ska ingripa mot ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Den bestämmelsen har utgått. Myndigheternas möjligheter att få tillgång till sådana uppgifter regleras i stället i rättegångsbalken respektive lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Som en följd av den angivna förändringen har numreringen i första stycket samt hänvisningen i andra stycket ändrats.

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

2 §

Nämnden ska utöva sin tillsyn genom inspektioner och andra undersökningar.

Nämnden ska biträdas av granskningsombud med uppgift att löpande följa tillämpningen av lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Ombud ska till nämnden anmäla förhållanden av betydelse för nämndens tillsyn.

Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps.

I paragrafen finns grundläggande bestämmelser om hur Säkerhets- och integritetsskyddsnämnden ska bedriva sin tillsynsverksamhet. Av första stycket framgår att nämndens löpande tillsyn ska genomföras i form av inspektioner eller andra slag av undersökningar. Undersökningarna utformas efter omständigheterna i det enskilda tillsynsärendet och kan alltså vara av olika art och omfattning.

I ett nytt *andra stycke* har särskilda bestämmelser införts om nämndens tillsyn över tillämpningen av lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. I den verksamheten ska nämnden biträdas av ett eller flera granskningsombud som löpande ska följa hur lagen tillämpas och anmäla till nämnden sådana förhållanden som är av betydelse för nämndens tillsyn. Frågan har behandlats i avsnitt 6.9.

Tredje stycket var tidigare andra stycke i bestämmelsen och reglerar vad nämndens tillsyn kan utmynna i.

4 §

> Nämnden har rätt att 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 nämnden de uppgifter som den begär. Granskningsombud har inom ramen för sitt uppdrag motsvarande rätt till uppgifter och biträde.

I paragrafen föreskrivs en uppgifts- och biträdesskyldighet för de myndigheter som omfattas av Säkerhets- och integritetsskyddsnämndens tillsyn. Myndigheterna är skyldiga att lämna de uppgifter och det biträde som nämnden begär. Nämnden avgör själv om en uppgift är relevant för tillsynen. Myndigheterna är skyldiga att lämna de begärda uppgifterna även om det förutsätter efterforskning från myndigheternas sida. Vidare föreskrivs att myndigheter som omfattas av tillsynen är skyldiga att biträda nämnden. Sådant biträde kan bestå i att lokaler, arkiv, register och andra databaser som omfattas av ett tillsynsärende görs tillgängliga för nämnden. Också domstolar och förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att på begäran lämna upplysning till nämnden. För sådana myndigheter finns dock ingen skyldighet föreskriven att biträda nämnden. Som en följd av den uppgiftsskyldighet

som föreskrivs i paragrafen kan begärda uppgifter lämnas till nämnden utan hinder av att sekretess annars gäller (jfr 14 kap. 1 och 2 §§ sekretesslagen). Sekretesskyddet för uppgift som nämnden erhållit av annan myndighet gäller i samma utsträckning hos nämnden som hos myndigheten (11 kap. 6 § sekretesslagen).

I paragrafen har den *sista meningen* lagts till. De granskningsombud som biträder nämnden vid tillsynen över tillämpningen av lagen om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet har samma rätt till uppgifter och biträde inom ramen för sitt uppdrag som nämnden har.

6 §

> Nämnden utser ett eller flera granskningsombud för en tid av högst fyra år. Ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet samt får inte vara ledamot av nämnden.

Paragrafen är ny och reglerar hur granskningsombuden utses och vilka kvalifikationer de ska ha. Den nuvarande 6 § betecknas i fortsättningen 7 § i lagen.

Det är Säkerhets- och integritetsskyddsnämnden som utser granskningsombuden. Det sker för en tid av högst fyra år. Att granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet motsvarar vad som gäller för ordföranden och vice ordföranden i nämnden. I paragrafen finns det ytterligare kravet att granskningsombud inte får vara ledamot av nämnden.

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

14 b §

> Underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken, 8 § lagen (1995:1506) om hemlig kameraövervakning eller 15 § lagen (2007:978) om hemlig rumsavlyssning, ska fullgöras av den som är eller har varit förundersökningsledare.
>
> När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket rättegångsbalken, 8 § lagen om hemlig kameraövervakning eller 15 §

lagen om hemlig rumsavlyssning, ska den som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.

Om den förundersökningsledare som avses i denna paragraf inte kan fullgöra underrättelseskyldigheten enligt första och andra styckena ska denna i stället fullgöras av annan åklagare, polisman eller tjänsteman vid Tullverket.

Bestämmelsen reglerar ansvaret för att enskilda får en underrättelse om användning av hemliga tvångsmedel. Hittills har åklagare haft det ansvaret. Med anledning av förslaget om att åklagare, polis och tull får besluta om hemlig teleövervakning i vissa fall (se förslaget till 27 kap. 20 d och 21 §§ RB) har paragrafen ändrats så att det är den förundersökningsledare som finns i varje läge som har ansvaret för att underrättelse sker. Har underrättelse inte kunnat lämnas under utredningens gång, är det den förundersökningsledare som fanns när utredningen avslutades som har ansvaret. Frågan behandlas i avsnitt 6.8.2.

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 provokation 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. Situationen 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)