Till statsrådet och chefen för Justitiedepartementet

Genom beslut den 7 december 2000 bemyndigade regeringen chefen för Justitiedepartementet att tillkalla en beredning med tre ledamöter med uppdrag att verka för rättsväsendets utveckling. Regeringen bemyndigade samtidigt departementschefen att utse en av ledamöterna att vara ordförande samt att besluta om sakkunniga, experter, sekreterare och annat biträde åt beredningen.

Som ledamöter i beredningen förordnades fr.o.m. den 7 december 2000 generaldirektören Anders Eriksson, ordförande, samt fr.o.m. den 1 januari 2001 dåvarande hovrättspresidenten numera lagmannen Lars Eklycke och ordföranden och chefen för Allmänna reklamationsnämnden Lotty Nordling.

Som sakkunniga förordnades fr.o.m. den 1 januari 2001 dåvarande expeditionschefen Lars Dahllöf (t.o.m. den 31 augusti 2001), sedermera länspolismästaren Anders Danielsson, enhetschefen Birgitta Holmgren och överåklagaren Krister Waern (samtliga t.o.m. den 31 december 2003) samt fr.o.m. den 1 februari 2002 dåvarande expeditionschefen numera generaldirektören Thomas Rolén och fr.o.m. den 7 april 2005 expeditionschefen Nils Öberg.

Som experter förordnades fr.o.m. den 1 januari 2004 överåklagaren Björn Ericson, professorn Peter Fitger (i viss del av uppdraget), numera biträdande chefsjuristen Lars-Åke Johansson, polismästaren Peter Tjäder och dåvarande avdelningschefen numera chefsrådmannen Lars Trägård samt fr.o.m. den 1 augusti 2004 generaldirektören Gudrun Antemar och fr.o.m. den 1 januari 2005 Birgitta Trägårdh (se nedan).

Beredningen har i de frågor som behandlas i detta betänkande haft tillgång till en referensgrupp bestående av representanter för riksdagspartierna. Som ledamöter i referensgruppen förordnades fr.o.m. den 6 februari 2004 kommunalrådet Kia Andreasson (mp) samt riksdagsledamöterna Viviann Gerdin (c), Maria Hassan (s), Bengt-Anders Johansson (m), Niclas Lindberg (s), Ragnwi Marcelind (kd), Rolf Olsson (v) och Christer Winbäck (fp). Med entledigande av Viviann Gerdin förordnades den 3 mars 2004 f.d. riksdagsledamoten Gunnel Wallin (c) som ledamot i referensgruppen.

Som sekreterare åt beredningen förordnades fr.o.m. den 7 december 2000 numera ämnesrådet Per Lagerud och f.d. hovrättsas-

sessorn Birgitta Trägårdh (t.o.m. den 31 december 2004, därefter som expert). Som sekreterare förordnades också fr.o.m. den 1 januari 2002 hovrättsassessorn Johan Sjöö (t.o.m. den 31 augusti 2003) och fr.o.m. den 1 augusti 2004 hovrättsassessorn Ulrika Geijer. Per Lagerud har varit sekreterare i de frågor som behandlas i detta betänkande.

Beredningen har tagit namnet Beredningen för rättsväsendets utveckling (BRU) och har tidigare överlämnat delbetänkandena

1. Snabbare lagföring 1 – Några förslag till förenklingar (SOU 2001:59),
2. Snabbare lagföring 2 – Förenklad brottsutredning (SOU 2001:93),
3. Snabbare lagföring 3 – Snatteribrott (SOU 2002:44),
4. Snabbare lagföring 4 – Ett snabbförfarande för brottmål (SOU 2002:45),
5. Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74), och
6. Läget i rättsväsendet och förslag till fortsatta reformer inom brottsutredningsverksamheten m.m. (SOU 2003:114).

Vi får härmed överlämna delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*

Lars Trägård har avgivit ett särskilt yttrande.

Vårt arbete fortsätter med andra utestående frågor.

Stockholm i maj 2005

Anders Eriksson Lars Eklycke Lotty Nordling
/Per Lagerud

Innehåll

Förkortningar

Bet.	betänkande
BrB	Brottsbalken
Dir.	Kommittédirektiv
Ds	Betänkande i departementsserien
FAP	Föreskrifter och allmänna råd för polisväsendet
JO	Riksdagens ombudsmän (Justitieombudsmannen) eller Justitieombudsmännens ämbetsberättelse
JuU	Justitieutskottet
LEK	Lagen (2003:389) om elektronisk kommunikation
NJA	Nytt juridiskt arkiv
Prop.	proposition
PTS	Post- och telestyrelsen
RB	Rättegångsbalken
RPS	Rikspolisstyrelsen
RPSFS	Rikspolisstyrelsens författningssamling
SFS	Svensk författningssamling
Skr.	Skrivelse
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning
TU	Trafikutskottet

Sammanfattning

Inledning

Vi har enligt våra huvuddirektiv (Dir. 2000:90, se *bilaga 1*) i uppdrag att undersöka möjligheterna att än mer öka effektiviteten och kvaliteten i rättsväsendets arbete. Inom ramen för det uppdraget har vi fyra särskilt angivna huvuduppgifter. När det gäller lagföringen av brott skall vi särskilt undersöka möjligheterna att förkorta den genomsnittliga tiden från brottsanmälan till dom och straffverkställighet. Vi skall också särskilt överväga på vilket sätt brottsutredningsverksamheten ytterligare kan förbättras. Därutöver skall vi även uppmärksamma frågor om utbildning, kompetensutveckling och personalrörlighet inom rättsväsendet samt övergripande frågor om rättsväsendets myndigheters lokalisering.

Genom tilläggsdirektiv från den 20 november 2003 (Dir. 2003:145, se *bilaga 2*) fick vi i uppdrag att göra en översyn av uppgifts- och ansvarsfördelningen mellan polis och åklagare och av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation.

I detta betänkande har vi valt att redovisa uppdraget rörande elektronisk kommunikation och vissa närliggande frågor. Regeringen anger i direktiven att i detta uppdrag ingår att överväga en anpassning och modernisering av rättegångsbalkens terminologi, att göra en översyn av vilka verksamheter som bör omfattas av den s.k. anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning samt att överväga vilka typer av trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndigheterna och om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna. Vi bör enligt våra direktiv samtidigt ana-

lysera om utökade möjligheter för de brottsbekämpande myndigheterna medför ökade kostnader och hur dessa kostnader i så fall skall finansieras samt göra en avvägning mellan den nytta som de utökade möjligheterna ger i förhållande till de kostnadsökningar som kan uppstå. Regeringen anger också i direktiven att en utgångspunkt för uppdraget skall vara att inte fler uppgifter bevaras för brottsbekämpande ändamål eller under längre tid än vad som är nödvändigt. En annan utgångspunkt skall vara att personuppgifter som bevaras inte skall användas för något annat ändamål än brottsbekämpning. Enligt regeringen bör målsättningen för arbetet vara att skapa en enhetlig reglering som, särskilt med hänsyn till den snabba tekniska utvecklingen, kan stå sig över tiden.

Parlamentarisk referensgrupp

I enlighet med våra tilläggsdirektiv har vi i arbetet med de frågor som behandlas i detta betänkande haft tillgång till en referensgrupp med representanter för de sju riksdagspartierna. I referensgruppen har det funnits stor enighet kring huvuddelen av de förslag som presenteras i betänkandet. I några frågor har det dock funnits olika uppfattningar. När så har varit fallet redovisas det särskilt i betänkandet. Det rör dels interimistisk beslutanderätt vid hemlig teleövervakning, dels underrättelseskyldighet i efterhand, den s.k. straffvärdeprincipen och rätten till tillträde vid hemlig dataavläsning, dels kostnadsansvaret.

Rättegångsbalkens terminologi

Utgångspunkter

Lagen (2003:389) om elektronisk kommunikation ersatte i juli 2003 telelagen (1993:597) och lagen (1993:599) om radiokommunikation. I den nya lagen genomfördes flera EG-direktiv. Begreppet elektronisk kommunikation är inte definierat i lagstiftningen men avser enligt förarbetena överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier. Tillämpningsområdet för lagen om elektronisk kommunikation är vidare än telelagens. Elektronisk kommunikation omfattar telefoni

och datakommunikation men till skillnad från telelagen även utsändningar till allmänheten genom radio och TV.

Terminologin i bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken bygger till stor del på begrepp som tidigare återfanns i telelagen men som inte har överförts till lagen om elektronisk kommunikation. Som en följd av detta behöver en anpassning och modernisering ske av terminologin i tvångsmedelsbestämmelserna i rättegångsbalken och anslutande lagar.

Elektronisk kommunikation rör ett mycket dynamiskt område där utvecklingen av ny teknik går med rasande fart. Det är i dagsläget omöjligt att förutse hur tekniken kommer att utvecklas i framtiden. Att binda tvångsmedelsreglerna till vissa typer av kommunikation eller vissa typer av teknik är direkt olämpligt. I stället bör man så långt som möjligt bygga vidare på nuvarande regler. Två grundläggande utgångspunkter måste därför vara dels att skilda lösningar för olika typer av elektronisk kommunikation skall undvikas, dels att regleringen om tillgång till elektronisk kommunikation i brottsbekämpningen i största möjliga utsträckning skall göras oberoende av den snabba tekniska utvecklingen. Regleringen skall med andra ord kunna stå sig över tiden. Det kräver att bestämmelserna ges en något mer generell utformning i jämförelse med dagens regler för att inte riskera att snabbt bli överspelade av utvecklingen. Det främjar varken effektiviteten eller rättssäkerheten i brottsutredningsverksamheten att regler på tvångsmedelsområdet, kanske kort tid efter ikraftträdandet, får en oklar innebörd som en följd av den tekniska utvecklingen på området.

Begreppen telemeddelande, telenät och teleadress

Tre centrala begrepp i bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning är telemeddelande, telenät och teleadress.

Telemeddelande definierades i telelagen och utgör det som enligt rättegångsbalkens regler avlyssnas respektive övervakas. I lagen om elektronisk kommunikation används inte begreppet telemeddelande annat än att telelagens definition har överförts till den lagen som en övergångslösning i avvaktan på förslagen i detta betänkande. Det kan konstateras att det inte är lämpligt att ha kvar begreppet telemeddelande i rättegångsbalken. I lagen om elektronisk kommunikation finns begreppet elektroniskt meddelande, som dock inte är

detsamma som telemeddelande och som därför inte bör användas i tvångsmedelsbestämmelserna. Bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning tar sikte på avlyssning eller övervakning av information vid överföring av denna. Det som får avlyssnas respektive övervakas enligt bestämmelserna bör därför i stället anges med det teknikneutrala begreppet meddelande, som avgränsas genom att lagen anger var meddelandet får avlyssnas eller övervakas.

I lagstiftningen behöver det anges att meddelandena skall befordras eller ha befordrats i någon typ av nät. I dagsläget används begreppet *telenät* i rättegångsbalken. I lagen om elektronisk kommunikation finns tre nät angivna, nämligen det överordnade begreppet elektroniskt kommunikationsnät samt allmänt telefonnät och allmänt kommunikationsnät. Inget av de sistnämnda begreppen har dock samma innebörd som telenät enligt rättegångsbalken och tidigare telelagen. Begreppet elektroniskt kommunikationsnät kan dock användas i rättegångsbalken med den inskränkningen att det inte skall avse nät som enbart är avsett för utsändning av program i ljudradio eller television.

I rättegångsbalken används begreppet *teleadress* som en gemensam beteckning för olika identifieringsmetoder, alltså den icke fysiska adress som ett telemeddelande skickas till eller från. Det kan vara t.ex. ett abonnemang, en enskild anknytning eller en e-postadress. Begreppet fanns tidigare även i telelagen men används inte i lagen om elektronisk kommunikation. I beslut om hemlig teleavlyssning och hemlig teleövervakning skall det enligt nuvarande bestämmelser anges vilken eller vilka teleadresser som tillståndet omfattar. Begreppet teleadress bör inte längre användas i tvångsmedelsbestämmelserna. Det är klart mer ändamålsenligt att bestämmelserna om avlyssning och övervakning i stället som utgångspunkt anknyter till ett särskilt tekniskt hjälpmedel med viss knytning till en person än till den tekniska identifieringsmetod som kan användas för att identifiera hjälpmedlet vid ett enskilt meddelande. Därför bör det mer teknikneutrala begreppet tekniskt hjälpmedel användas.

Begreppen hemlig teleavlyssning och hemlig teleövervakning m.m.

Telelagens tillämpningsområde utgjorde enbart en del av tillämpningsområdet för lagen om elektronisk kommunikation. Som en

följd av det och mot bakgrund av det behov som finns av en reglering som i största möjliga utsträckning är oberoende av den tekniska utvecklingen, bör de begrepp som innehåller uttrycket tele i de aktuella tvångsmedelsbestämmelserna ersättas med andra begrepp. Då är det heller inte ändamålsenligt att benämna tvångsmedlen teleavlyssning respektive teleövervakning. Dessa begrepp bör alltså mönstras ut ur lagtexten. Lagtexten bör utformas utan att nya särskilda benämningar på tvångsmedlen införs. Det är fullt tillräckligt att innebörden av och förutsättningarna för åtgärderna beskrivs där. Detta hindrar inte att begreppen avlyssning respektive övervakning används i andra författningar som hänvisar till tvångsmedlen.

Det finns flera andra begrepp i författningarna som innehåller uttrycket tele, t.ex. televerksamhet, teleoperatör och telebefordringsföretag. Flera av begreppen kommer säkert att mönstras ut ur lagtexten efter hand. Såvida det inte finns en direkt koppling till det arbete som redovisas i detta betänkande föreslås inte några ändringar i sådan terminologi.

En samlad reglering i rättegångsbalken

Upphävande av vissa bestämmelser i lagen om elektronisk kommunikation och sekretesslagen

Vid hemlig teleövervakning får de brottsutredande myndigheterna i dag uppgifter om telemeddelanden som befordras och har befordrats, dvs. såväl uppgifter i realtid som historiska uppgifter. De historiska uppgifterna har myndigheterna möjlighet att få även genom utlämnande från operatörerna enligt lagen om elektronisk kommunikation och, för det fall det är en myndighet som driver televerksamhet, enligt sekretesslagen (1980:100). De uppgifter det rör sig om är exempelvis uppringt nummer, uppringande nummer, starttid, sluttid och antalet ringsignaler samt vissa lokaliseringsuppgifter avseende mobiltelefon. Utlämnande enligt sekretesslagen har i dagsläget mycket liten, om ens någon, praktisk betydelse medan utlämnande enligt lagen om elektronisk kommunikation, enligt en grov uppskattning, äger rum i drygt 4000 fall årligen.

I såväl Buggningsutredningens förslag (SOU 1998:46) som i den lagrådsremiss som följde på betänkandet föreslogs att bestämmel-

serna i dåvarande telelagen, numera i lagen om elektronisk kommunikation, och i sekretesslagen om utlämnande av ”teleövervakningsuppgifter” skulle upphävas. Möjligheten för de brottsutredande myndigheterna att få tillgång till uppgifterna skulle i stället uteslutande regleras av tvångsmedelsbestämmelserna i rättegångsbalken. Förslagen har i väntan på övervägandena i detta betänkande inte lett till lagstiftning.

Vi föreslår att regelsystemen förs samman i rättegångsbalken. Det blir det lagtekniskt mest logiska. För den enskilde innebär det en förstärkning av integritetsskyddet bl.a. genom att det som huvudregel kommer att krävas domstolsbeslut, vilket inte är fallet i dag med ordningen enligt lagen om elektronisk kommunikation och sekretesslagen (jfr dock nedan förslaget om åklagares interimistiska beslutanderätt). Dessutom är den aktuella tvångsmedelsanvändningen enligt rättegångsbalken underkastad parlamentarisk kontroll. Mot bakgrund av hur de övriga förslagen i betänkandet är utformade, bör detta kunna ske samtidigt som effektiviteten i det brottsutredande arbetet inte minskar (se särkilt förslaget om övervakning även utan misstänkt gärningsman).

Övervakning även utan misstänkt gärningsman m.m.

Enligt nuvarande regler är det en förutsättning för att hemlig teleövervakning skall få användas att det går att peka ut en person som skäligen misstänkt för ett brott. Något sådant krav finns inte för utlämnande av uppgifter enligt lagen om elektronisk kommunikation. Om de brottsutredande myndigheterna inte längre skall få tillgång till sådan information enligt den sistnämnda lagstiftningen, måste det övervägas om det även i fortsättningen alltid skall krävas en skäligen misstänkt person vid användning av övervakning enligt rättegångsbalken.

Enligt Buggningsutredningens bedömning (SOU 1998:46), som delades av regeringen i den efterföljande lagrådsremissen, skulle hemlig teleövervakning kunna användas, trots att det saknas en skäligen misstänkt person, dels avseende de teleadresser som har använts i anslutning till tiden och platsen för brottet, dels rörande de telemeddelanden som har befordrats till eller från en teleadress som innehas eller av särskild anledning kan antas ha använts av en målsägande som inte kan samtycka till åtgärden.

Ofta är övervakningsuppgifter, däribland uppgifter om positionen hos mobiltelefoner, den absolut viktigaste nyckeln till att ut-

redningar rörande grova brott kan föras framåt. Det rör exempelvis utredningar om 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, som terroristbrott. Särskilt i de inledande skedena av sådana utredningar kan det många gånger saknas en skäligen misstänkt person. I utredningsarbetet kan polisen i sådana fall på olika sätt ”lägga pussel” med övervakningsuppgifterna, 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, är det alltså möjligt att klarlägga hur gärningsmännen har agerat och vilka personer som har varit inblandade i brottsligheten. Dessutom kan övervakningsuppgifterna i många fall ge som resultat att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans.

Övervakning enligt rättegångsbalken måste kunna användas även om det inte finns någon som är skäligen misstänkt för brottet. Från effektivitetssynpunkt är det helt nödvändigt att möjligheterna för de brottsutredande myndigheterna att använda övervakning i de fallen inte är begränsade på det sätt som följde av Buggningsutredningens tidigare förslag. I annat fall skulle det innebära en kraftig försämring av effektiviteten i utredningar rörande grova brott.

Den brottslighet som nämndes tidigare är i de flesta fall sådan att flera personer på olika sätt är inblandade. Skulle någon av de inblandade ha identifierats som skäligen misstänkt måste utredningen trots detta kunna fortsätta att drivas framåt genom framtagande och bearbetning av övervakningsuppgifter på samma sätt. Möjligheten att använda övervakning skall alltså inte vara begränsad till situationer när det saknas en skäligen misstänkt person utan måste kunna användas i utredningar även efter det att någon har bedömts vara skäligen misstänkt. En motsatt ordning skulle innebära en allt för stor begränsning av effektiviteten i förhållande till nuvarande bestämmelser.

Vid sidan om kravet på att åtgärden skall vara av synnerlig vikt för utredningen skall det i detta fall krävas att brottsligheten är så allvarlig att den kan ligga till grund för avlyssning (hemlig teleavlyssning). Det rör huvudsakligen brott med minst två års fängelse i

straffskalan och andra brott om straffvärdet överstiger två år. Liksom i andra fall har domstolen och de brottsutredande myndigheterna skyldighet att på olika sätt beakta enskildas integritetsintressen. Domstolen kan för att minska risken för integritetsintrång t.ex. föreskriva begränsningar i beslutet till viss tidsperiod, visst geografiskt område eller vissa basstationer.

Bl.a. som en följd av det förslaget och de problem som användningen av s.k. anonyma kontantkort skapar för de brottsutredande myndigheterna, skall det inte längre vara ett krav att ett specificerat tekniskt hjälpmedel (teleadress) anges i domstolens beslut. Därigenom uppkommer effektivitetsvinster för de brottsutredande myndigheterna, främst genom att användningen av tvångsmedlen snabbt kan anpassas till de faktiska förhållandena. Även om inte domstolens beslut behöver ange identifierade tekniska hjälpmedel, skall den begränsning som i dag gäller finnas kvar i fråga om anknytningen mellan den misstänkte och ett särskilt tekniskt hjälpmedel (jfr nedan vid identifiering av tekniska hjälpmedel). Domstolarna och de brottsutredande myndigheterna skall även i fortsättningen vara skyldiga att i lika stor omfattning som hittills ta hänsyn till integritetsintrånget hos den enskilde vid beslut om och användning av tvångsmedlen.

Det inträffar att de brottsutredande myndigheterna mycket snabbt behöver få tillgång till uppgifter om elektroniska meddelanden, särskild om positionen hos mobiltelefoner. Exempelvis har rånarligor kunnat gripas tack vare att polisen fått övervakningsuppgifter i akuta skeden i samband med att gärningsmännen har rekognoserat eller varit i färd med att begå själva rånet. Dessutom finns exempel på fall där en mycket snabb tillgång till uppgifterna lett till att gärningsmän till människorov har kunnat gripas kort efter brottet. Det har då varit möjligt att få fram åt vilket håll målsägande och gärningsmän färdats i bil. Ett annat fall av människorov som har nämnts är när en målsägande sattes i en container som sedan spårades innan den fraktades bort tack vare att gärningsmännen använde mobiltelefon vid containern.

I dagsläget har de brottsutredande myndigheterna möjlighet att få sådana uppgifter genom att kontakta operatörerna och begära uppgifterna enligt lagen om elektronisk kommunikation. Som framgick tidigare föreslås att den bestämmelsen skall upphävas. Myndigheternas tillgång till uppgifterna skall i stället enligt vår mening uteslutande regleras av tvångsmedelsbestämmelserna i rättegångsbalken, vilket bl.a. innebär att domstolen först måste ge tillstånd innan uppgifterna kan lämnas i brottsutredningar.

En ordning som innebär att de brottsutredande myndigheterna behöver invänta ett domstolsbeslut i sådana akuta skeden som nyss nämndes, skulle innebära att effektiviteten i bekämpningen av den grova brottsligheten blir klart försämrad. För sådana brådskande fall föreslår vi att det i stället skall finnas en möjlighet för åklagare att fatta interimistiska beslut om det mindre integritetskänsliga tvångsmedlet övervakning. Det skall vara fråga om situationer där ändamålet med åtgärden kan antas gå förlorat om man väntar med att företa den. Åklagarens beslut skall genast skriftligen anmälas hos rätten, som skyndsamt skall pröva frågan. Den ordningen finns för vissa speciella fall redan i dag.

Lokalisering av tekniskt hjälpmedel

Bland de uppgifter om telemeddelanden som de brottsutredande myndigheterna får tillgång till vid hemlig teleövervakning finns lokaliseringsuppgifter för mobiltelefon, dvs. uppgifter om från vilket geografiskt område ett samtal rings eller tas emot. För att tydliggöra att den typen av uppgifter skall kunna fås genom tvångsmedlet föreslogs såväl i Buggningsutredningens betänkande (SOU 1998:46) som i den efterföljande lagrådsremissen att detta skulle anges i lagtexten. På så sätt skulle det också stå klart att uppgifterna även får avse positionen hos påslagna mobiltelefoner utan att det samtidigt pågår ett samtal. I avvaktan på övervägandena i detta betänkande har någon ändring av bestämmelserna inte skett.

Det finns ett mycket stort behov i brottsutredningar av att få tillgång till uppgifter om positionen hos mobiltelefoner. I definitionen av övervakning i rättegångsbalken skall det klargöras att tvångsmedlet får användas för att hämta in uppgifter för lokalisering. Med uppgifter för lokalisering skall avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits (oavsett om det tekniska hjälpmedlet används eller har använts för samtal eller inte).

Identifiering av tekniskt hjälpmedel

Det har under lång tid skett en stadig ökning av antalet mobiltelefonabonnemang i Sverige. Det totala antalet abonnemang per capita uppgick den 31 december 2003 till nära 981 abonnemang per 1000

invånare, vilket är en ökning med drygt nio procent jämfört med motsvarande tidpunkt ett år tidigare.

Det finns en tydlig tendens bland mobiltelefonikunder att använda s.k. kontantkort i stället för att teckna kontraktsabonnemang. Från att i stort sett inte ha förekommit år 1996 uppgick antalet aktiva kontantkort den 31 december 2003 till 5 003 000 stycken, eller närmare 58 procent av samtliga GSM-abonnemang. Operatörer har ofta behov av att hålla register med uppgifter över sina abonnenter, kanske främst för att kunna sköta sin fakturering. Innehavarna av kontantkorten med förutbetalda tjänster förblir dock i regel anonyma för operatören, om inte innehavaren själv väljer att lämna abonnemangsuppgifter till denne.

I dagsläget är det mycket vanligt att mobiltelefoner på olika sätt används vid brottslig verksamhet. Det är ofta ett problem för de brottsutredande myndigheterna att kriminella personer har fullt klart för sig vilka gränser som finns för myndigheternas operativa möjligheter och utnyttjar den kunskapen i sin brottsliga verksamhet. Den anonymitet som kontantkorten ger och fördelarna med anonymiteten är enligt uppgifter från polisen helt känd i kriminella kretsar ”ner på lägsta nivå” och utnyttjas av personer vid all typ av brottslighet i syfte att försvåra eller omöjliggöra de brottsutredande myndigheternas arbete. Allt sker givetvis mot bakgrund av att det ofta ligger ett högt bevisvärde i den information hemlig teleavlyssning och hemlig teleövervakning kan ge.

I rättegångsbalken finns ett krav på att hemlig teleavlyssning och hemlig teleövervakning enbart får avse vissa identifierade teleadresser med koppling till en skäligen misstänkt person. Det rör teleadresser

1. 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. 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.

Även vid verkställigheten, alltså i de brottsutredande myndigheternas kontakter med operatören, måste det finnas uppgift om identifierade teleadresser.

När de brottsutredande myndigheterna har identifierat en skäligen misstänkt person innebär det givetvis inte att myndigheterna även har klart för sig vilka teleadresser som den personen disponerar eller t.ex. kan komma att kontakta. Det är där problemet med de anonyma kontantkorten finns. Det är i stort sett undantagslöst

så att de kriminella personerna köper, byter och slänger mobiltelefoner och/eller anonyma kontantkort mycket frekvent. Därigenom ändras också de teleadresser som används. Dessutom används flera telefoner och flera kort parallellt av samma person.

Företrädare för Säkerhetspolisen, Rikskriminalpolisen och länskriminalpolisen i Stockholm har alla uttryckt att anonyma kontantkort utgör ett av de absolut största effektivitetshindren vid utredning av grova brott. De anonyma kontantkorten och kravet på att teleadresser skall vara identifierade för att tvångsmedlen skall kunna beslutas och verkställas skapar så stora problem i brottsutredningarna att polisen uttrycker det som ”en utredningsmässig, tidsmässig och resursmässig katastrof”. Det sägs att det läggs ned ”fruktansvärt stora resurser” på att på olika sätt ändå identifiera de teleadresser som används av brottslingarna. Det 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 en uppenbar risk för att arbetet med att identifiera teleadresserna blir resultatlöst, vilket innebär att hemlig teleavlyssning och hemlig teleövervakning över huvud taget inte kan användas i arbetet med att utreda grova brott.

Användningen av anonyma kontantkort i brottslig verksamhet innebär alltså ett allvarligt effektivitetsproblem för de brottsutredande myndigheterna. Det är ytterligt otillfredsställande att personer som sysslar med grov brottslighet genom så relativt enkla åtgärder som det är frågan om kan undvika en verkställighet av tvångsmedel i de fall där detta är av synnerlig betydelse för det brottsutredande arbetet. Om inget görs för att förhindra detta, kommer den grova brottsligheten att i många fall ha ett försprång framför de brottsutredande myndigheterna. Det är uppenbart att i flertalet sådana fall kommer brottsligheten inte att avslöjas. I andra fall kommer avslöjandet inte att kunna ske utan att betydande resurser förbrukas.

Enligt uppgifter från Säkerhetspolisen finns det möjligheter att med hjälp av en speciell typ av tekniskt hjälpmedel, som används i vissa närliggande länder, identifiera andra tekniska hjälpmedel, dvs. de teleadresser som är aktuella och som används av en viss person. Metoden ger på ett relativt enkelt sätt uppgift om vilka tekniska hjälpmedel som finns inom ett begränsat geografiskt område. Den ger alltså uppgift om vilka telefonnummer, koder eller andra teleadresser som används inom området. De brottsutredande myndigheterna får genom metoden kännedom inte enbart om det tekniska

hjälpmedel som är intressant för myndigheterna utan även om andra som används i närheten. Allt efter omständigheterna kräver då detta att något fler än en enda ”sökning” sker i området kring en misstänkt person för att ett visst tekniskt hjälpmedel skall kunna ”ringas in”. Det sker genom en jämförelse mellan uppgifterna från de olika platserna. Det geografiska området i vilka de korta sökningarna sker (någon enstaka sekund) kan begränsas genom att utrustningens räckvidd justeras efter de enskilda förhållandena. Utgångspunkten är då att man genom fysisk spaning har klart för sig var inom ett klart begränsat område det tekniska hjälpmedel finns som man vill ha uppgift om. I stadsmiljö kan det i praktiken röra sig om en radie på högst ett hundratal meter. Därigenom begränsas också avsevärt de uppgifter som ges om vilka tekniska hjälpmedel som används i övrigt på platsen. För tydlighetens skull måste nämnas att det alltså inte är fråga om att avlyssna innehållet i meddelanden utan enbart att få fram uppgifter som identifierar de tekniska hjälpmedlen, alltså det som i nuvarande bestämmelser i 27 kap. rättegångsbalken benämns teleadresser.

Det kan konstateras att det finns ett påtagligt behov i det brottsutredande arbetet av att identifiera tekniska hjälpmedel. Dessutom framstår den metod som Säkerhetspolisen har redogjort för som effektiv. Under förutsättning att inga avgörande hinder möter från integritetssynpunkt, bör därför de brottsutredande myndigheterna genom lagstiftning ges rätt att använda sig av en sådan metod vid förundersökningar.

Liksom i andra fall kan det vara svårt att generellt ange omfattningen av det integritetsintrång som skulle blir följden av en användning av metoden att identifiera tekniska hjälpmedel. I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte kommer att bli större än vid hemlig teleövervakning. Metoden ger uppgifter om tekniska hjälpmedel och innebär i praktiken att den har så stora likheter med övervakning enligt 27 kap. 19 § rättegångsbalken att den bör utgöra en del av det tvångsmedlet. Genom den ordningen kommer de rättssäkerhetsgarantier och andra krav som omgärdar övervakning även att gälla för den nu aktuella metoden. Övervakning enligt 27 kap. 19 § rättegångsbalken skall därför i fortsättningen även innebära att uppgifter i hemlighet får hämtas in för identifiering av tekniska hjälpmedel. Med uppgifter för identifiering skall avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden. Övervakning i syfte att identifiera tekniska hjälpmedel skall få avse

sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte.

Övervakningsuppgifter vid avlyssning

Hemlig teleavlyssning innebär att innehållet i ett telemeddelande blir tillgängligt för de brottsutredande myndigheterna medan hemlig teleövervakning i stället ger tillgång till uppgifter om telemeddelandena. I dag tillämpas i princip alltid den ordningen att tillstånd till hemlig teleavlyssning kombineras med tillstånd till hemlig teleövervakning. Orsaken är främst att hemlig teleavlyssning ger åtkomst enbart till innehållet i ett telemeddelande men inte till uppgifterna som rör detta, exempelvis från vilken teleadress det inkommande samtalet rings.

Frågan om ett tillstånd till hemlig teleavlyssning även borde ge åtkomst till vissa övervakningsuppgifter diskuterades i Buggningsutredningens betänkande (SOU 1998:46) och i den efterföljande lagrådsremissen. I avvaktan på ytterligare utredning föreslogs i lagrådsremissen att uppgift om mellan vilka teleadresser som meddelandet utväxlas och uppgifter om samtalets längd skulle erhållas även vid hemlig teleavlyssning. Förslaget har ännu inte lett till lagstiftning.

Såväl effektivitetsskäl som skäl av mer administrativ karaktär talar för att tillstånd till avlyssning bör ge de brottsutredande myndigheterna tillgång även till samtliga övervakningsuppgifter. Att begränsa tillgången till enbart vissa sådana uppgifter är inte motiverat från integritetssynpunkt.

Polisens tillgång till uppgifter om abonnemang m.m.

Inledning

I två skrivelser till Justitiedepartementet och i en skrivelse till oss har Rikspolisstyrelsen framhållit behovet av lagändringar i vissa fall rörande polisens tillgång till uppgifter om abonnemang m.m. från operatörer. Justitiedepartementet har överlämnat skrivelserna till oss.

En effektiv tillgång till uppgifter om abonnemang

Polisen har möjlighet att få tillgång till uppgifter om abonnemang, dvs. ”kataloguppgifter” som namn, titel, adress och abonnentnummer, på samma sätt som enskilda personer, alltså via de tjänster för abonnentupplysning som finns. Sådana uppgifter omfattas också av den utlämnandeskyldighet operatörerna har enligt lagen om elektronisk kommunikation. För öppna uppgifter är det oftast enklast för polisen att använda sig av abonnentupplysningstjänsterna medan polisen vid hemliga nummer behöver utnyttja lagen om elektronisk kommunikation. Enligt den lagen har polisen rätt att få sådana uppgifter dels vid förundersökningar rörande andra brott än bötesfall, dels när uppgiften behövs i samband med underrättelser, efterforskning och identifiering vid olyckor och dödsfall och i samband med kontakten med vårdnadshavare i vissa fall.

Polisen saknar i dag generella tekniska system för inhämtning av abonnemangsuppgifter. Dagens manuella system för identifiering av och kontakt med operatörer är enligt uppgift långsamt och arbetskrävande både för polisen och för operatörerna. Det är dessutom kostsamt och risken för fel och misstag vid hanteringen bedöms som stor.

Hanteringen vid inhämtning av uppgifter sker i dagsläget i flera steg. Eftersom förfarandet är olika beroende på vilken operatör abonnenten använder sig av, måste först den aktuella operatören identifieras. Först jämförs telefonnumret med de tilldelningar som framgår av den svenska nummerplanen. Därefter kontaktas den operatör abonnenten tillhör enligt planen. Om en abonnent har valt att portera sitt nummer till en ny operatör och den ursprungliga operatören 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 och/eller efter motringning. Rutinerna hos de mindre operatörerna är dock enligt uppgift ibland bristfälliga.

Rikspolisstyrelsen har angett att det med nuvarande hantering i vissa fall är svårt att få fram upplysningar om aktuella nummer, både öppna och hemliga, särskilt från mindre operatörer, och att det finns säkerhets- och sekretessbrister i det nuvarande systemet, exempelvis genom att flera operatörer än den aktuella kan behöva tillfrågas av polisen. De får därigenom uppgift om pågående ärenden. Det är dessutom svårt att upptäcka om en operatör har andra

intressen än de rent affärsmässiga. Rikspolisstyrelsen har sammanfattat läget så att en fortsatt hantering med samma rutiner kommer att bli ohanterlig inom ett par år.

Rikspolisstyrelsen önskar få samma tillgång till uppgifter om abonnemang som SOS Alarm AB (SOSAB) har i dag. Regionala alarmeringscentraler har en generell rätt enligt lagen om elektronisk kommunikation att få del av sådana uppgifter. Tanken är att polisen och SOSAB skulle ha tillgång till en databas med komplett abonnentinformation.

Det har alltså framkommit flera nackdelar för såväl polisen som operatörerna med den ordning som gäller i dag. Den är långsam, arbetskrävande, kostsam och leder ibland till att uppgifterna över huvud taget inte erhålls, i vart fall inte under den tid som är nödvändig för ett effektivt polisarbete. Dessutom finns säkerhetsrisker, sekretessbrister och stora risker för fel och misstag i hanteringen.

Det står klart att det nuvarande systemet behöver förändras och att det finns stora fördelar med den ordning som Rikspolisstyrelsen förespråkar, dvs. att lagstiftningen ändras så att polisen får samma generella rätt som SOSAB att ta del av abonnemangsuppgifter. Genom de datatekniska lösningar som då kan användas uppkommer klara effektivitetsvinster och därigenom minskade kostnader genom en ökad snabbhet, minskade arbetsinsatser och ett minskat bortfall av uppgifter. Dessutom ökar skyddet för sekretessbelagda uppgifter när sådana inte längre behöver delges operatörerna. Även säkerhetsriskerna minskar bl.a. genom en minskad risk för att polisen undanhålls uppgifter och för att operatören eller personal hos operatören påverkas av kriminella personer att genomföra åtgärder som försvårar polisens arbete.

Flera av de fördelar som nyss nämndes uppkommer även för operatörerna, främst genom en mer effektiv och billig ordning och genom att personalen riskerar att i mindre grad utsättas för påtryckningar från kriminella personer.

De fördelar som uppkommer för myndigheterna och operatörerna måste givetvis vägas mot intresset hos enskilda att uppgifter om hemliga abonnemang inte sprids i onödan. Det är viktigt att hålla i minnet att det här enbart rör sig om ”kataloguppgifter”, alltså uppgifter som namn, titel, adress och abonnentnummer, och inte om de mer integritetskänsliga uppgifterna om särskilda elektroniska meddelanden (motsvarande teleövervakningsuppgifter). Det är också viktigt att nämna att polisen många gånger har behov av uppgifterna vid ageranden som sker i den persons intresse som de hemliga uppgifterna avser, t.ex. vid lokalisering av larm. Den utvidgning

som Rikspolisstyrelsen har föreslagit i lagstiftningen är dessutom relativt begränsad och borde om den genomfördes kunna bli föremål för någon form av reglering och kontroll inom myndigheterna för att t.ex. begränsa den krets av personer som har tillgång till uppgifterna och undvika eventuella misstankar om otillbörlig användning.

Efter en avvägning mellan å ena sidan de många fördelar som finns att hämta av en utvidgad möjlighet för polisen att ta del av abonnemangsuppgifter och å andra sidan den i praktiken relativt begränsade risken för ökade intrång i enskildas integritet som skulle följa, finns det enligt vår mening inte något hinder mot att lagen om elektronisk kommunikation ändras på det sätt som Rikspolisstyrelsen har föreslagit. Vi föreslår därför en sådan ändring.

Utlämnande av vissa uppgifter när personer har försvunnit

Enligt lagen om elektronisk kommunikation har polisen och i vissa fall åklagare möjlighet att utan samband med förundersökning få abonnemangsuppgifter från operatörerna. Det gäller exempelvis om det finns behov av uppgifterna i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att kunna överlämna en ung person som har omhändertagits till vårdnadshavare.

Utanför en förundersökning finns det däremot inte någon skyldighet för operatörerna att lämna ut uppgifter om kommunikationen, alltså motsvarande teleövervakningsuppgifter. Det finns dock ett stort behov hos polisen att få tillgång till sådana uppgifter, främst lokaliseringsuppgifter rörande mobiltelefon, i situationer där personer har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa. Genom tillgång till uppgifterna i sådana fall kan personen många gånger påträffas snabbare och stora resurser sparas i polisarbetet. Vi föreslår därför att lagen om elektronisk kommunikation kompletteras med en sådan regel, som alltså inte skall tillämpas vid misstankar om brott.

Skyldighet att registrera abonnemangsuppgifter för kontantkort

Det finns som nyss nämndes en tydlig tendens bland mobiltelefonkunder att använda anonyma kontantkort i stället för att teckna

kontraktsabonnemang. Som också framgick används den anonymitet som kontantkort ger i dag i kriminella kretsar för att försvåra polisens arbete.

Polisens möjligheter att få tillgång till abonnemangsuppgifter är ofta avgörande för om en brottsutredning skall vara framgångsrik. Operatörer har behov av att hålla register med uppgifter över sina abonnenter, kanske främst för att kunna sköta sin fakturering. Innehavarna av kontantkort förblir dock i regel anonyma för operatören, vilket leder till att de brottsutredande myndigheterna inte har möjlighet att få ut nödvändiga abonnemangsuppgifter. Rikspolisstyrelsen har i en skrivelse till beredningen påtalat behov av att operatörerna åläggs en skyldighet att registrera uppgifter om vem som innehar ett kontantkort samt uppgifter om var och när kortet köptes. Rikspolisstyrelsen har också redovisat att Norge, Schweiz och Tyskland redan har lagstiftning som ger operatörerna en sådan skyldighet.

Det är ett faktum att när mobiltelefoner förekommer vid brottslig verksamhet är det i princip uteslutande anonyma kontantkort som utnyttjas för att undgå upptäckt och försvåra det brottsutredande arbetet. I beredningen finns en mycket stor förståelse för de brottsutredande myndigheternas påtagliga behov av att i olika sammanhang få tillgång till uppgifter om abonnemang rörande kontantkort. Till en viss del är detta möjligt redan i dag, nämligen när kunden frivilligt har valt att lämna sådana uppgifter till operatören. Vissa operatörer behandlar i sådana fall uppgifterna som öppna abonnemangsuppgifter medan andra betraktar uppgifterna som hemliga. Har kunden valt att lämna uppgifterna till operatören har myndigheterna under alla förhållanden rätt att för vissa ändamål få tillgång till uppgifterna enligt lagen om elektronisk kommunikation. Det stora problemet för myndigheterna är alltså när operatören saknar uppgifter om innehavaren av kontantkortet.

De brottsutredande myndigheternas behov av att få tillgång till uppgifterna måste vägas mot andra intressen. En skyldighet att registrera abonnenten bakom ett visst kontantkort innebär inte enbart ett åliggande för operatörerna, med kostnader som följd, utan även en skyldighet för den stora mängd personer som köper kontantkort att ge upp den anonymitet som hittills har funnits och i stället lämna uppgifter om sig själva till operatörerna för brottsutredande ändamål. Särskilt som det får förutsättas att anonymiteten i sig inte generellt är av avgörande betydelse för konsumenterna vid köp av kontantkort, är det sistnämnda inte en så stor integritetsfrå-

ga att den ensam bör kunna hindra en reglering av det slag som Rikspolisstyrelsen föreslår.

Avgörande är dock den tveksamhet som finns rörande hur effektiv den föreslagna ordningen skulle bli för den brottsutredande verksamheten. För att undvika att registreringen blir ”ett slag i luften” skulle en hel del kontrollmekanismer och annat behövas för att i största möjliga mån undvika t.ex. att köpare av kontantkort uppger felaktiga personuppgifter och att vissa köpare registrerar sig för större mängder kontantkort och sedan tillhandahåller dessa i kriminella kretsar. Mot bakgrund av att regleringen inte heller skulle bli enhetlig i ett större antal länder i vårt närområde, t.ex. EU-länderna, skulle anonyma kontantkort kunna köpas utomlands och utnyttjas i Sverige i brottsliga sammanhang.

Det finns alltså stora effektivitetsproblem med den ordning som Rikspolisstyrelsen har föreslagit om registrering av abonnemangsuppgifter till i dagsläget anonyma kontantkort. Särskilt mot den bakgrunden anser vi att någon sådan skyldighet inte bör införas nu. Frågan kommer säkert att få allt större betydelse framöver. Därför är det till en början lämpligt att frågan drivs i internationella sammanhang eller utifrån de erfarenheter som finns i andra länder av nationell lagstiftning på området.

Det måste framhållas att genom förslaget om identifiering av tekniska hjälpmedel kommer de brottsutredande myndigheterna ändå att få betydligt lättare att komma runt det nuvarande problemet med anonyma kontantkort.

Anpassningsskyldigheten

Anpassningsskyldigheten enligt lagen om elektronisk kommunikation

År 1996 infördes den s.k. anpassningsskyldigheten i telelagen. Anpassningsskyldigheten, som numera finns föreskriven i lagen om elektronisk kommunikation, innebär att en operatör skall bedriva verksamheten så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Dessutom skall innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden göras tillgängliga så att informationen enkelt kan tas om hand.

Vårt uppdrag enligt direktiven är att göra en översyn av vilka verksamheter som bör omfattas av anpassningsskyldigheten och hur den skall vara reglerad i olika avseenden.

Att den enskilde operatören har anpassat verksamheten är i praktiken ofta en förutsättning för att beslut om tvångsmedlen över huvud taget skall kunna verkställas och att verkställandet kan ske i nära anslutning till domstolens beslut. När anpassningsskyldigheten infördes uttalade regeringen att hemlig teleavlyssning och hemlig teleövervakning är betydelsefulla och oumbärliga hjälpmedel i kampen mot särskilt den grova brottsligheten och att det av effektivitetsskäl är ytterst angeläget att möjligheterna till verkställighet av tvångsmedlen på området upprätthålls. Den slutsatsen är än mer giltig i dag, framför allt mot bakgrund av teknikutvecklingen under senare tid. Det bör särskilt framhållas att frågan har stor betydelse även för allmän ordning och allmän säkerhet, däribland rikets säkerhet och skyddet mot terrorism. Att en anpassningsskyldighet för operatörerna måste finnas även fortsättningsvis är helt givet. Något annat följer heller inte av direktiven.

Anpassningsskyldigheten är av central betydelse för effektiviteten vid verkställigheten av beslut om hemlig teleavlyssning och hemlig teleövervakning och har som syfte att möjliggöra användningen av tvångsmedlen och därmed skapa förutsättningar för effektiva utredningar när det gäller grövre brott. Även om bestämmelserna i lagen om elektronisk kommunikation, där anpassningsskyldigheten finns föreskriven, i första hand är av näringsrättslig art, har vi kommit fram till att det som en följd av våra förslag inte finns tillräckliga skäl att flytta bestämmelsen om anpassningsskyldighet från den lagen. Det bakomliggande syftet med anpassningsskyldigheten är och förblir att underlätta tvångsmedlen. Vi vill dock understryka att om det skulle visa sig att bestämmelsen får en allt för snäv tillämpning ur ett brottsutredande perspektiv, måste det övervägas att föreskriva om anpassningsskyldighet någon annanstans, kanske i rättegångsbalken.

De uttryck som används i dag i lagen om elektronisk kommunikation för att beskriva anpassningsskyldigheten är att verksamheten skall bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Dessutom skall innehållet i och uppgifter om avlyssnade eller övervakade meddelanden göras tillgängliga för polisen så att informationen enkelt kan tas om hand. Det uttryckssättet beskriver väl de krav som bör ställas på operatörerna i detta avseende. Det finns bl.a. mot bakgrund av den snabba teknikutvecklingen ingen anled-

ning att i lagtexten beskriva skyldigheten på en högre detaljnivå än så.

Verksamheter som skall omfattas av anpassningsskyldigheten

Bestämmelserna i rättegångsbalken om hemlig teleavlyssning och hemlig teleövervakning är teknikneutrala och således inte begränsade till en viss typ av teknik för att befordra meddelanden. Enligt reglerna får telemeddelanden avlyssnas eller övervakas om de befordras eller har befordrats till eller från ett telefonnummer, kod eller annan teleadress. Om det är fråga om fast telefoni, mobiltelefoni eller Internet har alltså ingen betydelse för frågan om meddelandet är sådant att det faller under tvångsmedelsregleringen. Anpassningsskyldigheten enligt lagen om elektronisk kommunikation är dock begränsad så till vida att den inte omfattar samtliga verksamheter där sådana meddelanden som omfattas av tvångsmedlen befordras eller med andra ord samtliga de tekniker som är aktuella. I dag omfattar anpassningsskyldigheten enligt lagen om elektronisk kommunikation verksamheter som avser tillhandahållande *antingen* av ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, *eller* av tjänster inom ett allmänt kommunikationsnät vilka består av *endera* en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, *eller* en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Trots att den legala möjligheten finns att avlyssna eller övervaka ett visst meddelande enligt rättegångsbalken, medför avsaknaden av anpassningsskyldighet för vissa verksamheter stora effektivitetsförluster vid utredning av grova brott, eftersom tvångsmedelsbesluten med stor sannolikhet inte kan verkställas över huvud taget. Till det kommer att anpassningsskyldigheten leder till en snabb verkställighet, vilket ofta kan vara av stor betydelse i det brottsutredande arbetet.

Rikspolisstyrelsens uppfattning är att den nuvarande regleringen är otillräcklig ur ett brottsutredande perspektiv. Även vi har kunnat konstatera att inte minst teknikutvecklingen medför att anpassningsskyldigheten behöver vidgas om inte den brottsutredande

verksamheten skall hamna hjälplöst efter den grövre brottsligheten. Genom uppgifter från såväl Rikspolisstyrelsen som operatörer kan det också konstateras att det finns många oklarheter i dagsläget i frågan om gränserna för anpassningsskyldigheten. Detta faktum, tillsammans med frågan om kostnadsansvaret för åtgärderna (se vidare nedan) förefaller vara de främsta orsakerna till att anpassningsarbetet hos operatörerna i många fall är lågt prioriterat.

Såväl de brottsutredande myndigheterna som operatörerna har efterlyst en tydlighet och förutsebarhet i regleringen av anpassningsskyldighetens omfattning. Redan när skyldigheten infördes i telelagen uttalade regeringen att varje gräns medför att det kan bli någon gråzon där det är osäkert om en viss operatör faller strax innanför eller utanför gränsen och att det därför är angeläget att se till att gränsdragningen blir så förutsebar och klar som möjligt.

Som har konstaterats av både Rikspolisstyrelsen och operatörerna måste anpassningsskyldighetens omfattning vara mycket tydligt reglerad. För att åstadkomma detta bör skyldigheten så långt det är möjligt regleras teknikneutralt i författning och inte t.ex. vara en förhandlingsfråga mellan en operatör och en myndighet. Vi föreslår därför att anpassningsskyldigheten i fortsättningen skall träffa verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. rättegångsbalken eller tjänster inom ett sådant nät. Den utvidgning av anpassningsskyldigheten som i praktiken följer av detta förslag och som främst motiveras av det stora allmänna intresset av att effektivt kunna verkställa tvångsmedlen vid misstankar om grova brott, är att kravet också kommer att omfatta verksamhet som avser tillhandahållande av Internettjänster. Dessutom kommer anpassningsskyldigheten i de fasta telenäten inte att bli begränsad till en viss lägsta datahastighet för funktionell tillgång till Internet.

Det är en självklarhet att det inte skall finnas ett anpassningskrav för sådana verksamheter där meddelandena enligt bestämmelserna i rättegångsbalken över huvud taget inte får bli föremål för beslut om hemlig teleavlyssning och hemlig teleövervakning. Av hänsyn till mindre operatörer finns det också skäl att begränsa omfattningen av anpassningsskyldigheten ytterligare. Många operatörer skall inte behöva vidta några anpassningsåtgärder över huvud taget eftersom de är så ointressanta ur ett polisoperativt perspektiv att det inte vore rimligt att med hänsyn framför allt till kostnaderna kräva sådana av operatören. I andra fall är det kanske bara vissa begränsade anpassningar som bör genomföras. Den verksamhet som omfat-

tas av skyldigheten skall därför avse ett *allmänt* tillhandahållande av näten respektive tjänsterna.

Genom att anpassningsskyldigheten skall omfatta ett allmänt tillhandahållande utesluts bl.a. sådana nät eller tjänster som inte står till förfogande för användning av allmänheten och som samtidigt inte heller effektivt konkurrerar med sådan verksamhet. Sålunda kommer företag, bostadsrättsföreningar eller andra sammanslutningar som internt tillhandahåller vissa tjänster generellt sett inte att vara anpassningsskyldiga, även om beslut om tvångsmedel kan omfatta meddelanden som befordras i deras nät. I den mån dessa erbjuder sina tjänster till en vid krets, t.ex. i en stadsdel eller ett motsvarande större geografiskt område, och därigenom kan sägas effektivt konkurrera med operatörer på marknaden, kommer de dock att omfattas av anpassningsskyldigheten.

Det skall också tilläggas att, även om verksamheten omfattar ett sådant allmänt tillhandahållande av nät eller tjänst, det måste finnas möjlighet till undantag från anpassningsskyldigheten i enskilda fall genom en avvägning mellan nytta eller effektivitet och ekonomi för respektive operatör.

Undantag genom beslut i enskilda fall

I samband med att anpassningsskyldigheten infördes avfärdade regeringen en synpunkt om att det skulle fastställas standardiserade normer som skulle gälla för samtliga operatörer. Skälen var främst den stora variation som finns hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar samt den fortlöpande tekniska utvecklingen. I stället skulle Post- och telestyrelsen meddela tillståndsvillkor för varje operatör och därigenom avgöra vilka åtgärder som skulle vidtas i det enskilda fallet för att uppfylla kraven på anpassning.

Post- och telestyrelsens arbete resulterade bl.a. i att likalydande, generella tillståndsvillkor utfärdades först ett par år efter det att bestämmelserna om anpassningsskyldighet hade trätt i kraft. Rikspolisstyrelsen har haft invändningar mot bl.a. de långa handläggningstiderna och uttalat att de har utgjort ett direkt hinder för en snabb anpassning. Enligt Rikspolisstyrelsens uppfattning var dessutom tillståndsvillkoren inte alls tillräckliga för att åstadkomma en effektiv verkställighet.

Numera gäller inte de tillståndsvillkor som tidigare beslutades med stöd av telelagen. I stället gäller anpassningsskyldigheten fullt

ut för de operatörer som bedriver sådan verksamhet som omfattas av bestämmelsen i lagen om elektronisk kommunikation. Skulle skyldigheten bli allt för betungande framför allt när det gäller ekonomiska aspekter, kan den enskilde operatören begära undantag hos Post- och telestyrelsen från kravet på anpassningsskyldighet i något avseende. Det har såvitt bekant aldrig skett. Post- och telestyrelsen har också möjlighet att meddela verkställighetsföreskrifter. Några sådana föreskrifter har inte utfärdats.

Den tekniska utvecklingen går fort. De tekniska förhållandena hos varje operatör är i många avseenden unika. I dag kan det sägas finnas en än högre grad av variation hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar jämfört med för tio år sedan då anpassningsskyldigheten infördes i telelagen. Detta ställer krav på differentierade lösningar vad gäller anpassningen i detalj. Den bedömning som regeringen gjorde tidigare har blivit bekräftad i den praktiska tillämpningen, nämligen att anpassningsskyldigheten i sig och särskilt undantag från denna inte lämpar sig att närmare beskriva i generella föreskrifter eller villkor av generell karaktär. Det kan leda till en osäkerhet såväl hos operatörerna som hos de brottsutredande myndigheterna om anpassningsskyldighetens innebörd och omfattning och därmed också till bristande effektivitet. Det skall också sägas att den grova brottsligheten enligt Rikspolisstyrelsen är uppmärksam på gränserna för de brottsutredande myndigheternas operativa möjligheter, dvs. generella föreskrifter om undantag från anpassningsskyldigheten, men även offentliga undantagsbeslut i enskilda fall, ger de kriminella personerna en bra uppfattning om vilka operatörer och vilka kommunikationsformer som är lämpliga att använda för deras verksamhet. Till detta kommer särskilt att operatörerna har påtalat för oss vikten av en tydlig, förutsebar reglering av anpassningsskyldigheten. Vi föreslår därför att undantaget från anpassningsskyldigheten skall kunna meddelas enbart i enskilda fall och inte i form av generella föreskrifter. Det är av flera skäl mest lämpligt att Rikspolisstyrelsen fattar dessa beslut med möjlighet att överklaga hos allmän förvaltningsdomstol.

Frågan blir då vilken avvägning som skall ske vid prövning av undantag. I den frågan får framför allt nyttan eller effektiviteten vägas mot den enskilde operatörens kostnader för anpassningsåtgärderna. Där måste anmärkas att nyttan eller effektiviteten av en anpassning svårligen kan mätas i beräknade antal verkställigheter hos en enskild operatör. I vissa fall kan en enskild lyckad verkställighet innebära en oerhört stor samhällelig nytta i olika avseenden.

Bestämmelserna om anpassningsskyldighet har en sådan väsentlig betydelse för möjligheterna att verkställa de aktuella tvångsmedelsbesluten och därigenom för samhällets förmåga att utreda allvarlig brottslighet, att de telepolitiska målen inte kan sättas före de kriminalpolitiska vid en tillämpning. Utgångspunkten för en prövning måste istället vara att samtliga de meddelanden som omfattas av tvångsmedlen också i praktiken skall vara möjliga att avlyssna respektive övervaka eftersom systemen är anpassade fullt ut. I fråga om bedömningar av nyttan eller effektiviteten är det alltså mycket viktigt att beakta det samhällsintresse som ligger i att kunna upprätthålla en beredskap för att ha möjlighet att snabbt verkställa beslut om tvångsmedlen.

Kostnadsansvaret för anpassningsåtgärderna

I dag gäller att operatörerna själva får stå för de kostnader som anpassningsåtgärderna medför. Det innebär att kostnaderna ytterst får bäras av abonnenterna. Den ordningen har gällt sedan anpassningsskyldigheten infördes i telelagen. Regeringen utvecklade ingående skälen i det lagstiftningsärendet. Vad som har förekommit under de år anpassningsskyldigheten har funnits ger i huvudsak inte anledning att införa en annan ordning. Även i fortsättningen bör alltså operatörerna stå för de kostnader som uppkommer.

De operatörer som vi har haft kontakt med har inte lämnat några konkreta uppgifter om hur stora kostnaderna i praktiken är. I frånvaro av sådana uppgifter är kostnaderna näst intill omöjliga för oss att uppskatta. I det tidigare lagstiftningsärendet har ett rimligt belopp för anpassning hos de största operatörerna uppskattats till ett engångsbelopp om något tiotal miljoner kronor med en tillkommande årlig driftkostnad på någon miljon kronor. De investeringar som krävs är dock i allt väsenligt redan gjorda, med undantag för den anpassningsskyldighet för vissa operatörer som tillkommer med vårt förslag. Mot bakgrund av bl.a. detta verkar det inte sannolikt att kostnaderna skulle överstiga vad berörda operatörer rimligen kan bära, särskilt som det sker en ”pulvrisering” så att kostnaderna tas igen genom intäkter från abonnenterna. Den avgiftshöjning som på detta sätt kan komma att drabba respektive abonnent kan antas bli marginell och är försvarlig med hänsyn till den nytta som den genom våra förslag förbättrade möjligheten till brottsbekämpning för med sig.

Vitesföreläggande vid bristande åtgärder

Sedan anpassningsskyldigheten infördes i telelagen har det funnits möjlighet för Post- och telestyrelsen att bl.a. meddela de förelägganden som har behövts för att skyldigheten skall efterlevas. Det är nödvändigt att det även i fortsättningen finns ett påtryckningsmedel på operatörerna att vidta de åtgärder som krävs. Därför skall det vara möjligt för Rikspolisstyrelsen att meddela de förelägganden som behövs för efterlevnaden av skyldigheten. Säkert kommer den möjligheten att aktualiseras ytterst sällan. Föreläggandet, som måste kunna förenas med vite, skall kunna överklagas hos allmän förvaltningsdomstol.

Som huvudregel gäller enligt viteslagen att frågor om utdömande av vite prövas av länsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet. Den ordningen skall gälla även för de förelägganden som Rikspolisstyrelsen meddelar i fråga om anpassningsskyldighet.

Sekretess

Det är ett faktum att särskilt den grova brottsligheten vidtar en mängd åtgärder för att skydda den olagliga verksamheten. Bl.a. innebär det att man noggrant följer de brottsutredande myndigheternas förmåga att genomföra olika brottsbekämpande åtgärder. Får de kriminella personerna tillgång till uppgifter om begränsningar i avlyssnings- och övervakningsmöjligheterna hos de enskilda operatörerna, kan det få allvarliga konsekvenser för myndigheternas arbete, eftersom det kan resultera i att personer väljer operatörer och kommunikationsformer där tvångsmedel inte kan verkställas.

Vid Rikspolisstyrelsens prövning av frågor om undantag och förelägganden kan det förekomma uppgifter som avslöjar begränsningar i möjligheten för de brottsutredande myndigheterna att verkställa tvångsmedelsbesluten. Det är därför nödvändigt att kunna hålla uppgifterna hemliga.

Vi föreslår att det bland de bestämmelser i sekretesslagen som rör intresset att förebygga eller beivra brott skall införas en regel som anger att sekretess skall gälla för uppgift som hänför sig till prövningen av sådana frågor, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

I samband med att en operatör ansöker hos Rikspolisstyrelsen om undantag från anpassningsskyldigheten ligger det i sakens natur att operatören måste lämna uppgifter om sina tekniska system och liknande. Sådana uppgifter kan vara mycket avslöjande i förhållande till framför allt konkurrenter på marknaden. Sådana uppgifter kan även förekomma i ärenden om föreläggande rörande efterlevnaden av skyldigheten. Sekretess måste därför också gälla för uppgift om den enskildes affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs.

Tid för att genomföra förslagen

Våra förslag innebär att vissa operatörer, vars verksamhet inte tidigare har omfattats av anpassningsskyldigheten, kommer att behöva anpassa sina system så att tvångsmedelsbesluten kan verkställas. Det är rimligt att operatörerna får en viss tid på sig för anpassningsåtgärder från det att bestämmelserna utfärdas till dess att de träder i kraft. Det finns inte anledning att bestämma den tiden till längre än ett år. Det får anses vara en tillräcklig tid för operatörerna att förbereda och vidta erforderliga åtgärder alternativt att förbereda en ansökan till Rikspolisstyrelsen om undantag från skyldigheten i något avseende.

Bevarandeskyldigheten

Inriktningen på vårt arbete

Vi har uppdrag att överväga om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna. Trafikuppgifter är främst kopplade till ”avsändande” och ”mottagande” identitet (t.ex. telefonnummer, e-postadress och IP-nummer), datum och klockslag, lokalisering och annat (t.ex. antalet ringsignaler).

Sedan regeringen beslutade om våra tilläggsdirektiv i november 2003 drabbades Europa av det största terroristattentatet sedan andra världskriget. Attentaten i Madrid den 11 mars 2004 tog omkring 200 personers liv och skadade över 1 500. Det är den främsta bakgrunden till att ett rambeslut håller på att arbetas fram inom EU. Det är ett svar på den uppmaning som EU:s stats- och regerings-

chefer gav vid toppmötet i Bryssel i mars 2004 i deklarationen om kampen mot terrorism. I deklarationen uppmanas rådet att med prioritet undersöka möjligheten till åtgärder för att fastställa regler för bevarande av trafikuppgifter hos operatörer som tillhandahåller tele- eller Internettjänster. Förslaget till rambeslut är lagt av Frankrike, Irland, Storbritannien och Sverige gemensamt och håller för närvarande på att förhandlas. Målet är att rambeslutet skall antas i juni 2005. Syftet med förslaget är att trafikuppgifter skall bevaras av operatörer under viss tid så att uppgifterna finns tillgängliga för de brottsbekämpande myndigheterna i det internationella straffrättsliga samarbetet.

Många europeiska länder har en nationell lagstiftning som innebär en skyldighet för operatörer att bevara trafikuppgifter under viss tid för brottsbekämpande ändamål. Vi kan konstatera att förutsättningarna för oss att arbeta fram ett ändamålsenligt förslag i frågan om bevarandeskyldighet har förändrats kraftigt sedan regeringen beslutade om våra direktiv. Vi har bedömt att det med hänsyn till de oklarheter som finns i dagsläget i fråga om resultatet av det arbete som nu bedrivs inom EU inte är meningsfullt att vi lämnar något förslag på nationell lagstiftning rörande bevarandeskyldigheten. Med hänsyn till frågans aktualitet och stora betydelse har vi dock funnit det angeläget att beskriva det behov som de brottsutredande myndigheterna har av att få tillgång till trafikuppgifter i förundersökningar och av de ”operativa” problem som de nuvarande reglerna på området skapar.

Nuvarande bestämmelser

I lagen om elektronisk kommunikation finns den huvudregel som säger att trafikuppgifter skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Lagen tillåter dock att uppgifterna sparas för viss behandling, t.ex. abonnentfakturering till dess att fordran är betald eller preskriberad och om uppgifterna är nödvändiga för att förhindra eller avslöja obehörig användning av nätet eller tjänsten. Uppgifterna måste givetvis också sparas om uppgifterna rör en adress som omfattas av beslut om hemlig teleavlyssning eller hemlig teleövervakning.

För direkt brottsutredande ändamål finns inte någon rätt att spara trafikuppgifterna annat än när ett beslut om hemlig teleavlyssning eller hemlig teleövervakning är fattat. I sådana fall är alltså de framtida uppgifterna, realtidsuppgifterna, ”säkrade” för de brotts-

utredande myndigheterna. Möjligheten att få tillgång till historiska uppgifter som har genererats före det att tvångsmedelsbeslutet kom operatören till del, blir beroende av om operatörerna av andra skäl har kvar uppgifterna i sina system. Det gäller oavsett om det är fråga om att få tillgång till uppgifterna inom ramen för hemlig teleövervakning eller genom en begäran enligt lagen om elektronisk kommunikation. Generellt kan sägas att historiska uppgifter har en större betydelse i brottsutredningar än vad realtidsuppgifter har.

Det är alltså inte enbart skyldigheten att utplåna trafikuppgifter utan även den bedömning respektive operatör gör i fråga om den skyldigheten, t.ex. vid vilken tidpunkt som det inte längre av faktureringsskäl finns anledning att ha kvar uppgifterna, som sätter en gräns för vilka historiska uppgifter som de brottsutredande myndigheterna i praktiken har möjlighet att få del av. Operatörernas bedömningar av egna behov styr med andra ord tillgången till uppgifterna i brottsutredningar och i förlängningen möjligheterna att klara upp grövre brottslighet.

Behovet av tillgång till trafikuppgifter i brottsutredningar

De trafikuppgifter som de brottsutredande myndigheterna får vid användning av hemlig teleövervakning är desamma som myndigheterna har möjlighet att erhålla genom utlämnande från operatörerna enligt lagen om elektronisk kommunikation. Uppgifterna är ofta den absolut viktigaste nyckeln till att utredningar rörande grövre brott kan föras framåt. 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 brottsligheten inleds ofta med en kontroll av de trafikuppgifter 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. I utredningsarbetet kan polisen på olika sätt ”lägga pussel” med uppgifterna, kanske sammanställda med annan information från t.ex. 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, är det alltså 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 trafikuppgifter 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.

I detta sammanhang är det också viktigt att framhålla den brottslighet som på olika sätt kan relateras till Internet. Enligt uppgift är avsaknad av en skäligen misstänkt person 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 trafikuppgifter, eftersom de uppgifterna är det enda som kan länka samman målsäganden och gärningsmannen. Möjligheten att vara anonym på Internet ger också problem vid 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 annat verktyg vid brottsligheten. Det har också då mycket stor betydelse att de brottsutredande 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. Även den ökade användningen av kryptering gör att betydelsen av tillgång till trafikuppgifter i brottsutredningarna blir större, eftersom krypteringen i princip innebär att de brottsutredande myndigheterna inte kommer åt innehållet i meddelanden genom hemlig teleavlyssning.

Det skall tilläggas att tillgång till trafikuppgifter från operatörer i Sverige är helt nödvändig även i det internationella samarbetet mellan brottsutredande myndigheter.

Betydelsen av att de brottsutredande myndigheterna får tillgång till trafikuppgifter i förundersökningar särskilt rörande grövre brott kan inte överskattas. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Det gäller inte minst i de fall där det från början saknas en skäligen misstänkt person.

Hur gamla trafikuppgifter finns det behov av?

Vissa europeiska länder har redan en nationell lagstiftning om skyldighet för operatörer att bevara trafikuppgifter för brottsbekämpande ändamål. Enligt uppgift är tiden för bevarandet satt till minst ett år i Belgien, maximalt ett år i Danmark och Frankrike, minst tre år i Irland, minst fyra år i Italien, tre månader i Nederländerna, maximalt ett år i Polen och Spanien samt maximalt sex månader i Schweiz. I Storbritannien finns ett frivilligt åtagande hos operatörerna att spara uppgifter i ett år.

Säkerhetspolisens uppfattning är att det är av synnerlig vikt för de brottsutredande myndigheterna att trafikuppgifter sparas under längre tid än tolv månader och då snarare 36 månader. Det gäller särskilt i utredningar av grov brottslighet, t.ex. grova våldsbrott, brott av organiserad karaktär och terroristbrott. I sådana fall kan planering och förberedelser pågå under mycket lång tid, kanske flera år, innan själva brottet genomförs. Säkerhetspolisen har gett som exempel att efter terroristattentaten i Madrid i mars 2004 efterfrågades trafikuppgifter från Sverige från år 1996. Som ytterligare exempel kan nämnas att i utredningen av den s.k. Nackabomben utgjorde historiska uppgifter en mycket viktig anledning till att misstänkta personer kunde knytas till platsen för gärningen. De uppgifter som blev intressanta i utredningen var mer än ett och ett halvt år gamla. Endast en av operatörerna kunde ta fram så gamla uppgifter.

Vi har kunnat konstatera från de exempel vi har fått, att de brottsutredande myndigheterna har behov av trafikuppgifter som är flera år gamla i utredningar av grova brott och att det finns flera orsaker till att operatörerna relativt sällan i dagsläget får förfrågningar på uppgifter som är äldre än tolv månader. De främsta skä-

len är givetvis att det finns en skyldighet för operatörerna att utplåna uppgifterna och att, när frågan om utlämnande blir aktuell, myndigheterna är medvetna om att utplånande måste ha skett och/eller att myndigheterna inte har möjlighet att av kostnadsskäl begära uppgifterna. Säkerhetspolisen har uppskattat att det finns behov av att få uppgifter äldre än tolv månader i några hundra förundersökningar årligen. Särskilt som det rör sig om grova brott där brottsligheten även många gånger kan sägas vara organiserad, instämmer vi i Säkerhetspolisens bedömning att det är av synnerlig vikt för det brottsutredande arbetet att uppgifter finns tillgängliga under längre tid tillbaka än tolv månader.

Problem med nuvarande ordning

Säkerhetspolisen har uttryckt stora bekymmer för effektiviteten i brottsutredningsverksamheten med anledning av att någon bevarandeskyldighet inte finns föreskriven och har tillagt att så fort en historisk trafikuppgift inte kan lämnas ut från operatörerna riskerar det allvarliga konsekvenser för utredningsresultatet i den enskilda förundersökningen. Det skall dock framhållas att det är näst intill en omöjlighet att peka på enskilda förundersökningar eller uppskatta antalet förundersökningar där utredningsresultatet, till skillnad från hur det verkligen blev, hade blivit mer lyckat om en viss trafikuppgift hade varit tillgänglig.

Säkerhetspolisen har givit ett flertal exempel på förhållanden som skapar problem. Variationen är stor hos operatörerna när det gäller vilka trafikuppgifter som sparas och under vilken tid det sker. Det förekommer att sådana uppgifter som vissa operatörer sparar under mer än ett år utplånar andra operatörer omedelbart efter samtalet. För vissa av de operatörer som över huvud taget kan redovisa uppgifter om inkommande trafik rör det bara trafik från egna abonnenter. Hos operatörer som sparar uppgifter om utgående trafik, kan det gälla enbart sådana begränsade uppgifter som behövs för faktureringsändamål, vilket ofta inte är fallet med lokaliseringsuppgifter. När operatörer tillhandahåller förutbetalda tjänster (t.ex. genom anonyma kontantkort) finns det ofta ingen anledning för dem att spara uppgifter över huvud taget. Dessutom kan viss teknik som används i dag hos operatörerna leda till att de brottsutredande myndigheterna inte kan få ut några uppgifter alls rörande viss kommunikation. Uppgifterna redovisas också på olika sätt hos

operatörerna, vilket kräver stora resurser hos de brottsutredande myndigheterna för den tekniska tolkningen av informationen.

Till det kommer att vissa operatörer enligt Säkerhetspolisens uppfattning inte lämnar så kompletta uppgifter som skulle kunna tas fram ur operatörens system, vilket Säkerhetspolisen bedömer beror på att systemen inte är anpassade för begäran från de brottsutredande myndigheterna, att operatörerna saknar den tekniska kompetens som behövs för att få fram uppgifterna och att för lite resurser läggs på att t.ex. förenkla framtagandet av uppgifterna. Dessutom är de brottsutredande myndigheterna utlämnade till att lita på att det besked som lämnas från operatörerna är korrekt vad gäller vilka uppgifter som finns tillgängliga.

Möjligheten att få tillgång till de historiska trafikuppgifterna i brottsutredningar blir som sagt ofta beroende av vilken operatör och vilken teknik som är aktuell i det enskilda fallet. Den brottsling som med kunskap eller av ren slump utnyttjar, från hans sida sett, ”rätt” operatör och teknik har därmed stor möjlighet att undgå lagföring, medan andra kanske blir lagförda för brottsligheten. Enligt uppgifter från Säkerhetspolisen finns det till och med risk för att de länder som saknar nationell lagstiftning om bevarandeskyldighet för brottsbekämpande ändamål utnyttjas av kriminella organisationer som bas för deras verksamhet.

Det är mycket otillfredsställande att de brottsutredande myndigheterna inte kan få tillgång till historiska trafikuppgifter, trots att förutsättningarna för det är uppfyllda enligt reglerna om hemlig teleövervakning enligt rättegångsbalken och om utlämnande enligt lagen om elektronisk kommunikation. Som vi nyss uttryckte är tillgången till historiska uppgifter av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Frånvaron av en bevarandeskyldighet för operatörerna medför många gånger stora problem för myndigheterna med att få tillgång till de uppgifter som behövs. Det förhållandet leder i sin tur till allvarliga problem med effektiviteten i förundersökningsarbetet. Särskilt som det rör sig om utredningar av grövre brottslighet kan konsekvenserna från brottsbekämpningssynpunkt i längden bli oacceptabla. Det uppstår även liknande effektivitetsproblem i de brottsutredningar som bedrivs i andra länder men där uppgifter från operatörer i Sverige efterfrågas.

Medverkan vid verkställigheten av vissa tvångsmedelsbeslut

Enligt rättegångsbalken får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas. Med detta avses bl.a. att de tekniska hjälpmedlen får anslutas, underhållas och återtas, dvs. operatörerna har en skyldighet att medverka genom att biträda och lämna tillträde för polisen.

Skyldigheten att medverka är inte densamma som anpassningsskyldigheten utan rör i stället kravet på att operatörerna vidtar andra åtgärder efter begäran om aktiv medverkan vid verkställigheten av tvångsmedelsbesluten. Exempel på det kan vara att lämna information om funktioner och andra tekniska förutsättningar som är nödvändiga för att kunna verkställa tvångsmedelsbesluten, tillhandahålla teknisk utrustning och vidta de personella och organisatoriska dispositioner som är nödvändiga för verkställighet inom kort tid av respektive tvångsmedelsbeslut, alltså att snabbt vidta nödvändiga åtgärder från det att verkställigheten har beställts av polisen.

Skyldigheten att medverka måste alltså ses helt skild från anpassningsskyldigheten. En medverkan från operatörernas sida skall aldrig kunna ersätta kraven på anpassning, som i sig garanterar en effektivitet vid verkställighet av tvångsmedelsbesluten. Skyldigheten att medverka skall ses som ett separat krav vid sidan av anpassningsskyldighet och får inte påverka bedömningen av om en viss anpassningsåtgärd skall vidtas. Skyldigheten att medverka träffar samtliga operatörer som tillhandahåller nät och tjänster där meddelandena får bli föremål för beslut om avlyssning och övervakning.

Den bestämmelse som finns i dag i rättegångsbalken har skapat osäkerhet och problem vid tillämpningen. Regleringen bör bli mer tydlig i kravet på en aktiv medverkan och innebära en skyldighet att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning eller övervakning. En sådan reglering kommer att leda till bl.a. en mer effektiv verkställighet av tvångsmedelsbesluten utan någon ökning av integritetsintrånget hos den enskilde.

Hemlig dataavläsning – ett nytt tvångsmedel

Bör hemlig dataavläsning tillåtas?

I Danmark har de brottsutredande myndigheterna sedan några år tillbaka en möjlighet att utnyttja det hemliga tvångsmedlet dataavläsning. Metoden kan också användas i flera andra europeiska länder inom ramen för hemlig teleavlyssning samt i exempelvis USA och Canada. Dataavläsning som metod kan innebära att myndigheterna i hemlighet sänder en viss mjukvara till en dator. Den mjukvaran, en s.k. programkod, ger sedan myndigheterna uppgifter om vilken information som finns i datorn och hur datorn används, med andra ord såväl historiska uppgifter som uppgifter som genereras under verkställigheten. Myndigheterna kan alltså läsa av informationen, t.ex. innan den förs vidare via trådbunden eller trådlös förbindelse. Vilken information det är fråga om i det enskilda fallet och hur informationen skall levereras till myndigheten beror på vad myndigheterna har bestämt vid utformningen av mjukvaran. Det är alltså möjligt att i viss utsträckning precisera och begränsa vilken information man vill ha uppgift om och om informationen skall skickas till myndigheten via radio, över Internet eller t.ex. lagras på olika sätt i datorn för att sedan tas ut vid exempelvis framtida husrannsakan och beslag. Dataavläsning kan också innebära att hård- eller mjukvara med liknande funktion placeras i den informationsbärande utrustningen genom ett fysiskt ingrepp, t.ex. vid ett hemligt intrång i en persons bostad eller på dennes arbetsplats.

Under vårt arbete har det från flera håll framförts att möjligheten för de svenska brottsutredande myndigheterna att använda dataavläsning bör utredas.

Bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning har funnits under lång tid. Under den tiden har teknikutvecklingen varit oerhört kraftig och mycket snabb. Det är självklart att de allra senaste nyheterna på teknikområdet utnyttjas som verktyg särskilt i grov brottslig verksamhet. Det är helt nödvändigt för samhället att myndigheterna inte hamnar hjälplöst efter utan, inom ramen för att ett godtagbart integritetsintrång, får rätt att använda brottsutredande metoder som är effektiva och anpassade till den tekniska situation som råder vid varje givet tillfälle. Frågan om att införa dataavläsning måste alltså ses i ljuset av den pågående teknikutvecklingen och särskilt de grovt kriminellas förmåga att hela

tiden ”ligga i framkant” och utnyttja allt mer ”säkra” kommunikationsformer och modern teknik i sin verksamhet.

Utvecklingen under senare år har inneburit ett ökat hot från den allvarliga och organiserade brottsligheten. Att ingripa mot den är en synnerligen angelägen uppgift för de brottsbekämpande myndigheterna. Några av de brottsområden där kriminaliteten ofta kan sägas vara organiserad är narkotikabrott inklusive smuggling av dopningsmedel och läkemedel, smuggling av alkohol och tobak, bedrägerier, ekonomisk brottslighet, illegal handel med stulna fordon, rån och stölder (inklusive häleri) bl.a. riktade mot åldringar, människosmuggling, utpressning, förfalskning, penningtvätt, mord, misshandel, olaglig vapenhandel och handel med kvinnor inklusive koppleri. Utredning av sådan allvarlig brottslighet ställer särskilda krav på effektiva arbetsmetoder. Även om de tvångsmedel som är tillåtna i dag, exempelvis hemlig teleavlyssning och hemlig kameraövervakning, är betydelsefulla kan det ifrågasättas om de numera är tillräckliga i alla fall. Internationaliseringen och det genomdatoriserade samhälle vi lever i får i högsta grad konsekvenser för brott och brottsbekämpning.

Det är således numera utan tvekan så att den organiserade brottsligheten utnyttjar modern teknik och använder IT, t.ex. Internet, som ett effektivt arbetsredskap i verksamheten. Det förekommer också att de personer som begår mindre kvalificerade brott tar den tekniken till hjälp. Utvecklingen kommer att fortsätta i samma takt som medborgarnas och då även de kriminellas kompetens i IT-frågor ökar. I Internetsammanhang använder de kriminella både öppna miljöer, som är tillgängliga för vem som helst, och mer slutna miljöer, till vilka bara ett begränsat antal personer har tillträde. I vissa av dessa miljöer träffas samma personer regelbundet för att utbyta information. En viktig omständighet som ökar Internets attraktionskraft i dessa sammanhang är möjligheten att kommunicera på ett relativt anonymt och säkert sätt. Anonymiteten och säkerheten (främst frågan om kryptering) är vid sidan av globaliseringen och mobiliteten stora utmaningar som den IT-relaterade brottsligheten ställer upp för rättsväsendet. Om den kvalificerade brottsligheten med dess struktur, inriktning och tillvägagångssätt skall kunna bekämpas, är det helt nödvändigt att de brottsbekämpande myndigheterna bl.a. har möjlighet att använda effektiva arbetsmetoder, inte minst med anknytning till IT.

Det är mot den bakgrunden mycket angeläget att se på frågan om att införa bestämmelser om dataavläsning i svensk rätt efter den modell som finns i Danmark.

Det största behovet av dataavläsning finns vid brottslighet som innehåller organisation och planering. Särskilt vid organiserad eller annan allvarlig brottslighet är ofta vissa av de deltagande personerna utomordentligt skickliga i användningen av datorer. De utnyttjar sina kunskaper fullt ut för att genom olika åtgärder via datorerna genomföra brott, gömma information, hålla sig anonyma och undgå upptäckt.

Den snabba tekniska utvecklingen medför att det i dagsläget finns stora problem i brottsutredningar med att få fram uppgifter ur datorer eller avlyssna meddelanden mellan datorer. Det gäller särkilt när den informationen är skyddad av kryptering eller när program används som på annat sätt döljer information. I ett ständigt ökande antal brottsutredningar påträffas krypterad information i form av enskilda filer eller i en viss yta av lagringsutrymmet (exempelvis en dators hårddisk).

Det är välkänt bland kriminella vilka arbetsmetoder polisen har och inte har och den kunskapen utnyttjas för att göra den brottsliga verksamheten så effektiv som möjligt. Problemen accelererar i och med att användarvänligheten i kryptosystem och liknande ökar. Programapplikationer för den enskilde datoranvändaren finns i dag både till försäljning och tillgängliga för att ladda ner kostnadsfritt från Internet. Dessutom utvecklas fortlöpande nya, än mer avancerade program. Vanliga standardprodukter levereras i dag i stor omfattning med funktioner för kryptering, som också används som en marknadsföringsåtgärd av företag som tillhandahåller kommunikationstjänster via Internet för att kunden skall garanteras fullgod informationssäkerhet. Det finns en kraftigt ökande medvetenhet hos allmänheten om möjligheten att skydda sig från ”insyn” genom t.ex. krypteringsprogram. Många företag ser t.ex. kryptering som en nödvändighet i konkurrensen med andra företag.

I informationsbärande utrustning bearbetar användaren informationen ”öppet” innan den sparas och eventuellt krypteras. Kryptering i samband med kommunikation kan ske dels genom att operatören skyddar överföringen genom att kryptera den, dels genom att användaren själv krypterar, vilket kan ske oavsett om operatören gör det eller inte. För att de brottsbekämpande myndigheterna skall kunna få fram information krävs att den, av någon anledning, finns även i klartext eller att myndigheten får tillgång endera till datorn när krypteringen är ”upplåst” eller till det hemliga lösenord och/eller de PIN-koder som används som krypteringsnycklar eller som ger åtkomst till krypteringsnycklar. Att detta sker är mycket

ovanligt i dagsläget. I några få fall har krypteringen dock kunnat forceras när krypterad information har påträffats i beslagtagna datorer (i form av enskilda filer eller utrymmen på hårddisken). Det finns program som är konstruerade så att de t.ex. raderar information vid en viss tidpunkt och program som har dold information till vissa personer i annan öppen information. Det finns exempelvis också möjlighet för personer att ha ”ospårbara” kontakter i tillfälliga nätverk. En användning av dataavläsning skulle innebära att de brottsbekämpande myndigheterna skulle ha betydligt lättare att komma runt problemet med krypterad information och andra liknande tillvägagångssätt och därmed få framgång i utredningar.

Hemlig teleavlyssning används i brottsutredningar för att få tillgång till innehållet i ett telemeddelande. Den metoden kan inte användas för dekryptering utan fångar enbart upp de krypterade meddelandena. Det gäller såväl elektronisk post, medsända filer som exempelvis Internettelefoni. För att få tillgång till innehållet okrypterat behöver informationen fångas upp redan i den dator eller annan anordning som används för uppkoppling mot Internet.

Ett annat och minst lika stort problem är möjligheten för dem som agerar i brottsliga syften att vara anonyma vid användning av informationsteknik. Det är möjligt för de brottsbekämpande myndigheterna att knyta ett handlande på Internet till en viss IP-adress och även få uppgift från operatören om vilket abonnemang som kan knytas till den IP-adressen vid en viss tidpunkt. En uppgift om abonnemanget säger dock ingenting säkert om vem som satt vid datorn och agerade vid den aktuella tidpunkten. En användning av dataavläsning skulle innebära att de brottsbekämpande myndigheterna kan identifiera personen genom andra ageranden på Internet.

Med anledning av de kriminella personernas allt mer avancerade sätt att utnyttja modern teknik och den snabba tekniska utvecklingen står det klart att de brottsbekämpande myndigheterna, som ett mycket värdefullt komplement till de övriga tvångsmedlen, behöver ha möjlighet att genomföra de åtgärder som dataavläsning innebär. Det finns knappast några alternativa sätt att få fram den gömda informationen på. Enligt uppgift används motsvarande tillvägagångssätt av brottsbekämpande myndigheter i vissa länder standardmässigt inför exempelvis husrannsakningar, eftersom myndigheterna annars bedömer sig vara chanslösa inför den grövre brottslighetens metoder.

Även om det står klart att det finns ett stort behov av dataavläsning i utredningar rörande grova brott och att metoden är effektiv, är en mycket viktig fråga i sammanhanget givetvis om intresset av

att upprätthålla ett starkt skydd för den personliga integriteten ger utrymme för att tillåta dataavläsning.

Det är en svår uppgift att avväga integritetsintresset mot nödvändigheten av att myndigheterna har effektiva metoder för bl.a. brottsutredning. Det ligger i sakens natur att varje tvångsmedel innefattar ett integritetsintrång. Samtidigt måste beaktas att detta intrång ofta är blygsamt i jämförelse med den kränkning som offren för den allvarliga brottsligheten måste utstå. Ju allvarligare och ju mer svårutredd som brottsligheten blir, desto mer tvingas statsmakterna tillåta i form av tvångsåtgärder i brottsbekämpningen. Det kan aldrig accepteras att brottsligheten tar överhanden och att statsmakterna kapitulerar inför utvecklingen av en allt mer avancerad och förslagen brottslighet.

Omfattningen av det integritetsintrång som skulle bli följden om dataavläsning användes kan vara svår att uppskatta generellt och blir naturligtvis beroende av omständigheterna i det enskilda fallet. I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte kommer att bli större än vid tvångsmedlen hemlig teleavlyssning och hemlig kameraövervakning.

Det är mycket angeläget att de brottsbekämpande myndigheterna får rätt att använda moderna tekniska metoder för att kunna bekämpa t.ex. den grova narkotikabrottsligheten och annan allvarlig brottslighet. Ofta rör de fall där dataavläsning skulle bli aktuellt att använda situationer där det i princip inte finns någon möjlighet att på annat sätt skaffa fram avgörande uppgifter och bevis rörande grova brott. Samtidigt råder det inget tvivel om att en användning av dataavläsning innebär ett integritetsintrång. Med hänsyn till vad som har redovisats rörande behovet och effektiviteten av dataavläsning är det dock klarlagt att det skulle innebära en så stor vinst för bekämpningen av den allvarliga brottsligheten att det inte är försvarligt att avstå från att införa en möjlighet för de brottsbekämpande myndigheterna att använda metoden. Det integritetsintrång som typiskt sett uppkommer vid användning av dataavläsning är alltså med hänsyn till vad som redovisades tidigare inte så stort att det får hindra en lagstiftning på området. Därför lägger vi fram ett förslag om dataavläsning som ett nytt straffprocessuellt tvångsmedel som benämns hemlig dataavläsning. Metoden innebär att information i ett informationssystem kan avläsas med hjälp av program eller annat tekniskt hjälpmedel.

En reglering av användning av hemlig dataavläsning måste omgärdas av sådana rättssäkerhetsgarantier som säkerställer att bestämmelserna inte kan missbrukas och att allmänheten kan ha till-

tro till de myndigheter som tillämpar regleringen. Tvångsmedelsregleringen måste omgärdas av tydliga och strikta ramar för att det inte skall kunna misstänkas att regelsystemet kommer att utnyttjas utöver vad det skall tillåta. Bestämmelserna måste även utformas på ett sådant sätt att de kan accepteras av allmänheten som ett nödvändigt redskap för de brottsutredande myndigheterna i kampen mot den grövre kriminaliteten. Regleringen måste också innefatta ett starkt skydd för den personliga integriteten. Det är av avgörande betydelse att undvika att personer som är ovidkommande för en brottsutredning får sin integritet kränkt. Det är också viktigt att i möjligaste mån begränsa de integritetsintrång som den misstänkte utsätts för.

Lagteknisk lösning

Förslaget om hemlig dataavläsning innebär att ett nytt tvångsmedel införs där bl.a. ny teknik kommer att användas i brottsutredningar. Det kan konstateras att det finns ett behov av metoden och att den framstår som effektiv. Närmare detaljer i de frågorna är inte helt enkla att bedöma innan tvångsmedlet har tillämpats under en tid. Därför bör lagstiftningen om hemlig dataavläsning, i vart fall till en början, vara tidsbegränsad. De nya bestämmelserna bör därför inte tas in i rättegångsbalken utan i en särskild lag. Utformningen av bestämmelserna bör i så stor utsträckning som möjligt ansluta till den reglering som finns i dag rörande hemlig teleavlyssning och hemlig kameraövervakning. Tillämpningsområdet bör vara utformat så att tvångsmedlet används endast vid misstanke om grov brottslighet. Det innebär att hemlig dataavläsning inte kommer att kunna användas i ett större antal fall. För att det senare skall finnas ett fullgott underlag för en utvärdering av bestämmelserna och för en bedömning av frågan om lagen bör ges förlängd giltighetstid eller t.ex. permanentas, bör lagens giltighetstid sättas något längre än vad som annars hittills skett, t.ex. i fråga om lagen (1995:1506) om hemlig kameraövervakning. Till det kommer att de brottsutredande myndigheterna behöver viss tid för att utarbeta metoder och verktyg för genomförandet. Giltighetstiden bör till en början vara i vart fall fem år.

Domstolsprövning och offentliga ombud

I tvångsmedelssammanhang är det viktigt att skapa fullgoda rättsskyddsgarantier. Att det finns kontrollmekanismer i form av medverkan av domstol och offentliga ombud är av central betydelse vid användning av de mest integritetskänsliga tvångsmedlen. Allmänt sett kan det också diskuteras metoder för kontroll i efterhand, alltså i första hand underrättelseskyldighet mot den enskilde. Den frågan diskuterades av Buggningsutredningen och i den efterföljande lagrådsremissen. I båda sammanhangen drogs den slutsatsen att övervägande skäl talade mot att föreslå en sådan regel men att frågan borde övervägas på nytt i annat sammanhang. Vi har bedömt att det inte är aktuellt att överväga frågan nu, utan att det får ske i ett annat sammanhang än i detta betänkande.

Det är domstolen som fattar beslut om bl.a. hemlig teleavlyssning och hemlig kameraövervakning. Beslutanderätten bör ligga på domstol också för hemlig dataavläsning. Ansökan till tingsrätten om tillstånd till åtgärden får göras av åklagaren. Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig dataavläsning.

Tillräckliga skäl att införa en rätt för åklagare att interimistiskt besluta om hemlig dataavläsning har för dagen inte framkommit.

Vid vilka brott skall hemlig dataavläsning få äga rum?

Hemlig dataavläsning är främst avsedd att användas mot den grova brottsligheten. Utgångspunkten är därför att enbart de allvarligaste brotten bör omfattas av tillämpningsområdet. Vid utformningen av regler för när hemlig dataavläsning skall få äga rum finns det med hänsyn till den integritetskänsliga karaktären skäl att i princip vara lika restriktiv som vid dagens regler för hemlig teleavlyssning och hemlig kameraövervakning. Hemlig dataavläsning skall därför få äga rum vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff,
3. dataintrång, hets mot folkgrupp som inte är ringa och barnpornografibrott som inte är ringa, eller
4. annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år.

Brottsmisstankens styrka och behovet av åtgärden m.m.

Vid hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning gäller i dag, med ett visst undantag rörande det sistnämnda tvångsmedlet, att metoderna får användas när utredningen har kommit så långt att någon är skäligen misstänkt för brottet. Vi föreslår att detta som huvudregel skall vara ett krav även vid användning av hemlig dataavläsning. Dessutom skall regleringen vara densamma som de övriga tvångsmedlen när det gäller att åtgärden skall vara av synnerlig vikt för utredningen och att skälen för åtgärden skall uppväga det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse (proportionalitetsprincipen).

Undantag från kravet på skäligen misstänkt person

De två huvudsakliga skälen för att införa hemlig dataavläsning är problemen med dels krypterad information och liknande i datorer, dels möjligheten att vara anonym vid användning av informationsteknik. I många fall finns båda dessa problem samtidigt. Anonymitetsproblemet bottnar i det förhållandet att även om de brottsutredande myndigheterna lyckas knyta en IP-adress till ett visst abonnemang, är det ändå många gånger osäkert om den som står bakom abonnemanget också är den som har suttit vid datorn vid det tillfälle myndigheterna är intresserade av. Det kan t.ex. röra köp och försäljning av narkotika samt tillfällen för spridning och konsumtion av barnpornografi. Genom att använda hemlig dataavläsning kan de brottsutredande myndigheterna lyckas identifiera en person som skäligen misstänkt för brottsligheten. Av effektivitetsskäl är det därför nödvändigt att hemlig dataavläsning får äga rum även om det saknas en skäligen misstänkt person. Av hänsyn till det integritetsintrång som uppkommer är det, som en parallell till bestämmelserna om hemlig kameraövervakning, rimligt att föreskriva att hemlig dataavläsning i dessa fall endast får äga rum om åtgärden syftar till att fastställa vem som skäligen kan misstänkas för brottet och att åtgärden endast får avse ett informationssystem som har använts eller används vid brottet.

Sambandet mellan en misstänkt och informationssystemet

Eftersom hemlig dataavläsning är ett integritetskänsligt tvångsmedel är det naturligt att det ställs upp ett krav på samband mellan den misstänkte och det eller de informationssystem som åtgärden skall avse. I fall där det finns en skäligen misstänkt person får hemlig dataavläsning endast avse ett informationssystem som det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av. Om åtgärden avser ett informationssystem i någon annans stadigvarande bostad, skall hemlig dataavläsning få äga rum bara om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.

Tillståndstiden, tillträde till platsen m.m.

Ett beslut om hemlig dataavläsning skall enligt förslaget gälla under viss tid. Tiden får, liksom vid t.ex. hemlig teleavlyssning och hemlig kameraövervakning, inte bestämmas längre än vad som är nödvändigt och får inte överstiga en månad från dagen för beslutet. Besluten kan förnyas av domstolen.

Tillståndet kan förenas med villkor för att begränsa integritetsintrånget i olika avseenden.

Ett beslut att tillåta hemlig dataavläsning skall innehålla uppgift om vilket eller vilka informationssystem som tillståndet avser samt, när någon är misstänkt för brottet, vem som är misstänkt.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, skall åklagaren eller rätten omedelbart häva beslutet.

Som nämndes tidigare är ett av sätten att verkställa hemlig dataavläsning att hård- eller mjukvaran placeras i datautrustningen genom ett fysiskt ingrepp, t.ex. vid intrång i hemlighet i någons bostad eller på en arbetsplats. Ett beslut om tillstånd får därför innefatta rätt för de brottsutredande myndigheterna att i hemlighet bereda sig tillträde till en plats som annars särskilt skyddas mot intrång i syfte att installera de tekniska hjälpmedlen. Vid genomförande av hemlig dataavläsning skall givetvis olägenhet eller skada inte få förorsakas utöver vad som är oundgängligen nödvändigt.

När ett tekniskt hjälpmedel som har installerats inte längre får användas, skall det tas bort så snart som möjligt. I stället för att återta hjälpmedlet skall det finnas en rätt att göra det obrukbart, om tekniken medger detta och det skulle vara lämpligare i ett visst

fall. För att skapa en slags yttre kontroll av verkställigheten skall rätten underrättas när hjälpmedlet har återtagits eller gjorts obrukbart.

Undantag för avläsning av meddelanden mellan den misstänkte och hans försvarare

Hemlig dataavläsning skall enligt förslaget inte få ske av meddelanden mellan den misstänkte och hans försvarare. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer.

Överskottsinformation

Vid användning av hemliga tvångsmedel kan det komma fram uppgifter som inte har något som helst samband med det brott som har legat till grund för tvångsmedelsbeslutet. Uppgifterna kan dock i stället vara av betydelse för utredningen av ett annat brott eller för att förhindra brott. De kan beröra den person som förundersökningen gäller eller andra personer som är ovidkommande i det sammanhanget. Det kan också röra sig om uppgifter som inte har samband med något brott men som är av betydelse i ett annat sammanhang och då främst för andra myndigheter, exempelvis sociala myndigheter. I vad mån sådan överskottsinformation får utnyttjas är inte generellt reglerat i lag även om frågan ändå inte kan sägas vara oreglerad.

Regeringen har nyligen lagt fram ett förslag om reglering av de brottsbekämpande myndigheternas användning av överskottsinformation som framkommer vid användning av hemliga tvångsmedel. Bestämmelserna avser användning av informationen för såväl brottsutredande som brottsförebyggande ändamål.

Den typ av reglering som regeringen har föreslagit för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning bör finnas även för användning av hemlig dataavläsning. Det innebär att om det vid hemlig dataavläsning har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avläsning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller
2. det finns särskilda skäl.

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

Hantering av inhämtad information

På samma sätt som för andra tvångsmedel skall en upptagning som har gjorts vid hemlig dataavläsning granskas snarast möjligt. De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brott. De skall därefter förstöras.

Parlamentarisk kontroll

Sedan många år tillämpas den ordningen att regeringen årligen i en skrivelse till riksdagen redovisar de brottsutredande myndigheternas tillämpning av hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Det är naturligt att en sådan redovisning även sker avseende tillämpningen av bestämmelserna om hemlig dataavläsning.

Konsekvenser och genomförande

Förslaget om att de brottsutredande myndigheternas tillgång till uppgifter om meddelanden uteslutande skall regleras i 27 kap. RB kan komma att kräva ett resurstillskott på högst tre miljoner kronor vardera för åklagar- respektive domstolsväsendet. I övrigt innebär förslagen i betänkandet inte några sådana ekonomiska konsekvenser att det behövs resursförstärkningar till någon del av statens verksamhet.

Våra förslag i de delar som gäller operatörernas anpassningsskyldighet och medverkan vid verkställighet av tvångsmedelsbeslut innebär en viss skärpning av kraven på operatörerna. Det kommer att leda till en något större kostnad för dessa än de har i dag. Liksom är fallet med de nuvarande kostnaderna kommer de dock att

kunna finansieras genom att operatörerna för dessa vidare på sina abonnenter. Den avgiftshöjning som på detta sätt kan komma att drabba respektive abonnent är försumbar.

Förslagen i betänkandet bör kunna träda i kraft den 1 januari 2007. Några övergångsbestämmelser behövs inte.

Författningsförslag

1. Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs att 4 kap. 8 § brottsbalken skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap. Om brott mot frihet och frid	
	8 §
Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller *telemeddelande*, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.	Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller *som sådant meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken*, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.

Denna lag träder i kraft den 1 januari 2007.

2. Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken
dels att rubriken till 27 kap. skall ha följande lydelse,
dels att 27 kap. 18-26 och 28 §§ skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
27 kap. Om beslag, *hemlig teleavlyssning* m.m.	**27 kap. Om beslag, *avlyssning* m.m.**
	18 §
Hemlig teleavlyssning innebär att telemeddelanden, som befordras eller har befordrats *till eller från ett telefonnummer, en kod eller annan teleadress,* i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.	*Ett meddelande* som befordras eller har befordrats *i ett elektroniskt kommunikationsnät får efter tillstånd* i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.
Hemlig teleavlyssning får användas vid förundersökning angående	*Sådan avlyssning* får användas vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff eller
3. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Ett tillstånd enligt denna paragraf omfattar även sådana åtgärder som avses i 19 §.

Med elektroniskt kommunikationsnät i detta kapitel avses detsamma som i lagen (2003:389) om elektronisk kommunikation med undantag för nät som enbart är avsett för utsändning av program i ljudradio eller television.

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.	Uppgifter *får efter tillstånd* i hemlighet hämtas in om *meddelanden* som befordras eller har befordrats *med tekniskt hjälpmedel till eller från ett elektroniskt kommunikationsnät och för lokalisering eller identifiering av ett sådant tekniskt hjälpmedel. Meddelanden får även* hindras från att nå fram *till eller lämna ett sådant tekniskt hjälpmedel*. *Med uppgifter för lokalisering i första stycket avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits. Med uppgifter för identifiering i samma stycke avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden.*
Hemlig teleövervakning får användas vid förundersökning angående	*Åtgärder som avses i första stycket (övervakning)* 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.

20 §

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*	*Avlyssning* och *övervakning enligt 18 respektive 19 §* får, *utom i fall som avses i tredje stycket, bara* ske om någon är skäligen misstänkt för brottet. *Åtgärden skall vara* av synnerlig

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.

vikt för utredningen *och* får, *utom i fall som avser identifiering av tekniska hjälpmedel, bara* avse

1. *sådana tekniska hjälpmedel* 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. *sådana tekniska hjälpmedel* som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Övervakning i syfte att identifiera tekniska hjälpmedel får avse sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte.

Vid förundersökning angående brott som anges i 18 § andra stycket får övervakning användas även om det inte finns någon som är skäligen misstänkt för brottet.

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

21 §

Frågor om *hemlig teleavlyssning* och *hemlig teleövervakning*

Frågor om *tillstånd till avlyssning* och *övervakning enligt 18*

prövas av rätten på ansökan av åklagaren.

I ett beslut att tillåta *hemlig teleavlyssning* eller *hemlig teleövervakning* skall det anges *vilken teleadress och* 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 tillstånd till avlyssning eller övervakning skall det särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga *telenät*.

respektive 19 § prövas av rätten på ansökan av åklagaren. *Åklagaren får dock i brådskande fall fatta beslut om övervakning enligt 19 §. Ett sådant beslut skall genast skriftligen anmälas hos rätten, som skyndsamt skall pröva frågan.*

I ett beslut att tillåta *avlyssning* eller *övervakning* skall 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. *Rätten får också i övrigt föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.*

I tillstånd till avlyssning eller övervakning skall det särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga *elektroniska kommunikationsnät*.

22 §

Hemlig teleavlyssning får *ej* ske av *telefonsamtal eller andra telemeddelanden* mellan den misstänkte och hans försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant *samtal eller* meddelande, skall avlyssningen avbrytas.

Avlyssning enligt 18 § får *inte* ske av *meddelanden* mellan den misstänkte och hans försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant meddelande, skall avlyssningen avbrytas.

Upptagningar och uppteckningar skall, i den mån de omfattas av förbudet, omedelbart förstöras.

23 §

Om det inte längre finns skäl för ett beslut om *hemlig teleav-*

Om det inte längre finns skäl för ett beslut om *avlyssning* eller

lyssning eller *hemlig teleövervakning*, skall åklagaren eller rätten omedelbart häva beslutet.	*övervakning enligt 18 respektive 19 §*, skall åklagaren eller rätten omedelbart häva beslutet.

23 a §[1]

Om det vid *hemlig teleavlyssning* eller *hemlig teleövervakning* har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avlyssning eller övervakning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om	Om det vid *avlyssning* eller *övervakning enligt 18 respektive 19 §* har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avlyssning eller övervakning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller

2. det finns särskilda skäl.

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

24 §[2]

En upptagning eller uppteckning som gjorts vid *hemlig teleavlyssning* skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.	En upptagning eller uppteckning som gjorts vid *avlyssning enligt 18 §* skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.

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

[1] Nuvarande lydelse enligt förslag i prop. 2004/05:143
[2] Nuvarande lydelse enligt förslag i prop. 2004/05:143

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

25 §

Har rätten lämnat tillstånd till *hemlig teleavlyssning* eller *hemlig teleövervakning*, får de tekniska hjälpmedel som behövs för *avlyssningen eller övervakningen* användas.

Har rätten lämnat tillstånd till *avlyssning* eller *övervakning enligt 18 respektive 19 §*, får de tekniska hjälpmedel som behövs för *åtgärden* användas.

En enskild är skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av avlyssning eller övervakning.

I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om *hemlig teleavlyssning* och *hemlig teleövervakning* som gäller för den som driver verksamhet som avses i 6 kap. 19 § den lagen.

I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om *avlyssning* och *övervakning* som gäller för den som driver verksamhet som avses i 6 kap. 19 § den lagen.

26 §

Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om *hemlig teleavlyssning*.

Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om *avlyssning enligt 18 §*.

Ett offentligt ombud har rätt att ta del av vad som förekommer i ärendet, att yttra sig i ärendet och att överklaga rättens beslut.

28 §

När en ansökan om *hemlig teleavlyssning* har kommit in till rätten, skall rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet skall åklagaren och det offentliga ombudet närvara.

När en ansökan om *avlyssning enligt 18 §* har kommit in till rätten, skall rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet skall åklagaren och det offentliga ombudet närvara.

Om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med tvångsmedlet, får sammanträde hållas och beslut fattas utan att ett offentligt ombud har varit närvarande eller annars fått tillfälle att yttra sig.

Ett uppdrag som offentligt ombud gäller även i högre rätt.

Denna lag träder i kraft den 1 januari 2007.

3. Förslag till lag om hemlig dataavläsning

Definition

1 § Med hemlig dataavläsning avses i denna lag att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål.

När hemlig dataavläsning får äga rum

2 § Hemlig dataavläsning får äga rum bara efter tillstånd enligt denna lag.

3 § Hemlig dataavläsning får äga rum vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff,
3. brott enligt 4 kap. 9 c § brottsbalken, brott enligt 16 kap. 8 § brottsbalken som inte är att anse som ringa, brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, eller
4. annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år.

4 § Hemlig dataavläsning får äga rum, om

1. någon är skäligen misstänkt för brottet,
2. åtgärden är av synnerlig vikt för utredningen, och
3. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.

Hemlig dataavläsning får också äga rum när det inte finns någon som är skäligen misstänkt för brottet, om åtgärden syftar till att fastställa vem som skäligen kan misstänkas för brottet.

Vad som får avläsas

5 § Hemlig dataavläsning i fall som avses i 4 § första stycket får endast avse informationssystem som det finns särskild anledning att

anta att den misstänkte har använt sig av eller kommer att använda sig av. Avser åtgärden informationssystem i någon annans stadigvarande bostad, får hemlig dataavläsning äga rum endast om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.

6 § Hemlig dataavläsning i fall som avses i 4 § andra stycket får endast avse informationssystem som har använts eller används vid brottet.

Genomförande av hemlig dataavläsning

7 § Vid genomförande av hemlig dataavläsning får olägenhet eller skada inte förorsakas utöver vad som är oundgängligen nödvändigt.

Hemlig dataavläsning får inte ske av sådana meddelanden mellan den misstänkte och hans försvarare som avses i 27 kap. 22 § rättegångsbalken. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer.

Vid hemlig dataavläsning får med särskilt tillstånd de tekniska hjälpmedlen i hemlighet installeras på en plats som annars särskilt skyddas mot intrång.

8 § Om det vid hemlig dataavläsning har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avläsning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller
2. det finns särskilda skäl.

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

9 § En upptagning som har gjorts vid hemlig dataavläsning skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 27 kap. 12 § första stycket rättegångsbalken.

De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra

föreståend brott skall de bevaras så länge det behövs för att förhindra brott. De skall därefter förstöras.

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

Prövning av frågor om hemlig dataavläsning

10 § Frågor om tillstånd till hemlig dataavläsning prövas av tingsrätten på ansökan av åklagaren. Därvid gäller i fråga om behörig domstol 19 kap. 12 § rättegångsbalken. Vid prövningen gäller vad som föreskrivs om offentligt ombud i 27 kap. 26-30 §§ samma balk.

Vad ett beslut om tillstånd skall innehålla

11 § Ett beslut att tillåta hemlig dataavläsning skall innehålla uppgifter om det informationssystem tillståndet gäller och, när någon är misstänkt för brottet, vem som är misstänkt.

Om tillståndet är förenat med en rätt att installera tekniska hjälpmedel enligt 7 §, skall det särskilt anges i beslutet.

I beslutet skall det också anges under vilken tid tillståndet gäller. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Rätten får också i övrigt föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.

Verkställighet och upphävande av beslut

12 § Rättens beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, skall åklagaren eller rätten omedelbart häva beslutet.

Förfarandet med tekniska hjälpmedel

13 § Ett tekniskt hjälpmedel som har installerats skall återtas eller göras obrukbart så snart det kan ske efter det att tiden för tillståndet gått ut eller tillståndet hävts. När hjälpmedlet har återtagits eller gjorts obrukbart, skall rätten underrättas om det.

Överklagande

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

Denna lag träder i kraft den 1 januari 2007 och gäller till utgången av år 2011.

4. Förslag till lag om ändring i lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål

Härigenom föreskrivs att 5 § lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §
Tillstånd *enligt 27 kap. rättegångsbalken* till *hemlig teleavlyssning* eller *hemlig teleövervakning* får meddelas, även om brottet inte omfattas av *27 kap. 18 eller 19 § rättegångsbalken*. Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § i den lagen.	Tillstånd till *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* får meddelas, även om brottet inte omfattas av *de angivna bestämmelserna*. Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § i den lagen. *Tillstånd till hemlig dataavläsning får meddelas enligt lagen (0000:00) om hemlig dataavläsning, även om brottet inte omfattas av 3 § i den lagen.*
Kan det befaras att inhämtande av rättens tillstånd till *hemlig teleavlyssning, hemlig teleövervakning eller* hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.	Kan det befaras att inhämtande av rättens tillstånd till *avlyssning, övervakning,* hemlig kameraövervakning *eller hemlig dataavläsning* skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.

Denna lag träder i kraft den 1 januari 2007.

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

Härigenom föreskrivs att 5 kap. 1 §, 9 kap. 8 §, 14 kap. 2 § och 16 kap. 1 § sekretesslagen (1980:100) skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 kap. Sekretess med hänsyn främst till intresset att förebygga eller beivra brott

1 §

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,

2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,

4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, *eller*	4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,
5. Finansinspektionens verksamhet som rör övervakning enligt insiderstrafflagen (2000:1086),	5. Finansinspektionens verksamhet som rör övervakning enligt insiderstrafflagen (2000:1086), *eller*
	6. prövning av frågor enligt 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott gäller sekretess, 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 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 underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndighet i konkurs och inom exekutionsväsendet för uppgift som angår misstanke om brott.

Utan hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av

1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,

2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid rikspolisstyrelsens säkerhetsavdelning, eller

3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

9 kap. Sekretess med hänsyn till skyddet för enskilds förhållanden av såväl personlig som ekonomisk natur

8 §

Sekretess gäller hos tillståndsmyndigheten på postområdet och hos myndighet som bedriver postverksamhet för uppgift som angår särskild postförsändelse. Om sekretess inte följer av annan bestämmelse, får dock sådan uppgift lämnas till den som är försändelsens avsändare eller mottagare.

Sekretess gäller hos myndighet som *driver televerksamhet* för *uppgift som angår särskilt telefonsamtal eller annat telemed-*

Sekretess gäller hos myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikations-*

delande. Om sekretess inte följer av annan bestämmelse, får dock sådan uppgift lämnas till den som har tagit del i *telefonsamtalet eller annars är telemeddelandets avsändare eller mottagare eller som innehar apparat som har använts för telemeddelandet*.	*tjänst* för *innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande*. Om sekretess inte följer av *någon* annan bestämmelse, får dock sådan uppgift lämnas till den som har tagit del i *utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller, beträffande något annat än innehållet i meddelandet, innehavaren av ett abonnemang som använts för ett elektroniskt meddelande*.

Sekretess gäller hos myndighet som handhar allmän samfärdsel för uppgift som angår enskilds förbindelse med samfärdselverksamheten och som inte avses i första eller andra stycket, om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Sekretess gäller för uppgift vid särskild sambandstjänst inom totalförsvaret, om uppgiften avser *telemeddelande* som utomstående utväxlar på *telenät*.	Sekretess gäller för uppgift vid särskild sambandstjänst inom totalförsvaret, om uppgiften avser *elektroniskt meddelande* som utomstående utväxlar på *elektroniskt kommunikationsnät*.

Sekretess gäller i ärenden som avser TV-avgifter för uppgift om enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon honom närstående lider skada eller men om uppgiften röjs.

I fråga om uppgift i allmän handling gäller sekretessen enligt tredje och femte styckena i högst tjugo år.

14 kap. Bestämmelser om vissa begränsningar i sekretessen och om förbehåll

2 §

Sekretess hindrar inte att uppgift i annat fall än som avses i 1 § lämnas till myndighet, om uppgiften behövs där för

1. förundersökning, rättegång, ärende om disciplinansvar eller skiljande från anställning eller annat jämförbart rättsligt förfarande vid myndigheten mot någon rörande hans deltagande i verksamheten vid den myndighet där uppgiften förekommer,

2. omprövning av beslut eller åtgärd av den myndighet där uppgiften förekommer, eller

3. tillsyn över eller revision hos den myndighet där uppgiften förekommer.

Sekretess hindrar inte att uppgift lämnas i muntligt eller skriftligt yttrande av sakkunnig till domstol eller myndighet som bedriver förundersökning i brottmål.

Sekretess hindrar inte att uppgift om enskilds adress, telefonnummer och arbetsplats eller uppgift i form av fotografisk bild av enskild lämnas till en myndighet, om uppgiften behövs där för delgivning enligt delgivningslagen (1970:428). Uppgift hos myndighet som *driver televerksamhet* om enskilds telefonnummer får dock, om den enskilde hos myndigheten begärt att abonnemanget skall hållas hemligt och uppgiften omfattas av sekretess enligt 9 kap. 8 § tredje stycket, lämnas ut endast om den myndighet som begär uppgiften finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl.

Sekretess hindrar inte att uppgift som angår misstanke om brott lämnas till åklagarmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet, om fängelse är föreskrivet för brottet och

Sekretess hindrar inte att uppgift om enskilds adress, telefonnummer och arbetsplats eller uppgift i form av fotografisk bild av enskild lämnas till en myndighet, om uppgiften behövs där för delgivning enligt delgivningslagen (1970:428). Uppgift hos myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst* om enskilds telefonnummer får dock, om den enskilde hos myndigheten begärt att abonnemanget skall hållas hemligt och uppgiften omfattas av sekretess enligt 9 kap. 8 § tredje stycket, lämnas ut endast om den myndighet som begär uppgiften finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl.

Sekretess hindrar inte att uppgift som angår misstanke om brott lämnas till åklagarmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet, om fängelse är föreskrivet för brottet och

detta kan antas föranleda annan påföljd än böter.	detta kan antas föranleda annan påföljd än böter. *Detta gäller dock inte uppgift som omfattas av sekretess enligt 9 kap. 8 § andra stycket.*
För uppgift som omfattas av sekretess enligt 7 kap. 1-6 och 34 §§, 8 kap. 8 § första stycket, 9 eller 15 § eller 9 kap. 4 eller 7 §, 8 § första *eller andra* stycket eller 9 § gäller vad som föreskrivs i fjärde stycket endast såvitt angår misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Dock hindrar sekretess enligt 7 kap. 1, 4 eller 34 § inte att uppgift som angår misstanke om brott enligt 3, 4 eller 6 kap. brottsbalken mot någon som inte har fyllt arton år lämnas till åklagarmyndighet eller polismyndighet. Inte heller hindrar sekretess enligt 7 kap. 1 eller 4 § att uppgift som gäller misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i ett år och som avser överföring eller försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168) lämnas till åklagarmyndighet eller polismyndighet.	För uppgift som omfattas av sekretess enligt 7 kap. 1-6 och 34 §§, 8 kap. 8 § första stycket, 9 eller 15 § eller 9 kap. 4 eller 7 §, 8 § första stycket eller 9 § gäller vad som föreskrivs i fjärde stycket endast såvitt angår misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Dock hindrar sekretess enligt 7 kap. 1, 4 eller 34 § inte att uppgift som angår misstanke om brott enligt 3, 4 eller 6 kap. brottsbalken mot någon som inte har fyllt arton år lämnas till åklagarmyndighet eller polismyndighet. Inte heller hindrar sekretess enligt 7 kap. 1 eller 4 § att uppgift som gäller misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i ett år och som avser överföring eller försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168) lämnas till åklagarmyndighet eller polismyndighet.

Sekretess enligt 7 kap. 1 § och 4 § första och tredje styckena hindrar inte att uppgift om enskild, som inte fyllt arton år eller som fortgående missbrukar alkohol, narkotika eller flyktiga lösningsmedel, eller närstående till denne lämnas från myndighet inom hälso- och sjukvården och socialtjänsten till annan sådan myndighet, om det behövs för att den enskilde skall få nödvändig vård, behandling eller annat stöd. Detsamma gäller i fråga om lämnande av upp-

gift om gravid kvinna eller närstående till henne, om det behövs för en nödvändig insats till skydd för det väntade barnet.

16 kap. Om ansvar på tryckfrihetsförordningens och yttrandefrihetsgrundlagens områden för brott mot tystnadsplikt

1 §

Nuvarande lydelse

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* och *hemlig teleövervakning eller* hemlig kameraövervakning på grund av beslut av domstol, undersökningsledare eller åklagare
5 kap. 7 §	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag, *hemlig teleavlyssning* och *hemlig teleövervakning eller* hemlig kameraövervakning på grund av beslut av domstol 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 teleövervakning* på grund av beslut av domstol, undersökningsledare eller åklagare

Föreslagen lydelse

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, *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken,* hemlig kameraövervakning *eller hemlig dataavläsning* på grund av beslut av domstol, undersökningsledare eller åklagare
5 kap. 7 §	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag, *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken,* hemlig kameraövervakning *eller hemlig dataavläsning* på grund av beslut av domstol 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 *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* på grund av beslut av domstol, undersökningsledare eller åklagare

---

Denna lag träder i kraft den 1 januari 2007.

6. Förslag till lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Härigenom föreskrivs att 28 § lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	28 §
Kan det befaras att inhämtande av rättens tillstånd till *hemlig teleavlyssning* eller *hemlig teleövervakning* enligt 27 kap. 18 *eller* 19 § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken *eller* hemlig kameraövervakning enligt lagen (1995:1506) om hemlig kameraövervakning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får åtgärden beslutas av åklagaren. I fråga om kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken får åtgärden även beslutas av undersökningsledaren. Anmälan som avses i tredje stycket i nämnda paragraf skall göras hos den som har fattat beslutet. Denne skall pröva beslagsfrågan.	Kan det befaras att inhämtande av rättens tillstånd till *avlyssning* eller *övervakning* enligt 27 kap. 18 *respektive* 19 § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, hemlig kameraövervakning enligt lagen (1995:1506) om hemlig kameraövervakning *eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning* skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får åtgärden beslutas av åklagaren. I fråga om kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken får åtgärden även beslutas av undersökningsledaren. Anmälan som avses i tredje stycket i nämnda paragraf skall göras hos den som har fattat beslutet. Denne skall pröva beslagsfrågan.

Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, skall det genast anmälas hos rätten. Anmälan skall vara skriftlig och innehålla skälen för beslutet. Rät-

ten skall pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, skall det upphävas.

Denna lag träder i kraft den 1 januari 2007.

7. Förslag till lag om ändring i lagen (1991:572) om särskild utlänningskontroll

Härigenom föreskrivs att 20-22 §§ lagen (1991:572) om särskild utlänningskontroll skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	20 §
För ett sådant ändamål som avses i 19 § första stycket kan rätten, om det finns synnerliga skäl, meddela Rikspolisstyrelsen eller en polismyndighet tillstånd *enligt 27 kap. rättegångsbalken* till *hemlig teleavlyssning* eller, om det är tillräckligt, *hemlig teleövervakning*.	För ett sådant ändamål som avses i 19 § första stycket kan rätten, om det finns synnerliga skäl, meddela Rikspolisstyrelsen eller en polismyndighet tillstånd till *avlyssning* eller, om det är tillräckligt, *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning.*

Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Rikspolisstyrelsen eller en polismyndighet tillstånd att närmare undersöka, öppna eller granska post- eller telegrafförsändelser, brev, andra slutna handlingar eller paket som har ställts till utlänningen eller som avsänts från honom och som påträffas vid husrannsakan, kroppsvisitation eller kroppsbesiktning eller som finns hos ett befordringsföretag.

I det tillstånd som avses i andra stycket kan rätten förordna att en försändelse som avses i tillståndet och som ankommer till ett befordringsföretag, skall hållas kvar till dess den närmare undersökts, öppnats eller granskats. Förordnandet skall innehålla underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den som har begärt åtgärden.

	21 §
Det tillstånd som avses i 20 § skall meddelas att gälla för en viss tid som inte överstiger en månad.	
Frågan om tillstånd prövas av Stockholms tingsrätt på yrkande	Frågan om tillstånd prövas av Stockholms tingsrätt på yrkande

av *r*ikspolisstyrelsen eller en polismyndighet. Rättens beslut om tillstånd gäller omedelbart. I fråga om förfarandet tillämpas i övrigt 27 kap. rättegångsbalken på motsvarande sätt.

av *R*ikspolisstyrelsen eller en polismyndighet. Rättens beslut om tillstånd gäller omedelbart. I fråga om förfarandet tillämpas i övrigt 27 kap. rättegångsbalken *respektive lagen (0000:00) om hemlig dataavläsning* på motsvarande sätt.

21 a §[1]

Om det vid *hemlig teleavlyssning* eller *hemlig teleövervakning* har kommit fram uppgifter om ett brott som inte är av betydelse för det ändamål som har föranlett avlyssningen *eller* övervakningen, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

Om det vid *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning* har kommit fram uppgifter om ett brott som inte är av betydelse för det ändamål som har föranlett avlyssningen, övervakningen *eller avläsningen*, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller
2. det finns särskilda skäl.

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

22 §[2]

En upptagning eller uppteckning som har gjorts vid *hemlig teleavlyssning* skall granskas snarast möjligt. Granskningen får utföras endast av rätten, Rikspolisstyrelsen, en polismyndig-

En upptagning eller uppteckning som har gjorts vid *avlyssning enligt 27 kap. 18 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning* skall

[1] Nuvarande lydelse enligt förslag i prop. 2004/05:143
[2] Nuvarande lydelse enligt förslag i prop. 2004/05:143

het eller en åklagare.

Om upptagningen eller upptecknin-gen innehåller något som inte är av betydelse för det ändamål som har föranlett avlyssningen, skall den i denna del omedelbart förstöras efter granskningen. I fråga om brott eller förestående brott som inte är av betydelse för det ändamål som har föranlett avlyssningen skall dock 27 kap. 24 § andra och tredje styckena rättegångsbalken tillämpas.

granskas snarast möjligt. Granskningen får utföras endast av rätten, Rikspolisstyrelsen, en polismyndighet eller en åklagare.

Om upptagningen eller upptecknin-gen innehåller något som inte är av betydelse för det ändamål som har föranlett avlyssningen *eller avläsningen*, skall den i denna del omedelbart förstöras efter granskningen. I fråga om brott eller förestående brott som inte är av betydelse för det ändamål som har föranlett avlyssningen *eller avläsningen* skall dock 27 kap. 24 § andra och tredje styckena rättegångsbalken *respektive 9 § andra och tredje styckena lagen (0000:00) om hemlig dataavläsning* tillämpas.

En försändelse eller någon annan handling som omfattas av tillstånd enligt 20 § får inte närmare undersökas, öppnas eller granskas av någon annan än rätten, Rikspolisstyrelsen, en polismyndighet eller en åklagare. En sådan handling skall undersökas snarast möjligt. När undersökningen har slutförts, skall en försändelse som finns hos ett befordringsföretag tillställas den till vilken försändelsen är ställd och en annan handling återlämnas till den hos vilken handlingen påträffats, om den inte tas i beslag.

Denna lag träder i kraft den 1 januari 2007.

8. Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 § och 4 kap. 25-28 §§ skall ha följande lydelse,

dels att rubrikerna närmast före 4 kap. 25-28 §§ skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap. Inledande bestämmelser	
2 §[1]	
Rättslig hjälp enligt denna lag omfattar följande åtgärder:	
---	---
6. *hemlig teleavlyssning* och *hemlig teleövervakning*,	6. *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*,
7. tekniskt bistånd med *hemlig teleavlyssning* och *hemlig teleövervakning*,	7. tekniskt bistånd med *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*,
8. tillstånd till gränsöverskridande *hemlig teleavlyssning* och *hemlig teleövervakning*,	8. tillstånd till gränsöverskridande *avlyssning* och *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*,
9. hemlig kameraövervakning,	9. hemlig kameraövervakning *och hemlig dataavläsning*,
---	---

Lagen hindrar inte att hjälp lämnas med annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

[1] Nuvarande lydelse enligt förslag i prop. 2004/05:144

4 kap. Särskilda bestämmelser om olika former av rättslig hjälp[2]

Rättslig hjälp och tekniskt bistånd med *hemlig teleavlyssning* och *hemlig teleövervakning*

Rättslig hjälp och tekniskt bistånd med *avlyssning* och *övervakning*

Rättslig hjälp i Sverige med *hemlig teleavlyssning* och *hemlig teleövervakning*

Rättslig hjälp i Sverige med *avlyssning* och *övervakning*

25 §

En ansökan om *hemlig teleavlyssning* eller *hemlig teleövervakning* av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden.

En ansökan om *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden.

Upptagningar och uppteckningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken.

[2] Nuvarande lydelse enligt förslag i prop. 2004/05:144

Omedelbar överföring av *telemeddelanden* eller uppgifter om *telemeddelanden* från Sverige till den ansökande staten

Omedelbar överföring av *meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken* eller uppgifter om *sådant meddelande* från Sverige till den ansökande staten

25 a §

Rättens beslut enligt 25 § att tillåta *hemlig teleavlyssning* eller *hemlig teleövervakning* får verkställas genom omedelbar överföring av *telemeddelanden* eller uppgifter om *telemeddelanden* till den ansökande staten, om det kan ske under betryggande former. Verkställighet genom omedelbar överföring får endast ske i förhållande till en stat som är medlem i Europeiska unionen eller till Island eller Norge. Åklagaren prövar om förutsättningar för omedelbar överföring finns. Om omedelbar överföring av *telemeddelanden* sker, får upptagning eller uppteckning inte göras i Sverige.

Rättens beslut enligt 25 § att tillåta *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* får verkställas genom omedelbar överföring av *meddelandena* eller uppgifter om *dessa* till den ansökande staten, om det kan ske under betryggande former. Verkställighet genom omedelbar överföring får endast ske i förhållande till en stat som är medlem i Europeiska unionen eller till Island eller Norge. Åklagaren prövar om förutsättningar för omedelbar överföring finns. Om omedelbar överföring av *meddelanden* sker, får upptagning eller uppteckning inte göras i Sverige.

Tekniskt bistånd i Sverige med *hemlig teleavlyssning* och *hemlig teleövervakning*

Tekniskt bistånd i Sverige med *avlyssning* och *övervakning*

25 b §

Tekniskt bistånd med *hemlig teleavlyssning* eller *hemlig teleövervakning* i form av omedelbar överföring av *telemeddelanden* eller uppgifter om *telemeddelanden* får lämnas i Sverige enligt denna paragraf.

Tekniskt bistånd med *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* i form av omedelbar överföring av *meddelande som avses i de bestämmelserna* eller uppgifter om *sådant meddelande* får lämnas i Sverige enligt denna paragraf.

Tekniskt bistånd lämnas på ansökan av en annan stat som är medlem i Europeiska unionen eller av Island eller Norge, om	Tekniskt bistånd lämnas på ansökan av en annan stat som är medlem i Europeiska unionen eller av Island eller Norge, om
1. *teleavlyssningen* eller *teleövervakningen* avser någon som befinner sig i en av dessa stater,	1. *avlyssningen* eller *övervakningen* avser någon som befinner sig i en av dessa stater,
2. ansökan innehåller en bekräftelse på att ett beslut om *hemlig teleavlyssning* eller *hemlig teleövervakning* i en brottsutredning har meddelats i den ansökande staten, och	2. ansökan innehåller en bekräftelse på att ett beslut om *avlyssning* eller *övervakning* i en brottsutredning har meddelats i den ansökande staten, och
3. omedelbar överföring av *telemeddelanden* eller uppgifter om *telemeddelanden* kan ske under betryggande former till den ansökande staten.	3. omedelbar överföring av *meddelanden* eller uppgifter om *meddelanden* kan ske under betryggande former till den ansökande staten.

Av ansökan skall det framgå under vilken tid åtgärden önskas. Ansökan skall vidare innehålla sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Om den person som ansökan avser inte befinner sig i den ansökande staten, skall det också framgå av ansökan att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Ansökan skall prövas av åklagare. För beslutet om tekniskt bistånd tillämpas bestämmelserna i 27 kap. 18 § första stycket, 19 § första stycket, 20 § *andra* stycket, 21 § andra och tredje styckena samt 23 § rättegångsbalken.	Ansökan skall prövas av åklagare. För beslutet om tekniskt bistånd tillämpas bestämmelserna i 27 kap. 18 § första stycket, 19 § första stycket, 20 § *fjärde* stycket, 21 § andra och tredje styckena samt 23 § rättegångsbalken.
Om omedelbar överföring av *telemeddelanden* sker, får upptagning eller uppteckning inte göras i Sverige.	Om omedelbar överföring av *meddelanden* sker, får upptagning eller uppteckning inte göras i Sverige.

25 c §

Om en stat har begärt tekniskt bistånd enligt 25 b § men omedelbar överföring inte kan ske, skall åklagaren ge den ansö-	Om en stat har begärt tekniskt bistånd enligt 25 b § men omedelbar överföring inte kan ske, skall åklagaren ge den ansö-

kande staten tillfälle att få ansökan behandlad som en ansökan enligt 25 §. Prövningen av rättslig hjälp med *hemlig teleavlyssning* eller *hemlig teleövervakning* avser dock i detta fall någon som befinner sig i en annan stat. Om den person som åtgärden avser inte befinner sig i den ansökande staten, skall det av ansökan framgå att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

kande staten tillfälle att få ansökan behandlad som en ansökan enligt 25 §. Prövningen av rättslig hjälp med *avlyssning* eller *övervakning* avser dock i detta fall någon som befinner sig i en annan stat. Om den person som åtgärden avser inte befinner sig i den ansökande staten, skall det av ansökan framgå att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Rättslig hjälp och tekniskt bistånd i utlandet med *hemlig teleavlyssning* och *hemlig teleövervakning*

Rättslig hjälp och tekniskt bistånd i utlandet med *avlyssning* och *övervakning*

26 §

Åklagare får 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.

Om den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får rätten på begäran av svensk åklagare pröva frågan om att tillåta den *hemliga teleavlyssningen* eller *hemliga teleövervakningen* som ansökan enligt första stycket avser.

Åklagare får ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* av någon som befinner sig i en annan stat eller i Sverige.

Om den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får rätten på begäran av svensk åklagare pröva frågan om att tillåta den *avlyssning* eller *övervakning* som ansökan enligt första stycket avser.

Av ansökan enligt första stycket skall det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Om den andra staten kräver ett tillstånd enligt andra stycket, skall ansökan innehålla en bekräftelse på att ett sådant tillstånd har meddelats. Befinner sig den person som åt-

gärden avser inte i den stat där rättslig hjälp eller tekniskt bistånd söks, skall det av ansökan framgå att ett sådant tillstånd som avses i 26 c § har lämnats av den stat där personen finns.

Tillstånd till gränsöverskridande *hemlig teleavlyssning* och *hemlig teleövervakning*

Tillstånd till gränsöverskridande *avlyssning* och *övervakning*

Tillstånd i Sverige till gränsöverskridande *hemlig teleavlyssning* och *hemlig teleövervakning*

Tillstånd i Sverige till gränsöverskridande *avlyssning* och *övervakning*

26 a §

En stat som är medlem i Europeiska unionen eller Island eller Norge får ansöka om tillstånd till att, utan svenskt biträde, i en brottsutredning genomföra *hemlig teleavlyssning* eller *hemlig teleövervakning* av någon som befinner sig i Sverige. Ansökan handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett beslut om *hemlig teleavlyssning* eller *hemlig teleövervakning* har meddelats i den ansökande staten.

Åklagaren skall genast pröva om det finns förutsättningar för *hemlig teleavlyssning* eller *hemlig teleövervakning* och, om så är fallet, ansöka om rättens tillstånd till åtgärden.

En stat som är medlem i Europeiska unionen eller Island eller Norge får ansöka om tillstånd till att, utan svenskt biträde, i en brottsutredning genomföra *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* av någon som befinner sig i Sverige. Ansökan handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett beslut om *avlyssning* eller *övervakning* har meddelats i den ansökande staten.

Åklagaren skall genast pröva om det finns förutsättningar för *avlyssning* eller *övervakning* och, om så är fallet, ansöka om rättens tillstånd till åtgärden.

De förutsättningar som gäller enligt 27 kap. 18-22 §§ rättegångsbalken skall tillämpas vid tillståndsprövningen. Rätten skall även tillämpa motsvarande förfarande som anges i 27 kap. 26 och 28-30 §§ samma balk. Tingsrättens beslut får inte överklagas.

26 b §

Ett beslut enligt 26 a § skall meddelas inom 96 timmar från det att ansökan inkom eller, om det finns särskilda skäl, inom högst tolv dagar från ansökan.

Åklagaren skall genast underrätta den ansökande staten när ett beslut enligt 26 a § har meddelats. Om tillstånd vägras, skall underrättelsen ange att *teleavlyssningen* eller *teleövervakningen* inte får ske eller omedelbart skall upphöra. I sådant fall skall underrättelsen även ange att det material som tagits upp eller hämtats in inte får användas eller att det endast får användas på de villkor som åklagaren ställer.

Åklagaren skall genast underrätta den ansökande staten när ett beslut enligt 26 a § har meddelats. Om tillstånd vägras, skall underrättelsen ange att *avlyssningen* eller *övervakningen* inte får ske eller omedelbart skall upphöra. I sådant fall skall underrättelsen även ange att det material som tagits upp eller hämtats in inte får användas eller att det endast får användas på de villkor som åklagaren ställer.

Tillstånd från en annan stat till gränsöverskridande *hemlig teleavlyssning* och *hemlig teleövervakning*

Tillstånd från en annan stat till gränsöverskridande *avlyssning* och *övervakning*

26 c §

Har beslut om *hemlig teleavlyssning* eller *hemlig teleövervakning* i en brottsutredning meddelats i Sverige och befinner sig den person som beslutet avser i en annan stat som är medlem i Europeiska unionen eller i Island eller Norge, får *telemeddelanden eller uppgifter om telemeddelanden som befordras till eller från personen* avlyssnas eller övervakas i den andra staten, utan hjälp från denna stat, om

1. åtgärden får ske enligt en internationell överenskommelse som är bindande mellan Sverige och den andra staten, och

2. den andra staten lämnar

Har beslut om *avlyssning* eller *övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken* i en brottsutredning meddelats i Sverige och befinner sig den person som beslutet avser i en annan stat som är medlem i Europeiska unionen eller i Island eller Norge, får *meddelanden enligt de bestämmelserna* avlyssnas eller övervakas i den andra staten, utan hjälp från denna stat, om

1. åtgärden får ske enligt en internationell överenskommelse som är bindande mellan Sverige och den andra staten, och

2. den andra staten lämnar

tillstånd till åtgärden.

Ansökan om tillstånd görs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett svenskt beslut om *hemlig teleavlyssning* eller *hemlig teleövervakning* har meddelats.

Om beslut om *hemlig teleavlyssning* eller *hemlig teleövervakning* har meddelats i Sverige men avlyssningen eller övervakningen inte har påbörjats när det blir känt att den person som åtgärden avser befinner sig i en sådan främmande stat som anges i första stycket, skall tillstånd från den andra staten sökas innan avlyssningen eller övervakningen påbörjas. Har avlyssningen eller övervakningen redan påbörjats i Sverige och vill åklagaren att avlyssningen eller övervakningen skall fortsätta i den andra staten, skall han eller hon omedelbart ansöka om tillstånd hos den andra staten. Avlyssningen eller övervakningen får i ett sådant fall fortsätta där under den tid frågan om tillstånd prövas.

Vad som sägs i tredje stycket andra och tredje meningarna tillämpas på motsvarande sätt, om *teleavlyssningen* eller *teleövervakningen* genomförts med stöd av tillstånd i en främmande stat och det kommer fram att den person som åtgärden avser befinner sig i en annan stat än den som har meddelat tillstånd till åtgärden.

Ansökan om tillstånd görs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett svenskt beslut om *avlyssning* eller *övervakning* har meddelats.

Om beslut om *avlyssning* eller *övervakning* har meddelats i Sverige men avlyssningen eller övervakningen inte har påbörjats när det blir känt att den person som åtgärden avser befinner sig i en sådan främmande stat som anges i första stycket, skall tillstånd från den andra staten sökas innan avlyssningen eller övervakningen påbörjas. Har avlyssningen eller övervakningen redan påbörjats i Sverige och vill åklagaren att avlyssningen eller övervakningen skall fortsätta i den andra staten, skall han eller hon omedelbart ansöka om tillstånd hos den andra staten. Avlyssningen eller övervakningen får i ett sådant fall fortsätta där under den tid frågan om tillstånd prövas.

Vad som sägs i tredje stycket andra och tredje meningarna tillämpas på motsvarande sätt, om *avlyssningen* eller *övervakningen* genomförts med stöd av tillstånd i en främmande stat och det kommer fram att den person som åtgärden avser befinner sig i en annan stat än den som har meddelat tillståndet.

det.

Hemlig kameraövervakning	**Hemlig kameraövervakning *och hemlig dataavläsning***
Hemlig kameraövervakning *av* någon i Sverige	**Hemlig kameraövervakning *och hemlig dataavläsning rörande* någon i Sverige**
27 §	
En ansökan om hemlig kameraövervakning *av* någon som befinner sig i Sverige handläggs av åklagare. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd.	En ansökan om hemlig kameraövervakning *eller hemlig dataavläsning rörande* någon som befinner sig i Sverige handläggs av åklagare. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd.
Hemlig kameraövervakning *av* någon i utlandet	**Hemlig kameraövervakning *och hemlig dataavläsning rörande* någon i utlandet**
28 §	
Om hemlig kameraövervakning skall äga rum *av* någon som befinner sig i en annan stat och den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får tingsrätten på begäran av svensk åklagare besluta att tillåta kameraövervakningen.	Om hemlig kameraövervakning *eller hemlig dataavläsning* skall äga rum *rörande* någon som befinner sig i en annan stat och den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får tingsrätten på begäran av svensk åklagare besluta att tillåta kameraövervakningen *eller dataavläsningen*.

Denna lag träder i kraft den 1 januari 2007.

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

Härigenom föreskrivs att 6 kap. 8, 19 och 21-23 a §§ lagen (2003:389) om elektronisk kommunikation skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap. Integritetsskydd	
8 §[1]	
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 omfattas av beslut om *avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*, tekniskt bistånd med *avlyssning* eller med *övervakning*, 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.	
19 §	
En verksamhet skall bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av	*En verksamhet som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. rättegångsbalken eller tjänster inom ett sådant nät skall bedrivas så att beslut om avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken kan*
1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten	

[1] Nuvarande lydelse enligt förslag i prop. 2004/05:144

av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller

2. tjänster inom ett allmänt kommunikationsnät vilka består av

a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller

b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Innehållet i och uppgifter om avlyssnade eller övervakade *telemeddelanden* skall göras tillgängliga så att informationen enkelt kan tas om hand.

Med telemeddelande avses ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om frågor som avses i första och andra styckena samt får i enskilda fall medge undantag från kravet i första stycket.

verkställas och så att verkställandet inte röjs.

Innehållet i och uppgifter om avlyssnade eller övervakade *meddelanden* skall göras tillgängliga så att informationen enkelt kan tas om hand.

Regeringen eller den myndighet som regeringen bestämmer får i enskilda fall medge undantag från skyldigheten enligt första stycket och får meddela de förelägganden som behövs för efterlevnaden av skyldigheterna enligt första och andra styckena. Förelägganden får förenas med vite.

21 §[2]

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

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

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.

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

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 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,*

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till myndighet som skall ingripa mot brottet *och även i andra fall till polismyndighet eller åklagarmyndighet,*

3. uppgift som avses i 20 § första stycket 3 *och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller*

3. uppgift som avses i 20 § första stycket 3 *samt sådana uppgifter för lokalisering av ett tekniskt hjälpmedel som avses i*

[2] Nuvarande lydelse enligt förslag i prop. 2004/05:144

någon annan myndighet som skall ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,	*27 kap. 19 § rättegångsbalken till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa,*
4. uppgift som avses i 20 § första stycket 1 till en kronofogdemyndighet som behöver uppgiften i exekutiv verksamhet, om 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),	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), *och*
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.	*6*. 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.	Ersättning för att lämna ut uppgifter enligt första stycket *6* skall vara skälig med hänsyn till kostnaderna för utlämnandet.
	23 §
Den som i annat fall än som avses i 20 § första stycket och 21 § i radiomottagare har avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett radiobefordrat *telemeddelande* som inte är avsett för honom eller henne själv eller för allmänheten får inte obehörigen föra det vidare.	Den som i annat fall än som avses i 20 § första stycket och 21 § i radiomottagare har avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett radiobefordrat *meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken och* som inte är avsett för honom eller henne själv eller för allmänheten får inte obehörigen föra det vidare.
	23 a §[3]
Den som i verksamhet som anges i 19 § första stycket lämnar ut innehållet i och uppgifter om avlyssnade eller övervakade *telemeddelanden* har inte rätt till ersättning.	Den som i verksamhet som anges i 19 § första stycket lämnar ut innehållet i och uppgifter om avlyssnade eller övervakade *meddelanden* har inte rätt till ersättning.

Den som lämnar ut uppgifter enligt 22 § första stycket 2 och 3 har inte rätt till ersättning.

Regeringen får meddela föreskrifter om undantag från första och andra styckena.

Denna lag träder i kraft den 1 januari 2007.

---

[3] Nuvarande lydelse enligt förslag i lagrådsremiss den 3 mars 2005 Kostnadsansvar för hemlig teleavlyssning m.m.

10. Förslag till förordning om ändring i sekretessförordningen (1980:657)

Härigenom föreskrivs att 6 § sekretessförordningen (1980:657) och bilagan till den förordningen skall ha följande lydelse.

Föreskrifter med stöd av 15 kap. 2 § sekretesslagen

6 §

Nuvarande lydelse

Följande myndigheter skall i den utsträckning som framgår nedan inte tillämpa föreskriften i 15 kap. 2 § andra stycket sekretesslagen (1980:100).

Myndigheter	*Register*
allmänna domstolarna	diarier över ärenden om kvarhållande av försändelser på *befordringsanstalt* och om *hemlig teleavlyssning*, *hemlig teleövervakning och* hemlig kameraövervakning
---	---
polismyndigheterna	diarier över ärenden om kvarhållande av försändelse på *befordringsanstalt* och om *hemlig teleavlyssning*, *hemlig teleövervakning och* hemlig kameraövervakning
---	---
åklagarmyndigheterna	diarier över ärenden om kvarhållande av försändelse på *befordringsanstalt* och om *hemlig teleavlyssning*, *hemlig teleövervakning och* hemlig kameraövervakning samt diarier över förundersökningar som rör brott mot rikets säkerhet

Föreslagen lydelse

Följande myndigheter skall i den utsträckning som framgår nedan inte tillämpa föreskriften i 15 kap. 2 § andra stycket sekretesslagen (1980:100).

Myndigheter	*Register*
allmänna domstolarna	diarier över ärenden om kvarhållande av försändelser på *befordringsföretag* och om *avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*, hemlig kameraövervakning *och hemlig dataavläsning*
---	---
polismyndigheterna	diarier över ärenden om kvarhållande av försändelse på *befordringsföretag* och om *avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*, hemlig kameraövervakning *och hemlig dataavläsning*
---	---
åklagarmyndigheterna	diarier över ärenden om kvarhållande av försändelse på *befordringsföretag* och om *avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken*, hemlig kameraövervakning *och hemlig dataavläsning* samt diarier över förundersökningar som rör brott mot rikets säkerhet

Bilaga

Verksamheten består i	Särskilda begränsningar i sekretessen

Nuvarande lydelse

1. utredning, planering, tillståndsgivning, prisreglering, tillsyn och stödverksamhet hos regeringen i frågor som rör näringslivet	
----	
133. utredning, planering, tillståndsgivning och tillsyn enligt lagen (2004:656) om utsläpp av koldioxid	sekretessen gäller inte beslut i ärenden

Föreslagen lydelse

1. utredning, planering, tillståndsgivning, prisreglering, tillsyn och stödverksamhet hos regeringen i frågor som rör näringslivet	
----	
133. utredning, planering, tillståndsgivning och tillsyn enligt lagen (2004:656) om utsläpp av koldioxid	sekretessen gäller inte beslut i ärenden
134. Rikspolisstyrelsens prövning av frågor enligt 36 § förordningen (2003:396) om elektronisk kommunikation	

Denna förordning träder i kraft den 1 januari 2007.

11. Förslag till förordning om ändring i polisförordningen (1998:1558)

Härigenom föreskrivs att 3 kap. 8 § polisförordningen (1998:1558) skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap. Polismyndighetens uppgifter	
8 §	
Länspolismästare, biträdande länspolismästare, polismästare, polisöverintendenter, polisintendenter eller polissekreterare får fatta beslut	
---	---
20. om att göra en anmälan som rör utvisning enligt 2 § lagen (1991:572) om särskild utlänningskontroll, om förvar enligt 8 § första stycket samma lag, om husrannsakan, kroppsvisitation m.m. enligt 19 § samma lag eller om att framställa yrkande om tillstånd till *hemlig teleavlyssning* m.m. enligt 21 § andra stycket samma lag,	20. om att göra en anmälan som rör utvisning enligt 2 § lagen (1991:572) om särskild utlänningskontroll, om förvar enligt 8 § första stycket samma lag, om husrannsakan, kroppsvisitation m.m. enligt 19 § samma lag eller om att framställa yrkande om tillstånd till *avlyssning* m.m. enligt 21 § andra stycket samma lag,
---	---
Polismyndigheten får uppdra åt en annan anställd än som anges i första stycket att fatta beslut i ärenden som anges där, om den anställde har den kompetens, utbildning och erfarenhet som behövs.	

Denna förordning träder i kraft den 1 januari 2007.

12. Förslag till förordning om ändring i förordningen (2000:704) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs att 7 § förordningen (2000:704) om internationell rättslig hjälp i brottmål skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 §
Följande kostnader skall återkrävas av den ansökande staten:	
---	---
4. *hemlig teleavlyssning*: myndighets utlägg för *teleoperatörs* kostnader för verkställandet av *hemlig teleavlyssning*.	4. *avlyssning enligt 27 kap. 18 § rättegångsbalken*: myndighets utlägg för *operatörs* kostnader för verkställandet av *avlyssning*.

Denna förordning träder i kraft den 1 januari 2007.

13. Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

Härigenom föreskrivs att 36 § förordningen (2003:396) om elektronisk kommunikation skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	36 §
Post- och telestyrelsen får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen meddela de verkställighetsföreskrifter som behövs för hemlig teleavlyssning och hemlig teleövervakning enligt 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation samt får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från krav enligt 6 kap. 19 § första stycket samma lag.	*Rikspolisstyrelsen får medge undantag och meddela föreläggande enligt 6 kap. 19 § tredje stycket lagen (2003:389) om elektronisk kommunikation.* *I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande hos allmän förvaltningsdomstol.*

Denna förordning träder i kraft den 1 januari 2007.

1 Allmänt

1.1 Vårt uppdrag i stort

Rättsväsendet har under senare år genomgått stora reformer. Reformeringen har avsett både den inre och den yttre organisationen. Även regelverk, arbetsmetoder och annat har förändrats.

En förutsättning för ett väl fungerande rättsväsende är att myndigheterna är ändamålsenligt organiserade, har en fungerande administration, är lokaliserade på ett rationellt sätt och har ett väl utformat regelverk i form av lagar och andra författningar till sin hjälp. Ett väl fungerande rättsväsende förutsätter också att rättsväsendet ges tillräckliga resurser. Därutöver krävs att det inom myndigheterna finns en generellt sett hög kompetens inom respektive ansvarsområde. Rättsväsendet skall dessutom kunna ge en god service till enskilda. Med god service avses bl.a. en effektiv och snabb handläggning av mål och ärenden, en hög juridisk kvalitet eller rättssäkerhet och ett gott bemötande.

Vi har i uppdrag att undersöka möjligheterna att än mer öka effektiviteten och kvaliteten i rättsväsendets arbete. Det finns två ledstjärnor i det arbetet.

Den ena ledstjärnan är rättskedjeperspektivet. Det innebär att vi skall verka för att utvecklingen inom rättsväsendet sker samordnat och utifrån ett helhetsperspektiv på verksamheterna. Detta skall ske med respekt för den grundläggande rollfördelningen mellan rättsväsendets myndigheter.

Den andra ledstjärnan är medborgarintresset. Det innebär att det alltid är nyttan för den enskilde medborgaren av tilltänkta förändringar och reformer som skall stå i fokus.

Vi har enligt våra ursprungliga direktiv (Dir. 2000:90, se *bilaga 1*) fyra särskilt angivna huvuduppgifter. Dessa är att undersöka möjligheterna att förkorta genomströmningstiderna i brottmål, att

överväga hur den brottsutredande verksamheten ytterligare kan förbättras, att se över frågan om utbildning, kompetensutveckling och personalrörlighet inom rättsväsendet och att behandla övergripande frågor om lokaliseringen av rättsväsendets myndigheter. Våra överväganden bör enligt direktiven kunna leda till förslag som kan komma att omfatta allt från författningsändringar till ändringar av såväl administrativ som organisatorisk karaktär.

1.2 Våra tidigare överväganden

Vi har hittills lagt fram sex delbetänkanden. I det första, Snabbare lagföring 1 – Några förslag till förenklingar (SOU 2001:59), föreslog vi ett huvudalternativ för snabb handläggning av brottmål. Förslagen innebar att åklagares behörighet att utfärda stämning och kallelse till huvudförhandling skulle utvidgas. De bestämmelser i rättegångsbalken som reglerar dessa frågor skulle enligt vårt förslag inte längre betraktas som undantagsregler. Vi föreslog också att åklagare skulle få möjlighet att besluta om viss personutredning. Sådana beslut skulle enligt förslagen fattas redan under förundersökningen. Författningsändringarna i anledning av våra förslag i betänkandet trädde i kraft den 1 juli 2002 (prop. 2001/02:147, bet. 2001/02:JuU24, SFS 2002:440 och 2002:441).

I vårt andra betänkande, Snabbare lagföring 2 – Förenklad brottsutredning (SOU 2001:93), var förslagen koncentrerade till frågan om att åstadkomma förbättringar av den brottsutredande verksamheten, bl.a. genom ett utvidgat användningsområde för förenklad brottsutredning enligt 23 kap. 22 § rättegångsbalken (RB). Förslagen innebar på samma sätt som vårt huvudalternativ för snabb handläggning även ett sätt att åstadkomma en snabbare genomströmning i hela landet i brottmål. Regeringen har bedömt att våra förslag inte bör genomföras annat än i ett visst mindre avseende, nämligen så att beslag enligt 27 kap. RB får användas inom ramen för det förenklade brottsutredningsförfarandet (prop. 2003/04:89, bet. 2003/04:JuU26). Författningsändringarna i den delen trädde i kraft den 1 juli 2004 (SFS 2004:504).

Genom tilläggsdirektiv i juni 2001 (Dir. 2001:61) fick vi i uppdrag att undersöka möjligheterna att med bibehållen rättssäkerhet förenkla utredningen och lagföringen av i första hand butikssnatterier. Vi redovisade förslagen i vårt tredje betänkande, Snabbare lagföring 3 – Snatteribrott (SOU 2002:44). Förslagen innebar bl.a. att en försöksverksamhet skulle inledas med förenklad handläggning

av snatteribrott och att föreläggande av ordningsbot skulle få utfärdas för vissa sådana brott. Regeringen överlämnade i januari 2005 en remiss till Lagrådet rörande den förenklade handläggningsformen men gick inte vidare med frågan om en utvidgning av ordningsbotsinstitutet. Efter Lagrådets yttrande har det enligt uppgift fattats beslut om att någon proposition inte skall läggas fram.

Även i vårt fjärde betänkande, Snabbare lagföring 4 – Ett snabbförfarande för brottmål (SOU 2002:45), var förslagen huvudsakligen inriktade på att åstadkomma en förkortning av genomströmningstiderna i brottmål. I betänkandet behandlade vi vårt uppdrag att överväga ett permanent snabbförfarande för brottmål. Med anledning av bl.a. de klara effektivitets-, kvalitets- och rättssäkerhetsvinster som vi såg, bedömde vi att ett sådant skulle kunna införas i vissa större städer och att det fanns möjlighet att reducera tiden från polismyndighetens kännedom om brottet till huvudförhandling till omkring fem veckor. En tvåårig försöksverksamhet med snabbare handläggning av brottmål enligt vårt förslag pågår vid Stockholms tingsrätt fram till och med juni 2006 (prop. 2003/04:89, bet. 2003/04:JuU26, SFS 2004:505 och 2004:506).

Som en del i vårt uppdrag att överväga om det behövs författningsändringar för att förbättra möjligheten att förhindra, avslöja, utreda eller lagföra brott, föreslog vi i vårt femte betänkande, Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74), bl.a. en lagreglering av vissa av de brottsbekämpande myndigheternas arbetsmetoder och en utvidgning av möjligheterna att använda strafföreläggande. Förslagen bereds för närvarande i Justitiedepartementet. Regeringen har dock i en lagrådsremiss från den 3 mars 2005, i enlighet med vårt förslag i betänkandet, föreslagit att operatörerna inte skall ha rätt till ersättning vid bl.a. de enskilda verkställigheterna av beslut om hemlig teleavlyssning och hemlig teleövervakning.

Våra ursprungliga direktiv anger ingen sluttidpunkt för uppdraget. Däremot skulle vi enligt direktiven senast före utgången av år 2003 redovisa det vid det tillfället aktuella läget inom rättsväsendet för de frågor som ankommer på oss och en plan för det fortsatta arbetet. Det gjorde vi i vårt sjätte betänkande, Läget i rättsväsendet och förslag till fortsatta reformer inom brottsutredningsverksamheten m.m. (SOU 2003:114). I betänkandet behandlade vi dessutom andra frågor som framför allt rörde två av våra särskilt angivna huvuduppgifter, nämligen utbildning, rekrytering m.m. och vissa frågor om lokalisering av rättsväsendets myndigheter. Frågorna bereds för närvarande i Justitiedepartementet.

För närmare uppgifter om innebörden av våra tidigare förslag hänvisar vi till respektive betänkande. Dessutom hänvisar vi till det senaste betänkandet för närmare uppgift om hur vårt arbete bedrevs fram till utgången av år 2003.

1.3 Vad behandlas i detta betänkande?

En av våra huvuduppgifter är att överväga hur den brottsutredande verksamheten ytterligare kan förbättras. Vi har behandlat den frågan i några av de tidigare betänkandena. I uppgiften ingår att överväga frågor om de brottsbekämpande myndigheternas arbetsmetoder, inklusive frågor om tvångsmedel och möjligheten att utnyttja modern teknik i arbetet.

I november 2003 beslutade regeringen om tilläggsdirektiv för vårt uppdrag (Dir. 2003:145, se *bilaga 2*). Tilläggsdirektiven tar upp dels en översyn av uppgifts- och ansvarsfördelningen mellan polis och åklagare, dels en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I detta betänkande har vi valt att ta upp frågorna som rör elektronisk kommunikation och vissa närliggande frågor och återkommer till övriga frågor i ett senare betänkande.

Vi vill särskilt framhålla att många av förslagen i betänkandet kan leda till stora effektivitetsvinster och är sinsemellan självständiga, dvs. de går att genomföra separat även om inte andra förslag genomförs.

1.4 Utredningsarbetet

I enlighet med våra tilläggsdirektiv har vi i arbetet med de frågor som behandlas i detta betänkande haft tillgång till en referensgrupp med representanter för de sju riksdagspartierna. I referensgruppen har det funnits stor enighet kring huvuddelen av de förslag som presenteras i betänkandet. I några frågor har det dock funnits olika uppfattningar. När så har varit fallet redovisas det särskilt i det följande (se avsnitten 4.3, 9.4.3, 9.4.4, 9.4.9 och 10 rörande dels interimistisk beslutanderätt vid hemlig teleövervakning, dels underrättelseskyldighet i efterhand, den s.k. straffvärdeprincipen och rätten till tillträde vid hemlig dataavläsning, dels kostnadsansvaret).

Vårt arbete skall enligt de ursprungliga direktiven bedrivas i nära samverkan med berörda myndigheter inom rättsväsendet. Vi har under arbetet inhämtat synpunkter från Åklagarmyndigheten i Stockholm, Säkerhetspolisen, Rikskriminalpolisen, Polismyndigheterna i Stockholms och Västmanlands län och Tullverket. Vi har också fört diskussioner med operatörer rörande de s.k. anpassnings- och bevarandeskyldigheterna. Dessutom har vi haft kontakt med den nationella narkotikapolitiska samordningen Mobilisering mot narkotika (S 2002:03).

Sverige undertecknade i november 2001 Europarådets konvention om IT-relaterad brottslighet (den s.k. Cyber Crime-konventionen) och i januari 2003 ett tilläggsprotokoll till konventionen. En departementspromemoria med bl.a. de förslag till lagändringar som krävs för en anpassning till dessa har samtidigt med vårt arbete utarbetats inom Justitiedepartementet och har nyligen skickats ut på remiss, Brott och brottsutredning i IT-miljö (Ds 2005:6). I det sammanhanget förekommer det frågor som berörs även i detta betänkande. Med anledning av Justitiedepartementets pågående arbete har vi dock inte analyserat innehållet i konventionen i vårt arbete.

2 Elektronisk kommunikation, hemliga tvångsmedel och personlig integritet

2.1 Vårt uppdrag rörande elektronisk kommunikation

Vid utredning av brott är uppgifter kopplade till elektronisk kommunikation ofta av helt central betydelse. Utan sådana uppgifter kan det många gånger vara omöjligt att göra framsteg i utredningsarbetet. Genom uppgifterna kan sakförhållanden klarläggas, misstankar stärkas och gärningsmän identifieras, men det kan också hända att uppgifterna kan fria någon från misstankar. Den sistnämnda aspekten är mycket viktig att komma ihåg i sammanhanget.

Såväl den tekniska utvecklingen som lagstiftningen på området har inneburit problem för de brottsutredande myndigheterna med att få tillgång till uppgifter om elektronisk kommunikation i utredningar. Exempelvis har den distinktion som görs i lagstiftningen mellan framtida uppgifter, som hämtas in med stöd av rättegångsbalken, och historiska uppgifter, som de brottsutredande myndigheterna får bl.a. med stöd av lagen (2003:389) om elektronisk kommunikation (LEK), framstått som i viss mån teoretisk och föråldrad med hänsyn till dagens teknik, där exempelvis skillnaden mellan realtid och dåtid kan vara svår att urskilja.

Vårt uppdrag rörande elektronisk kommunikation innebär att vi skall göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I detta ingår bl.a. att överväga en anpassning och modernisering av rättegångsbalkens terminologi, att göra en översyn av vilka verksamheter som bör omfattas av den s.k. anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning, att överväga vilka typer av trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndig-

heterna och om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna. Vi bör enligt våra direktiv samtidigt analysera om utökade möjligheter för de brottsbekämpande myndigheterna medför ökade kostnader och hur dessa kostnader i så fall skall finansieras samt göra en avvägning mellan den nytta som de utökade möjligheterna ger i förhållande till de kostnadsökningar som kan uppstå. Regeringen anger också i direktiven att en utgångspunkt för uppdraget skall vara att inte fler uppgifter bevaras för brottsbekämpande ändamål eller under längre tid än vad som är nödvändigt. En annan utgångspunkt skall vara att personuppgifter som bevaras inte skall användas för något annat ändamål än brottsbekämpning. Enligt regeringen bör målsättningen för arbetet vara att skapa en enhetlig reglering som, särskilt med hänsyn till den snabba tekniska utvecklingen, kan stå sig över tiden (Dir. 2003:145, se *bilaga 2*).

I detta avsnitt vill vi ge en kortare beskrivning av innebörden av begrepp som elektronisk kommunikation och telemeddelande, av bestämmelser rörande vissa hemliga tvångsmedel, av den rättsliga möjligheten för de brottsutredande myndigheterna att få uppgifter om elektronisk kommunikation enligt bl.a. lagen om elektronisk kommunikation, av regler i bl.a. regeringsformen om personlig integritet och av den parlamentariska kontroll som utövas över tillämpningen av vissa bestämmelser om hemlig teleavlyssning och hemlig teleövervakning.

Det är Säkerhetspolisen som inom polisen har huvudansvaret för tekniska och administrativa frågor som rör hemlig teleavlyssning och hemlig teleövervakning. Det gäller t.ex. utveckling av teknik samt inköp, installation och teknisk drift av utrustning liksom slutande av avtal rörande verkställighet och kontakterna i övrigt med operatörerna (RPSFS 1999:9, FAP 171-1). Varje begäran om verkställighet av hemlig teleavlyssning och hemlig teleövervakning skickas från Säkerhetspolisen till den aktuella operatören. Den enhet vid Säkerhetspolisen som handhar frågor om dessa tvångsmedel har personal i tjänst dygnet runt hela året. Därmed finns det förutsättningar för att hantera brådskande fall. Sedan har varje polismyndighet utrustning och personal för att ta hand om de uppgifter från operatörerna som hör till respektive ärende. I de ärenden där Tullverket driver förundersökning verkställs ännu beslut om tvångsmedlen via polisens tekniska utrustning.

I 1 kap. 7 § LEK definieras begreppet operatör som den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. Beteckningen operatör används i detta

betänkande i en något vidare betydelse (jfr bestämmelsen om tystnadsplikt i 6 kap. 20 § LEK som träffar alla som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst).

2.2 Elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation samt utsändningar till allmänheten genom radio och TV. Utvecklingen går tydligt mot att dessa tre sektorer gradvis växer samman. Denna utveckling brukar kallas konvergens. Den sker inom infrastruktur-, tjänste- och utrustningsområdena och har blivit möjlig framför allt genom den s.k. digitaliseringen och den tekniska standardiseringen genom framväxten av Internet. Utvecklingen på området för elektronisk kommunikation innebär att olika infrastrukturer och tekniker för överföring av kommunikation och tjänster som tidigare kunde tillhandahållas genom endast en teknik nu kan tillhandahållas genom flera. Det gör att det exempelvis är möjligt att telefonera via datorn, använda Internet via TV:n och se på TV i mobiltelefonen (jfr prop. 2002:03:110 s. 58).

Via elektroniska kommunikationsnät befordras ständigt en ofantlig mängd information. Där förmedlas bl.a. telefonsamtal, telefaxmeddelanden, elektronisk post, datakommunikation och annan kommunikation som innehåller meddelanden, dvs. information i form av text, bild eller ljud.

När det gäller s.k. *fast telefoni* har alla företag och hushåll som så vill i dag tillgång till analog taltelefoni. Även digital anslutning i form av ISDN (Integrated Services Digital Network) används för telefoni. Enligt uppgifter från Post- och telestyrelsen (PTS) finns det omkring 5 800 000 fasta telefoniabonnemang i Sverige. Antalet operatörer inom fast telefoni till privatkunder är ungefär 35 stycken (prop. 2002/03:110 s. 60).

Mobiltelefonnäten finns spridda över i stort sett hela landet. De tillstånd som mobiloperatörer behöver för att bedriva sin verksamhet innehåller även krav på hur täckningen skall se ut. Det finns på marknaden fortfarande både analoga system som NMT (Nordisk Mobil Telefoni) och digitala som GSM (Global Service for Mobile Communications). Dagens mobiltelefoni är fortfarande till stor del en taltelefonitjänst. Nya tjänster och tekniker som SMS (Short Message Service) och WAP (Wireless Application Protocol) med-

ger dock överföring av text och webbliknande innehåll. GSM-näten har sedan sitt införande utvecklats tekniskt med bl.a. GPRS-teknik (General Packet Radio Service) och fått högre överföringskapacitet, vilket möjliggör nya tillämpningar och tjänster med större informationsinnehåll. Den tredje generationens mobiltelesystem, UMTS (Universal Mobile Telecommunications System), innebär att överföringskapaciteten ökar ytterligare. Sverige har en i internationell jämförelse mycket hög ”mobiltelepenetration”. Enligt PTS rapport Hur fungerar telefoni och Internet för användarna (år 2002) använde 87 procent av Sveriges befolkning mellan 16 och 75 år mobiltelefon i september/oktober 2002. Konkurrenssituationen på mobilteleområdet skiljer sig från den på området för fast telefoni. För NMT finns endast en operatör, nämligen TeliaSonera. På GSM-marknaden finns för närvarande tre stora operatörer som också äger nät. Det är TeliaSonera, Tele2 Sverige AB (Tele2) och Vodafone Sverige AB (Vodafone), med en sammanlagd marknadsandel på 99 procent år 2001 både när det gäller omsättning och abonnemang. PTS har under år 2002 delat ut ett fjärde GSM-tillstånd till Swefour AB. Utöver Tele2 och Vodafone har två nya operatörer, Orange Sverige AB och Hi3G Access AB, fått tillstånd för UMTS. Tillståndsvillkoren för UMTS innehåller krav på utbyggnad av nät men möjliggör även delad infrastruktur till viss grad (prop. 2002/03:110 s. 60 ff.).

Beträffande *informationsteknik och datakommunikation* kan följande nämnas. De nationella stomnäten, dvs. rikstäckande allmänt tillgängliga nät som förbinder nationella noder och huvudnoder i landets olika delar med varandra, är främst baserade på optiska fiberkablar men även till en viss del radiolänk. De största ägarna av nationella stomnät är TeliaSonera, Utfors AB/Telenor Business Solutions AB, Affärsverket svenska kraftnät, Teracom AB och Banverket. Det mest omfattande nationella stomnätet innehas av TeliaSonera, som når alla kommuner. Ortssammanbindande nät förbinder olika orter med varandra samt med huvudnoderna i nätet. Områdesnäten är spridningsnät som sammanbinder fastighetsnäten i en ort eller ett geografiskt avgränsat område med det ortssammanbindande nätet. I områdesnät kan även inräknas de nät som ofta benämns accessnät. De ortssammanbindande näten och områdesnäten ägs till en del av kommunala bolag och kommuner. En möjlighet till trådlös access med hög överföringskapacitet är fast yttäckande radioaccess som används för sändningar av datakommunikation, t.ex. LMDS (Local Multipoint Distribution Service). Nationella tillstånd för denna teknik innehas av TeliaSonera, Quad-

racom Wireless AB, Vodafone samt Broadnet AS. En fördelning av tillstånd för fast yttäckande radioaccess på regional nivå har också utförts. Även elnäten kan användas för elektronisk kommunikation, s.k. Power Line Communication (PLC). Därutöver används också uppgraderade telefonnät, satellit samt marknätet för digital-TV för datakommunikation. Den svenska marknaden för Internetaccess är fragmenterad. En bedömning av PTS är att det finns ett hundratal Internetoperatörer som tillhandahåller anslutning till Internet till slutkund. Leverantörerna är många och ofta små, och inriktar sig i hög grad på olika nischer och delsegment av marknaden där de erbjuder olika typer av anslutningsformer. De flesta erbjuder traditionella uppringda anslutningar över det vanliga metallbaserade accessnätet. Även kabel-TV-operatörer erbjuder anslutning till Internet via sina kabelnät, medan andra erbjuder anslutning till Internet med hög överföringskapacitet via fastighetsnät – LAN (Local Area Network) – framför allt i flerbostadshus. I juni 2002 fanns det strax över tre miljoner kunder med anslutning till Internet i Sverige. Det är Internet som i första hand driver fram nya typer av tjänster och skapar förutsättningar för ytterligare konvergens inom området. Det är främst användningen av telefon och TV som har minskat som en följd av den ökade Internetanvändningen (prop. 2002/03:110 s. 61 ff.).

2.3 Telemeddelande

Begreppet telemeddelande definieras i 6 kap. 19 § tredje stycket LEK, såsom ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskild anordnad ledare. I stort sett all information som går genom ett s.k. elektroniskt kommunikationsnät utgör telemeddelanden enligt den definitionen, vilken får anses vägledande för bl.a. bestämmelserna i 27 kap. RB om hemlig teleavlyssning och hemlig teleövervakning (se vidare avsnitt 2.4.1 och 2.4.2).

När telemeddelanden befordras genom nät, t.ex. mellan två datorer, sker överföringen på några sekunder. Signalerna kan fångas upp, alltså avlyssnas, på vägen till mottagaren. Den som har avlyssnat signalerna kan därefter få ut dessa i form av t.ex. text. Telemeddelanden som inte innefattar samtal, t.ex. elektronisk post, kan avlyssnas på samma sätt som ett telefonsamtal. Detsamma gäller överföringar av datafiler med hjälp av t.ex. FTP (File Transfer Pro-

tocol) liksom överföringar från hemsidor, nyhetsgrupper och chatkanaler, vilket alltså är telemeddelanden som kan avlyssnas med hjälp av hemlig teleavlyssning eller ge andra uppgifter till de brottsutredande myndigheterna vid hemlig teleövervakning.

Det finns flera olika tjänster som lagrar telemeddelanden. Som exempel kan nämnas att det finns telefonsvarartjänster som innebär att den enskilde abonnenten får en röstbrevlåda kopplad till abonnemanget. Mottagaren tar del av meddelandena i röstbrevlådan genom att slå ett visst nummer på den telefon som tjänsten är kopplad till. För att ta del av meddelanden från en annan telefon, krävs ofta tillgång till en personlig kod. Meddelandena lagras på en server hos operatören och finns ibland tillgängliga genom tjänsten under ett visst antal dagar, oavsett om mottagaren har lyssnat på meddelandet eller inte.

Motsvarande tjänster finns för elektronisk post. Ett exempel på en sådan tjänst är att kunden har en eller flera s.k. brevlådor med en e-postadress hos en Internetoperatör. Meddelanden lagras då i första hand på operatörens server. Ett annat system innebär att elektronisk post går direkt till kundens egen s.k. mail-server i kundens eget nätverk. Meddelandena mellanlagras då inte hos operatören.

Ett annat sätt att förmedla och lagra telemeddelanden är att textmeddelanden (t.ex. SMS) sänds till mobiltelefoner. Textmeddelanden befordras på i stort sett samma sätt som muntliga meddelanden. Till skillnad från muntliga meddelanden lagras ett mottaget textmeddelande i telefonen. Meddelandena kan lagras antingen direkt i telefonen eller på det s.k. SIM-kortet.

2.4 Rättegångsbalken

2.4.1 Hemlig teleavlyssning

Före andra världskriget saknades regler om telefonavlyssning i brottsutredande syfte. Det antogs att det krävdes Kungl. Majt:s beslut i varje särskilt fall för att avlyssning skulle kunna genomföras. Förslag till regler om telefonavlyssning i samband med brottsutredning lades första gången fram i betänkandet Förslag till rättegångsbalk (SOU 1938:43 och 44, se prop. 1975/76:202 s. 85).

Redan före andra världskriget infördes dock regler om telefonavlyssning i två av de lagar som föranleddes av kriget, nämligen la-

gen (1939:724) om särskilda tvångsmedel vid utredning rörande brott som avses i 8 eller 19 kap. strafflagen m.m. och lagen (1940:3) om vissa tvångsmedel vid krig eller krigsfara m.m. Båda lagarna fick provisorisk karaktär och skulle gälla till utgången av mars 1941. Giltighetstiden för 1939 års lag förlänges inte medan däremot 1940 års lag successivt förlängdes och upphörde att gälla med utgången av juni 1945.

Mellan den 1 juli 1945, då 1940 års lag upphörde att gälla och den 1 januari 1948, då rättegångsbalken trädde i kraft, saknades bestämmelser om telefonavlyssning i svensk lag.

Det utrikespolitiska läget ansågs 1952 påkalla utvidgade möjligheter till bl.a. telefonavlyssning vid vissa brott mot rikets yttre och inre säkerhet. Efter mönster från 1939 och 1940 års lagar tillkom en ny provisorisk lag, lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål (benämnd 1952 års tvångsmedelslag). Lagen har förlängts och gäller enligt det senaste beslutet till utgången av år 2007.

De nuvarande huvudsakliga bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning finns i 27 kap. 18-30 §§ RB, som senast ändrades den 1 oktober 2004. Hemlig teleavlyssning innebär att telemeddelanden som befordras eller har befordrats till eller från ett visst telefonnummer, en kod eller en annan teleadress avlyssnas eller spelas in i hemlighet genom ett tekniskt hjälpmedel. Bestämmelser som för vissa fall ger rätt att använda hemlig teleavlyssning finns också i 1952 års tvångsmedelslag, lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och lagen (1991:572) om särskild utlänningskontroll (se vidare avsnitt 2.7).

Med telemeddelande avses i rättegångsbalken och i övriga nämnda lagar detsamma som i 6 kap. 19 § tredje stycket LEK, nämligen ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare. Exempel på telemeddelanden som får avlyssnas enligt bestämmelserna om hemlig teleavlyssning är telefonsamtal, telefax, elektronisk post och annan datakommunikation.

För att ett telemeddelande skall få avlyssnas krävs att meddelandet befordras eller har befordrats till eller från ett telefonnummer, en kod eller annan teleadress. Med teleadress avses t.ex. ett abonnemang, en enskild anknytning, adressen för elektronisk post, en kod eller någon annan motsvarande tillförlitlig identifieringsmetod. Elektronisk post får alltså avlyssnas under samma förutsättningar

som telefonsamtal, dvs. innehållet i meddelandet görs tillgängligt för de brottsutredande myndigheterna. I lagstiftningen fanns tidigare begreppet teleanläggning. I samband med att det ersattes av begreppet teleadress uttalade regeringen följande (prop. 1994/95:227 s. 18).

> Utvecklingen på teleområdet har inneburit att de beskrivna närmast fysiska avgränsningarna som bygger på teleanläggningar och telenät inte kan tillämpas konsekvent. Ett samband mellan den misstänkte och viss plats, ledning och telefon var tidigare en naturlig och närmast självklar utgångspunkt för en tydlig avgränsning av tvångsmedlen på teleområdet. Nya IT-baserade rutiner har emellertid fört med sig att förutsättningarna förändrats. Numera kan det vanligtvis inte förutsägas vilken typ av teleanläggning – telefax, telefon, modem, etc. – som ansluts till en viss telelinje. Kombinationer har blivit vanliga, t.ex. att telefon, telefax och telefonsvarare ansluts till samma abonnentledning. Vidare har sambandet mellan abonnentnummer och abonnentledning delvis suddats ut. Telemeddelanden kan t.ex. kopplas vidare och flyttas med. Sådana omdirigeringar av telemeddelanden sker redan i teleoperatörens växel så att telemeddelandena aldrig når ursprungligen avsedd abonnentledning. Andra exempel på frikoppling från viss teleanläggning kan hämtas från mobil telefoni och moderna företagsväxlar. Alla telemeddelanden till ett visst mobilteleabonnemang styrs direkt i teleoperatörens växel till den radiosändare inom vilkens räckvidd mottagaren befinner sig. Är abonnemanget GSM-baserat kan valfri telefon användas under förutsättning att den har försetts med mottagarens personliga kort. På motsvarande sätt ger vissa televäxlar möjligheter att – efter en indikation via t.ex. personsökare – ta emot ett samtal vid den fysiska anknytning där mottagaren för tillfället befinner sig. Mottagaren anger en kod genom vilken meddelandet dirigeras till den aktuella telefonapparaten. Ett annat exempel där t.ex. telefonapparater inte fysiskt knyts till viss plats är televäxlar som nu börjat marknadsföras vilka knyter telefonapparaten till televäxeln via radiokommunikation.
>
> En fysisk gränsdragning i de nu beskrivna fallen medför närmast slumpvis att vissa, men inte andra, av de telemeddelanden som befordras via televäxeln till eller från den misstänkte kan tas upp. Traditionella gränser har i allt högre grad

suddats ut och vedertagna rutiner för att knyta telemeddelanden till viss teleanläggning har ersatts av flexibla IT-baserade rutiner som inte är beroende av vilken telefonapparat, telelinje eller annan teleanläggning som används i det enskilda fallet. Följden blir – som på andra områden där IT-rutiner genomförs och de traditionella, närmast fysiska avgränsningarna faller bort – att kvar finns endast sådana avgränsningar som följer av ändamål, funktioner och tekniska strukturer som byggs upp.

Tillstånd till hemlig teleavlyssning kan 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 kan också ges vid förundersökning angående annat brott, om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år (se 27 kap. 18 § andra stycket RB och prop. 2002/03:74 s. 31 ff.).

Beslutet får avse 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. Exempel på det sistnämnda kan beroende på omständigheterna vara en teleadress som innehas av en sambo till en misstänkt, en teleadress på den misstänktes arbetsplats eller teleadressen till en telefonkiosk som den misstänkte regelbundet använder.

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 (27 kap. 20 § första stycket RB).

Beslutet skall avse telemeddelanden som utväxlas under en i beslutet viss angiven tid.

När åklagarens ansökan om tillstånd till hemlig teleavlyssning har kommit in till rätten, skall rätten så snart som möjligt utse ett offentligt ombud i ärendet. Det offentliga ombudet, som skall vara eller ha varit advokat eller ha varit ordinarie domare, har till uppgift att bevaka enskildas integritetsintressen i ärendet (27 kap. 26-30 §§ RB). Det offentliga ombudet skall lyfta fram alla aspekter, t.ex. skydd för tredje mans integritet.

2.4.2 Hemlig teleövervakning

Tvångsmedlet hemlig teleövervakning (27 kap. 19-25 §§ RB) innebär att det i hemlighet hämtas in uppgifter om telemeddelanden som befordras eller har befordrats till eller från 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. Hemlig teleövervakning 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 (27 kap. 20 § första stycket RB). Uppgifter om innehållet i telemeddelanden (avlyssning) omfattas inte av hemlig teleövervakning.

Liksom vid hemlig teleavlyssning finns bestämmelser som för vissa fall ger rätt att använda hemlig teleövervakning i 1952 års tvångsmedelslag, lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och lagen om särskild utlänningskontroll (se vidare avsnitt 2.7).

Om hemlig teleövervakning avser ett telefonnummer kan en brottsutredande myndighet med hjälp av tvångsmedlet 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. Ett beslut om 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 då kommunikationen 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 (s.k. lokaliseringsuppgifter).

Tillstånd till hemlig teleövervakning får meddelas av rätten vid förundersökning om brott för vilket det inte är föreskrivet lindri-

gare straff än fängelse i sex månader, brott enligt 4 kap. 9 c § brottsbalken (BrB) (dataintrång), 16 kap. 10 a § BrB (barnpornografibrott som inte är att anse som ringa), 1 § narkotikastrafflagen (1968:64, narkotikabrott) eller brott enligt 6 § första stycket lagen (2000:1225) om straff för smuggling (narkotikasmuggling). Vidare får tillstånd meddelas vid misstanke om försök, förberedelse eller stämpling till nämnda brott (27 kap. 19 § andra stycket RB).

2.4.3 Förutsättningar gemensamma för hemlig teleavlyssning och hemlig teleövervakning

Hemlig teleavlyssning och hemlig teleövervakning får användas endast i förundersökning där någon är skäligen misstänkt för ett visst brott och åtgärden är av synnerlig vikt för utredningen om brottet (27 kap. 20 § första stycket RB). Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen skall ge avgörande bevisning som omedelbart kan leda till en fällande dom. Synnerlig vikt för utredningen inrymmer däremot ett kvalitetskrav beträffande de upplysningar som avlyssningen kan ge. Det får inte vara fråga om obetydliga detaljer som man både kan ha och mista. Uttrycket omfattar även ett krav på att utredningsläget skall 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 uppgifter eller realtidsuppgifter (27 kap. 21 § andra stycket RB). Tiden kan dock förlängas på begäran av åklagaren. Domstolens beslut om tillstånd går enligt 30 kap. 12 § RB genast i verkställighet.

Från tillämpningsområdet undantas 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 (27 kap. 20 § andra stycket RB). Därmed avses bl.a. system för snabbtelefoner, porttelefoner, PC-nät och liknande utrustning inom eller intill en bostad, hörslingor för hörselskadade eller interna system för personsökning i form av fasta installationer. Även interna telekommunikationer på mindre arbetsplatser via t.ex. PC-nät utgör telenät av mindre betydelse. Motsatsen gäller vanligtvis beträffande sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät eller större företagsnät. Detsamma gäller fristående datorer som är för-

sedda med modem och datorer i t.ex. små interna nätverk som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem. Om kommunikationen endast sker internt inom ett slutet nät bör det krävas att nätet är av större omfattning för att en tvångsåtgärd skall få äga rum. Frågan om ett telenät skall anses vara av mindre betydelse prövas utifrån en samlad bedömning av de olika omständigheter som rör ett telenäts betydelse från allmän kommunikationssynpunkt. Då kan bl.a. antalet anslutningar, geografisk spridning och hur utrustningen fungerar och används ha betydelse (prop. 1994/95:227 s. 27 och 31 och Fitger, Rättegångsbalken 2 s. 27:41).

2.4.4 Beslag och editionsföreläggande avseende telemeddelanden

Det har i praxis förelegat en osäkerhet huruvida ”generella” tvångsmedel i rättegångsbalken kan användas för att hämta in uppgifter som finns om telemeddelanden *hos operatörer*. 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 telelagen och numera lagen om elektronisk kommunikation (SOU 1998:46 s. 71 och JO 1997/98 s. 47 ff., jfr avsnitt 2.6). Regeringen har under senare tid uttalat att uppgifter om telemeddelanden, eller, som det benämns i 6 kap. 20 § första stycket 3 LEK, ”uppgifter som angår ett särskilt elektroniskt meddelande”, hos operatörer 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, att detta får anses följa redan av allmänna principer och att något lagstiftningsbehov därför inte finns (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 operatör* 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).

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

2.5 Sekretesslagen

I sekretesslagen finns bestämmelser som formellt ger de brottsutredande myndigheterna vissa möjligheter att utan domstolsprövning hämta in uppgifter om telemeddelanden. Förutsättningarna för att få tillgång till uppgifter om telemeddelanden skiljer sig mellan sekretesslagens regler och rättegångsbalkens.

I sekretesslagen finns bestämmelser om sekretess som gäller för myndigheter som driver televerksamhet. 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 uppgift som angår misstanke om brott får emellertid lämnas till en myndighet som har att ingripa mot brottet, om det är föreskrivet fängelse i minst två år för brottet (14 kap. 2 § fjärde och femte styckena sekretesslagen). Såväl innehållet i ett telemeddelande som uppgifter om ett telemeddelande, t.ex. när och mellan vilka abonnemang som meddelandet har utväxlats, 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 brottsutredande myndigheten. Bestämmelserna i sekretesslagen är inte begränsade till att gälla endast uppgifter som har anknytning till en person som är misstänkt för ett brott.

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 brottsutredande myndigheternas verksamhet. I stället fick telelagen och senare lagen om elektronisk kommunikation den betydelse som sekretesslagen tidigare hade.

2.6 Telelagen och lagen om elektronisk kommunikation

Telelagen infördes i samband med att verksamheten i Televerket överfördes till Telia AB. Bestämmelserna om tystnadsplikt i telelagen skulle enligt regeringen utgöra en huvudsaklig motsvarighet till vad som gällde enligt sekretesslagen för Televerkets verksamhet (se prop. 1992/93:200 s. 162 ff.).

År 2000 presenterade EG-kommissionen ett förslag till nytt regelverk för elektronisk kommunikation i syfte att modernisera gemenskapens lagstiftning på området. Förslaget lades fram mot bakgrund av den snabba tekniska och marknadsmässiga utvecklingen. Kommissionens förslag behandlades av Europaparlamentet och rådet. Det regelverk som senare beslutades omfattar flera direktiv, bl.a. direktivet (2002/21/EG) om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet), direktivet (2002/20/EG) om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet, direktivet (2002/19/EG) om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet), direktivet (2002/22/EG) om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (USO-direktivet) och direktivet (2002/58/EG) om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

För att genomföra EG-direktiven tillsatte regeringen under år 2001 en utredning, e-komutredningen. På grundval av utredningens arbete infördes lagen om elektronisk kommunikation. Lagen ersatte i juli 2003 telelagen och lagen om radiokommunikation.

E-komutredningen angav i sitt delbetänkande Lag om elektronisk kommunikation (SOU 2002:60 s. 267) att elektronisk kommunikation ofta används som en samlande benämning på den verksamhet som bedrivs inom det nya område som växer fram mot bakgrund bl.a. av konvergensutvecklingen och Internet och att en sådan beskrivning inte är speciellt klargörande. E-komutredningen ansåg att begreppet elektronisk kommunikation behövde konkretiseras ytterligare men konstaterade också att varken ramdirektivet eller de s.k. särdirektiven innehåller någon definition av begreppet. Däremot definieras vad som menas med elektroniska kommunikationsnät och elektroniska kommunikationstjänster i ramdirektivet.

Lagen om elektronisk kommunikation gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning (1 kap. 4 § första stycket LEK). I 1 kap. 7 § LEK definieras elektroniskt kommunikationsnät som system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs. Enligt samma bestämmelse avses med elektronisk kommunikationstjänst en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (se även avsnitt 3.4).

Till skillnad från telelagen är den nya lagen tillämplig inte endast på telefoni och datakommunikation utan även på utsändningar till allmänheten av program i ljudradio och TV. Riksdagen har i samband med att lagen om elektronisk kommunikation antogs beslutat om nya mål för sektorn elektronisk kommunikation. Enligt riksdagens beslut är målen att enskilda och myndigheter skall få tillgång till effektiva och säkra elektroniska kommunikationer med största möjliga utbyte när det gäller urvalet av överföringstjänster samt deras pris och kvalitet. Sverige skall i ett internationellt perspektiv ligga i framkanten i dessa avseenden (prop. 2002/03:110 s. 101 f. och bet. 2002/03:TU6 s. 23 f.).

Vissa bestämmelser i lagen om elektronisk kommunikation knyter an till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Enligt 6 kap. 19 § LEK skall vissa verksamheter bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand. Med detta avses den s.k. anpassningsskyldigheten (se vidare avsnitt 6).

I lagen om elektronisk kommunikation, liksom tidigare i telelagen, finns också bestämmelser som ger de brottsutredande myndigheterna vissa möjligheter att utan domstolsprövning hämta in bl.a. uppgifter som angår s.k. elektroniska meddelanden. Vid utlämnande av uppgifter enligt lagen om elektronisk kommunikation är det i princip fråga om samma typ av uppgifter som de brottsutredande myndigheterna erhåller genom hemlig teleövervakning.

I 6 kap. 20 § LEK finns följande bestämmelse om *tystnadsplikt*.

> 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.

Enligt 6 kap. 21 § LEK har operatörerna dessutom tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel, nämligen 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 brottsutredande myndigheterna har möjligheter att få uppgifter i olika hänseenden. 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 skall 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 skall ingripa mot brottet,

om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,

---

Uppgift om abonnemang, enligt 6 kap. 20 § första stycket 1 LEK, avser uppgifter som identifierar en abonnent och/eller ett abonnemang, framför allt namn, titel, adress och abonnentnummer. Abonnent är enligt 1 kap. 7 § LEK den som har ingått avtal med en leverantör av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster. Även s.k. IP-adresser bör falla in under kategorin uppgift om abonnemang, oavsett om IP-adressen är statiskt eller dynamiskt tilldelad (se nedan). Huruvida uppgift om den s.k. PUK-koden (Personal Unblocking Key, Personlig UpplåsningsKod) är uppgift om abonnemang eller annan uppgift som angår ett särskilt elektroniskt meddelande (se nedan) är något oklart i den praktiska tillämpningen. PUK-koden ingår exempelvis inte i meddelandet. Enligt vår mening talar det mesta för att PUK-koden inte kan räknas till annat än uppgift om abonnemang.

IP-telefoni kan sägas vara telefoni som förmedlas med hjälp av Internetprotokoll. När t.ex. ett e-postmeddelande skickas på Internet tilldelas den uppkoppling som är aktuell när meddelandet skickas en IP-adress. Varje operatör disponerar ett visst antal IP-adresser, som ”lånas ut” till abonnenterna. Detta kan ske på permanent basis (s.k. fasta eller statiska IP-adresser) eller dynamiskt, där abonnenten tilldelas en IP-adress varje gång uppkoppling sker mot operatören. En fast eller statisk IP-adress innebär alltså att IP-adressen är fast knuten till ett Internetabonnemang och att samma IP-adress därför tilldelas vid varje tillfälle som uppkoppling sker. I Sverige är det vanligast med tilldelning av dynamiska IP-adresser när det gäller privata abonnemang.

Uppgifterna om abonnemang skall som framgår av bestämmelsen lämnas ut, om fängelse är föreskrivet för brottet och brottet enligt den brottsutredande myndighetens bedömning kan föranleda annan påföljd än böter.

Annan uppgift som angår ett särskilt elektronisk meddelande, enligt 6 kap. 20 § första stycket 3 LEK, avser t.ex. uppgift om vilka som har deltagit i utväxlingen av ett elektroniskt meddelande samt när och under hur lång tid utväxlingen ägde rum. Även uppgifter om positionen hos en mobiltelefon när uppgiften samtidigt angår ett elektroniskt meddelande är uppgifter som omfattas av tystnadsplikten i bestämmelsen. Att det skall vara fråga om ett särskilt elek-

troniskt meddelande kan dock inte förstås så att den brottsutredande myndigheten måste specificera enskilda meddelanden, t.ex. genom att ange en viss abonnent och tidpunkt för meddelandet. S.k. basstationstömning, där de brottsutredande myndigheterna begär uppgifter som omfattas av tystnadsplikt om t.ex. samtliga de mobiltelefoner som haft kontakt med en basstation i närheten av en brottsplats under en begränsad tid, anses vara annan uppgift som angår ett särskilt elektroniskt meddelande. Uppgifterna skall lämnas ut till de brottsutredande myndigheterna om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år.

Det kan för tydlighetens skull nämnas att det inte finns 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 brottsutredande myndigheterna att få uppgifter från operatörer finns dock i skyldigheten för operatörerna att utplåna eller avidentifiera uppgifter. I 6 kap. 5 § LEK föreskrivs att trafikuppgifter som huvudregel skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Undantag gäller i vissa fall. Det rör framför allt uppgifter som krävs för abonnentfakturering (6 kap. 6 § LEK), uppgifter som omfattas av beslut om hemlig teleavlyssning eller hemlig teleövervakning (6 kap. 8 § 1 LEK) och uppgifter som sparas för att förhindra eller avslöja obehörig användning av ett nät eller en tjänst (6 kap. 8 § 3 LEK). Vi återkommer till den s.k. bevarandeskyldigheten i avsnitt 7.

Bestämmelserna i lagen om elektronisk kommunikation är inte begränsade till att gälla uppgifter som har anknytning till en person som är misstänkt för brott (jfr exempelvis 27 kap. 20 § första stycket RB). Det är med andra ord inte nödvändigt att som vid hemlig teleavlyssning och hemlig teleövervakning ha en skäligen misstänkt person för att myndigheten skall få begära att uppgifterna lämnas ut från operatören. Inte heller behöver uppgiften ha en särskild anknytning till en eventuell misstänkt person.

Dessutom bör nämnas att skyldigheten för operatörerna att lämna ut uppgifter till brottsutredande myndigheter enbart gäller uppgifter som omfattas av tystnadsplikten i 6 kap. 20 § LEK. I andra fall får operatören alltså välja fritt om uppgifterna skall lämnas ut eller inte. Uppgifterna kan då också hämtas in av de brottsutredande myndigheterna genom husrannsakan, beslag och editionsföreläggande (jfr avsnitt 2.4.4).

2.7 Övriga lagar om hemlig teleavlyssning m.m.

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns också i 1952 års tvångsmedelslag. Denna lag gäller vid förundersökning om dels vissa allmänfarliga brott, t.ex. mordbrand och sabotage, dels vissa högmålsbrott (brott mot rikets inre säkerhet) som uppror och olovlig kårverksamhet, dels vissa brott mot rikets (yttre) säkerhet, t.ex. spionerі, dels terroristbrott. Lagen gäller också straffbara fall av försök, förberedelse och stämpling till sådana brott. I förhållande till regleringen i rättegångsbalken innebär lagen större möjligheter att använda bl.a. hemlig teleavlyssning och hemlig teleövervakning. Tillstånd till dessa tvångsmedel får lämnas även om det är föreskrivet lindrigare straff än vad som stadgas i rättegångsbalken. Åklagaren får i brådskande fall, till skillnad från vad som gäller enligt rättegångsbalken, själv besluta om användning av tvångsmedlen. Har åklagaren gjort detta, skall han genast anmäla det hos rätten, som skyndsamt skall pröva ärendet. Lagen är tidsbegränsad. Efter den senast beslutade förlängningen gäller lagen till utgången av år 2007.

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns också i lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Även enligt denna lag får åklagaren fatta interimistiska beslut om tvångsmedlen, om det kan befaras att inhämtande av rättens tillstånd skulle medföra fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen.

I lagen om särskild utlänningskontroll finns också bestämmelser om hemlig teleavlyssning och hemlig teleövervakning. Bestämmelserna avviker från vad som gäller enligt t.ex. rättegångsbalken och 1952 års tvångsmedelslag bl.a. på det sättet att det inte krävs att förundersökning är inledd. Åtgärderna får alltså vidtas i förebyggande syfte enligt vissa angivna rekvisit. Tvångsmedlen får användas om det är påkallat för att utröna om en utlänning eller en organisation eller grupp som han tillhör eller verkar för planlägger eller förbereder terroristbrott. Frågan om tillstånd prövas av i första hand Stockholms tingsrätt på yrkande av Rikspolisstyrelsen eller en polismyndighet.

2.8 Regler till skydd för den personliga integriteten

2.8.1 Allmänt

I samband med överväganden om de brottsutredande myndigheternas arbetsmetoder och om tvångsmedel har självfallet frågor om personlig integritet en central betydelse. Integritetsskyddet kan inte ses isolerat för sig utan måste vägas mot andra befogade intressen, däribland effektiviteten inom t.ex. brottsbekämpningen. Behovet av effektivitet i brottsbekämpningen måste alltså ställas i relation till det eventuella integritetsintrång som kan befaras uppkomma och även mot andra intrång, t.ex. i ett företags intressen av närmast ekonomiskt slag. Vid överväganden som t.ex. rör införande av nya tvångsmedel eller liknande metoder är syftet givetvis att förbättra möjligheterna att bekämpa brott. En ibland oundviklig konsekvens av detta är att integritetsintresset får stå tillbaka (se vidare Dir. 2004:51).

En svårighet är att definiera vad som avses med begreppet personlig integritet, eller med andra ord hur det skyddsvärda området skall bestämmas. I lagstiftningen finns ingen definition av begreppet. I olika utredningar (se t.ex. Tvångsmedelskommitténs betänkande Tvångsmedel – Anonymitet – Integritet, SOU 1984:54 s. 42) har man med utgångspunkt bl.a. i de grundläggande fri- och rättigheterna i regeringsformens andra kapitel försökt ringa in begreppet genom att skilja mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skyddet för liv och hälsa samt mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin).

Ett annat sätt att bestämma begreppet personlig integritet är enligt Stig Strömholm (se bl.a. SvJT 1971 s. 695) att ange vilka handlingar som kan kränka någons integritet. Man kan då dela in kränkningarna i tre huvudgrupper: 1) intrång i en persons privata sfär, oavsett om det sker i fysisk eller annan mening; 2) insamlande av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annan användning (t.ex. som bevisning i rättegång) av uppgifter om en persons privata förhållanden. För att ge en mer kon-

kret bild av begreppet har Stig Strömholm givit följande exempel på olika slag av kränkningar:

1. tillträde till och genomsökande av privata lokaler eller annan egendom;
2. kroppsundersökning;
3. medicinska undersökningar, psykologiska tester osv.;
4. intrång i en persons privata sfär genom skuggning, spionerande, telefonterror o.d.;
5. som ett speciellt kvalificerat eller, genom sina möjliga konsekvenser, speciellt farligt särfall till grupperna 1 och 4: ofredande genom företrädare för massmedierna, t.ex. i form av ”snokreportage” men även påträngande och brutala intervjuer (av olycksoffer, dessas anhöriga eller eljest personer som har svårt att värja sig);
6. olovlig ljudupptagning, fotografering eller filmupptagning;
7. brytande av brevhemlighet;
8. telefonavlyssning;
9. utnyttjande av elektronisk avlyssningsapparatur;
10. spridande av förtroliga uppgifter (t.ex. genom advokater, läkare, själasörjare o.d.);
11. avslöjande inför offentligheten av annans privata förhållanden;
12. olika former av nyttjande av annans namn, bild eller liknande identifieringsmedel;
13. missbruk av annans ord eller meddelande (exempelvis genom förvrängda eller uppdiktade intervjuer);
14. angrepp på annans heder och ära.

Integriteten kan alltså kränkas på många olika sätt. Även om det inte finns någon entydig definition av begreppet kan man säga att kränkningarna innebär ett intrång i en fredad sfär eller zon som den enskilde bör vara tillförsäkrad.

Det är en svår uppgift att avväga integritetsintresset mot nödvändigheten av att tillse att myndigheterna har effektiva metoder till sin hjälp. Varje tvångsmedel innefattar ett mått av integritetsintrång. Det ligger i sakens natur. Samtidigt måste det beaktas att denna integritetskränkning ofta är blygsam i jämförelse med den kränkning som brottsoffren många gånger måste utstå. Ju allvarligare och mer svårutredd brottsligheten blir, desto mer tvingas statsmakterna tillåta i form av tvångsåtgärder för att bekämpa och utreda den brottsligheten. Det kan aldrig accepteras att brottsligheten tar överhanden och att statsmakterna kapitulerar inför utvecklingen. En utgångspunkt måste vara att ingen medborgare i varje situation kan hävda rätt till handlingsfrihet eller rätt att bli lämnad i

fred. Integritetskommittén uttryckte sig på följande sätt (SOU 1970:47 s. 56).

> En individ som lever i ett samhälle och sålunda ingår i en gemenskap med andra människor kan självfallet inte göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostört av samhällets organ. Eftersom gemenskapen med andra människor och samhörigheten med samhället är grundläggande för den enskilda människans villkor, är det tydligt att tanken på skydd för dylika anspråk står i motsats till åtskilligt som av andra skäl måste gälla. Regler som syftar till att skydda den enskildes personliga integritet måste sålunda förses med olika, i skilda situationer mer eller mindre vittgående undantag eller på annat sätt begränsas till sin giltighet, så att andra människors och samhällets intressen i övrigt inte träds för när.

I det sammanhanget måste nämnas att en annan och minst lika viktig utgångspunkt är att de brottsbekämpande myndigheterna inte får ges sådana befogenheter att medborgarnas tilltro till dem och rättssystemet påverkas negativt. Förtroendet kan skadas om medborgarna upplever att det finns risk för att t.ex. polisen utan tillräckliga skäl samlar information om enskilda och deras privatliv. Den skada som ett minskat förtroende för de brottsbekämpande myndigheterna kan komma att medföra kan väga tyngre än fördelen av att viss brottslighet kan förhindras eller klaras upp.

En annan sida av saken är att de brottsbekämpande myndigheterna måste ha sådana arbetsmetoder att man uppnår i tillräckligt hög grad positiva resultat i arbetet. I annat fall kan medborgarna även av den anledningen få ett minskat förtroende för myndigheterna.

Skyddet för integriteten är i viss utsträckning fastställt i internationella konventioner och svensk rätt. Den rättsliga regleringen kan sägas utgöra den yttre ramen för en diskussion kring den personliga integriteten i samband med de brottsbekämpande myndigheternas arbetsmetoder. Därmed är inte sagt att en särskild metod är godtagbar från integritetssynpunkt enbart på den grunden att användningen är lagligen grundad. Integritetsskäl kan naturligtvis göra sig så starkt gällande att en åtgärd som i och för sig ryms inom den legala ramen ändå inte bör godtas. Allmänhetens tilltro till rättsväsendet får under inga förhållanden skadas.

Det kan nämnas att en parlamentariskt sammansatt kommitté, Integritetsskyddskommittén, för närvarande utreder frågor om skyddet för den personliga integriteten (Dir. 2004:51). Kommitténs uppdrag är bl.a. att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten och att överväga om det, vid sidan av befintlig lagstiftning, behövs generellt tillämpliga bestämmelser till skydd för den personliga integriteten. När det gäller intresset av effektivitet i brottsbekämpningen skall kommittén särskilt analysera förhållandet mellan å ena sidan den totala verkan av befintliga tvångsmedel och övervakningsmetoder och å andra sidan skyddet för den personliga integriteten. Kommittén skall slutredovisa sitt arbete senast den 30 mars 2007.

2.8.2 Regeringsformen och principer för tvångsmedelsanvändning

En grundläggande bestämmelse om skydd för den enskildes personliga integritet finns i 1 kap. 2 § fjärde stycket regeringsformen. Där sägs bl.a. att det allmänna skall värna den enskildes privatliv och familjeliv. Bestämmelsen har inte karaktären av en rättsligt bindande föreskrift utan anger en målsättning för den samhälleliga verksamheten. Den målsättningen följs upp i 2 kap. regeringsformen om grundläggande fri- och rättigheter med rättsligt bindande föreskrifter som skyddar den personliga integriteten i förhållande till det allmänna. Bestämmelserna är bindande för lagstiftaren och i viss utsträckning för domstolarna och andra rättstillämpande organ.

Vissa av bestämmelserna ger ett absolut skydd i den meningen att skyddet inte kan begränsas på annat sätt än genom grundlagsändring. För andra bestämmelser gäller att skyddet är relativt så till vida att det kan begränsas genom lag. Det gäller t.ex. bestämmelsen om skydd mot vissa påtvingande kroppsliga ingrepp i 2 kap. 6 § regeringsformen. Där föreskrivs att varje medborgare gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Bestämmelsen ändrades senast år 1976, dock utan att någon saklig ändring var avsedd (prop. 1975/76:209 s. 147 f.). I lagstiftningsärendet anfördes bl.a. att det förhållandet att skyddet avser endast meddelanden som är förtroliga innebär att skyddet inte omfattar t.ex. samtal i en folksamling

eller i radiosändningar. Skyddet omfattar däremot meddelanden som sänds med post eller på annat sätt som brev, telegram, bandinspelningar osv. Skyddet omfattar såväl hemlig avlyssning som sker samtidigt med ett samtal som upptagning av ett samtal för senare avlyssning (SOU 1998:46 s. 51). Fotografering av skriftliga handlingar och filmning av samtalandes läpprörelser är exempel på sådana upptagningar av förtroliga meddelanden som avses i bestämmelsen.

I begreppet ”husrannsakan och liknande intrång” torde inte innefattas intrång i datorer eller andra upptagningar för automatisk databehandling (se prop. 1987/88:65 s. 62 och SOU 1992:110 s. 351 f.).

Skyddet mot undersökning av brev eller annan förtrolig försändelse gäller under den tid försändelsen är under befordran. Om denna avgränsning anges i motiven att mottagaren kan välja att förstöra meddelandet när han tagit emot och tagit del av försändelsen. När försändelsen har nått adressaten, kan också enligt motiven andra skyddsregler träda i funktion, såsom t.ex. skyddet mot kroppsvisitation och husrannsakan (se SOU 1975:75 s. 200).

Det skydd som avses i 2 kap. 6 § regeringsformen kan begränsas endast genom lag och i övrigt enligt vad som föreskrivs i 2 kap. 12 § regeringsformen. I det sistnämnda lagrummet anges att begränsningar får göras endast för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

De nu behandlade bestämmelserna i regeringsformen gäller för svenska medborgare. Om inte annat är föreskrivet är utlänning här i riket dock likställd med svenska medborgare i angivet avseende (2 kap. 22 § andra stycket 3 regeringsformen).

Regleringen i 2 kap. 12 § regeringsformen har legat till grund för de s.k. ändamåls-, behovs- och proportionalitetsprinciperna som gäller för det allmännas användning av tvångsmedel i olika sammanhang (se bl.a. SOU 1998:46 s. 54).

Ändamålsprincipen innebär att en myndighets befogenhet att använda tvångsmedel skall 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 och en mindre ingripande åtgärd inte är tillräcklig.

Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet skall stå i rimlig proportion till vad som står att vinna med åtgärden. Proportionalitetsprincipen finns uttryckt på många håll i lagstiftningen. I exempelvis 27 kap. 1 § tredje stycket RB finns en sådan bestämmelse som gäller vid tillämpning av de tvångsmedel som regleras i det kapitlet i rättegångsbalken, däribland hemlig teleavlyssning och hemlig teleövervakning. Regeln skall beaktas av bl.a. domstolen när den tar ställning till frågor om tvångsmedlen. En tillämpning av proportionalitetsprincipen innebär en skyldighet för den som beslutar om tvångsmedel att göra en avvägning mellan skälen för åtgärden och de olägenheter som åtgärden kan förorsaka den misstänkte eller något annat motstående intresse, alltså i nu aktuella fall en avvägning mellan intresset av att utreda brott och de risker som en användning av tvångsmedlet innefattar för den personliga integriteten hos den misstänkte och tredje man.

Det blir en mängd olika faktorer som skall vägas in vid en proportionalitetsbedömning; vad är det som skall övervakas, hur drabbas tredje man, hur länge skall åtgärden pågå, vad står att vinna med åtgärden, vilken svårighetsgrad har brottet, används flera olika tvångsmedel samtidigt mot samma person, osv. Ju större integritetsrisker som är förenade med en användning av tvångsmedlet, desto större krav måste ställas för att tvångsmedlet skall få användas.

Frågan om en ansökan om tvångsmedel skall bifallas eller inte blir också beroende av vilka skäl som talar för åtgärden. Gäller misstankarna särskilt allvarlig brottslighet kan det vara godtagbart att tillåta användning av ett tvångsmedel även i fall där integritetsriskerna är mycket betydande. En konsekvens av proportionalitetsprincipen kan bli att det ställs upp inskränkande villkor för tvångsmedelsanvändningen, t.ex. att en telefon i en viss telefonkiosk, som ibland används av den misstänkte, får avlyssnas enbart när polisen kan iaktta att den misstänkte använder telefonen. Proportionalitetsprincipen ger också utrymme för att avslå en ansökan om t.ex. hemlig teleavlyssning även om de formella förutsättningarna i övrigt är uppfyllda. Principen är tillämplig inte endast vid prövningen av tvångsmedelsfrågan, utan aktualiseras under hela förfarandet, dvs. principen gäller även för de brottsutredande myndigheterna på verkställighetsstadiet.

Proportionalitetsprincipen regleras även i 8 § polislagen, där det bl.a. sägs att en polisman som har att verkställa en tjänsteuppgift skall ingripa på det sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Den bestämmelsen tar bl.a. sikte på verkställigheten av nu aktuella tvångsmedelsbeslut (SOU 1998:46 s. 376 ff. och 480 f.).

Det skall också sägas att det i regeringsformen finns en grundläggande bestämmelse om integritetsskydd på IT-området, 2 kap. 3 § andra stycket. Där anges att varje medborgare skall i den utsträckning som närmare anges i lag skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Sådana integritetsskyddande regler finns huvudsakligen i personuppgiftslagen (1998:204).

2.8.3 Europakonventionen

Europarådet antog den 4 november 1950 konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Ett antal tilläggsprotokoll har under åren öppnats för ratifikation. Genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna gäller europakonventionen jämte tilläggsprotokoll sedan den 1 januari 1995 som svensk lag (SOU 1998:46 s. 52).

Enligt artikel 8:1 i konventionen har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet är av mycket allmän art och omfattar skydd mot en mängd åtgärder. Med korrespondens avses olika former för att överföra meddelanden mellan individer. Överföring av meddelanden med hjälp av telefon, telefax, radio och datorer omfattas av konventionens skydd för korrespondens (se Danelius, Mänskliga rättigheter i europeisk praxis, 2002, s. 270). Ett ingrepp i skyddet för korrespondens är bl.a. när någon hindrar eller kontrollerar sådan kommunikation.

Av artikel 8:2 följer att inskränkningar i dessa rättigheter får ske under vissa förutsättningar. En inskränkning måste ske med stöd av lag och inskränkningen skall vara ägnad att tillgodose något av de i artikel 8:2 uppräknade allmänna eller enskilda intressena, däribland statens säkerhet, den allmänna säkerheten och förebyggande av oordning eller brott. Inskränkningen måste anses vara nödvändig i ett demokratiskt samhälle för att tillgodose detta intresse. Det kan

i huvudsak sägas innebära att det måste finnas ett angeläget samhälleligt behov av inskränkningen och att den måste stå i rimlig proportion till det syfte som skall tillgodoses genom ingreppet (jfr Danelius s. 263). Vidare måste undantaget vara utformat med sådan precision att inskränkningen av rättigheten är förutsebar i rimlig utsträckning. I t.ex. målet Kruslin och Huvig mot Frankrike (dom den 24 april 1990, 176 A) framhöll Europadomstolen att telefonavlyssning var ett allvarligt ingrepp i privatliv och korrespondens och att ett tydligt lagstöd med klara och detaljerade regler måste krävas. Så ansågs inte fallet vara med den mycket allmänna bestämmelsen i den franska straffprocesslagen på vilken beslut om telefonavlyssning grundades (Danelius s. 271). Det skall framhållas att kravet på tydligt lagstöd inte hindrar att de rättstillämpande myndigheterna ges ett visst tolkningsutrymme eller en ”diskretionär” prövningsrätt genom lagstiftningen.

Europadomstolen har funnit att bl.a. buggning och inspelning av telefonsamtal, inhämtande av uppgifter om telefonsamtal samt övervakning med hjälp av fjärrstyrda kameror utgör intrång i rätten till skydd för privatliv och/eller korrespondens.

När de gäller frågan om ett intrång har varit berättigat enligt artikel 8, har Europadomstolen noterat att det stipulerade kravet på laglighet innebär dels att intrånget måste vara grundat på lag eller rättspraxis enligt den inhemska rättsordningen, dels att tillämplig nationell lag uppfyller rimliga krav på rättssäkerhet. Bland annat måste den nationella lagen vara tillgänglig, skydda mot godtycke och vara så klar och detaljerad att konsekvenserna av dess tillämpning kan förutses. I fråga om kravet på förutsebarhet har Europadomstolens framhållit nödvändigheten av att ett så allvarligt intrång som teleavlyssning regleras genom klara och detaljerade bestämmelser samt att lagstiftningen inte får lämna utrymme för missbruk. Domstolen har bland annat hänvisat till att det i bestämmelserna bör finnas preciseringar av den personkrets som kan komma att bli föremål för teleavlyssning och de brott i fråga om vilka teleavlyssning kan beslutas. Vidare bör besluten begränsas tidsmässigt (se prop. 2004/05:143 s. 27 f.). Det måste också finnas en effektiv kontroll av att systemet inte missbrukas (se SOU 1993:40, del B s. 58 med hänvisningar). När teleavlyssning har ansetts utgöra en kränkning av artikel 8 har i de flesta fall bristande lagenlighet utgjort grunden för kränkningen.

Vid frågor om polisiära arbetsmetoder är också artikel 6 i Europakonventionen av intresse. Artikeln berör rätten till en rättvis rättegång och ger en tilltalad bl.a. rätt till en rättvis domstolsförhand-

ling. Även om artikeln berör domstolsförfarandet och inte tidigare stadier i processen, som underrättelseinhämtning, spaning och förundersökning, är det ändå nödvändigt att beakta artikeln tidigt, eftersom olika ageranden från polisens sida, t.ex. genom otillåten brottsprovokation, kan få den kommande rättegången att framstå som orättvis.

Enligt 2 kap. 23 § regeringsformen får lag eller annan författning inte meddelas i strid med Sveriges åtaganden på grund av europakonventionen.

2.8.4 Brottsbalken

Det grundlagsfästa skyddet för den enskildes integritet gäller i förhållande till det allmänna. Integritetskränkningar från enskilda straffas genom bestämmelser i annan lag, däribland brottsbalken. Även brott av tjänstemän hos det allmänna straffas genom sådana bestämmelser. Integritetsskyddet regleras främst genom bestämmelserna i 4 kap. BrB om brott mot frihet och frid samt 5 kap. BrB om ärekränkningsbrott. Även 3 kap. BrB om brott mot liv och hälsa samt 6 kap. BrB om sexualbrotten innehåller regler som kan sägas utgöra ett skydd för den personliga integriteten. Här skall sägas något om vissa bestämmelser i 4 kap. BrB.

Enligt 4 kap. 8 § BrB är det straffbart som *brytande av post- eller telehemlighet* att olovligen bereda sig tillgång till ett meddelande som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande. Det saknar betydelse om telemeddelandet förmedlas via det allmänna telenätet eller på annat sätt. För straffansvar fordras dock en medverkan av ett telebefordringsföretag. Meddelanden i helt privata kommunikationsnät skyddas alltså inte.

För att bestämmelsen skall vara tillämplig förutsätts alltså att försändelsen innehåller ett meddelande. Det är inte straffbart att lyssna på telemeddelanden som befordras endast med radio (t.ex. mobiltelefoni som inte sker via kabel, prop. 1992/93:200 s. 166 f. och SOU 1992:110 s. 431). Avlyssning av radiotrafik faller med andra ord utanför det straffbara området. Det är sedan länge en vedertagen princip att ”etern är fri”. Det står därför var och en fritt att avlyssna såväl sådan radiokommunikation som är riktad till allmänheten som annan typ av radiokommunikation (se 6 kap. 17 § andra stycket 3 LEK). En annan sak är att det i 6 kap. 23 § LEK föreskrivs att den som via en radiomottagare har avlyssnat eller på

annat sätt fått tillgång till ett meddelande, som varken är avsett för honom eller för allmänheten, inte obehörigen får föra det vidare. Tystnadsplikten är straffsanktionerad i 7 kap. 15 § första stycket LEK. Det kan nämnas att lagen om elektronisk kommunikation omfattar i nu aktuellt hänseende enbart kommunikation i allmänna kommunikationsnät eller via allmänt tillgängliga elektroniska kommunikationstjänster.

Med telemeddelande torde i brottsbalken avses detsamma som i 6 kap. 19 § tredje stycket LEK, nämligen ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskild anordnad ledare. Den som tar del av ett e-postmeddelande kan alltså göra sig skyldig till brytande av post- eller telehemlighet liksom den som tar del av överföringar av datafiler med hjälp av t.ex. FTP (File Transfer Protocol) och överföringar från hemsidor, nyhetsgrupper och chatkanaler.

Liksom grundlagsskyddet och skyddet enligt europakonventionen omfattar det straffrättsliga skyddet ett meddelande som är under befordran. Om någon olovligen bereder sig tillgång till ett brev eller liknande sedan brevet överlämnats till adressaten, kan straff enligt 4 kap. 8 § BrB inte komma ifråga. När meddelandet kommit fram till mottagaren kan i stället bestämmelserna om intrång i förvar eller dataintrång bli aktuella (se nedan). För straffansvar krävs inte att meddelandet är förtroligt. Därigenom skyddas även meddelanden som riktar sig mot en mer obestämd krets av personer. För straffansvar krävs inte heller att personen faktiskt tagit del av innehållet i meddelandet, utan enbart att han har haft möjlighet till det. En förutsättning för straffbarhet är att gärningen sker olovligen. Även utan samtycke kan en gärning anses vara fri från ansvar, exempelvis om förfarandet utgör tvångsmedelsanvändning såsom beslag av brev eller hemlig teleavlyssning.

Den som olovligen bryter ett brev eller ett telegram eller annars bereder sig tillgång till något som förvaras förseglat, under lås eller annars tillslutet kan dömas för *intrång i förvar* enligt 4 kap. 9 § BrB. Bestämmelsen är subsidiär i förhållande till 4 kap. 8 § BrB. Straffskyddet omfattar exempelvis brev och meddelanden som ännu inte har lämnats till befordran eller som redan har kommit mottagaren tillhanda. Liksom vid 4 kap. 8 § BrB kan gärningen vara fri från ansvar på grund av att den enligt särskilda bestämmelser är lovlig.

I 4 kap. 9 a § BrB regleras *olovlig avlyssning*. För det brottet döms den som i annat fall än som sägs om brytande av post- eller telehemlighet olovligen medelst tekniskt hjälpmedel för återgivning

av ljud i hemlighet avlyssnar eller upptar tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten inte äger tillträde och som han själv inte deltar i eller som han obehörigen berett sig tillträde till. I dessa fall rör det straffbara området en buggningssituation, dvs. ingen av dem som deltar i t.ex. samtalet är medveten om att avlyssningen sker. Avlyssningen sker alltså olovligen i hemlighet med tekniskt hjälpmedel.

Bestämmelsen om *dataintrång* i 4 kap. 9 c § BrB, som tidigare fanns i 21 § i den numera upphävda datalagen (1973:289), täcker såväl intrång i och störning av datorsystem som störning av och påverkan på datainformation. Enligt bestämmelsen är det straffbart att olovligen bereda sig tillgång till en upptagning för automatisk databehandling. Med upptagning för automatisk databehandling avses en hantering av uppgifter som sker med hjälp av dator som försetts med ett program som anger vilka åtgärder som skall vidtas, dvs. en programstyrd behandling. Det kan vara fråga om behandling av alla typer av uppgifter, alltså inte enbart personuppgifter. Uppgifterna måste dock vara fixerade på ett datamedium (hårddisk, diskett, CD-rom, band eller liknande) som antingen finns i eller kan matas in i en dator och som endast är läsbar med ADB-teknik (prop. 1973:33 s. 74 f.). Utskrifter från en dator skyddas alltså inte av bestämmelsen. Det är enligt samma bestämmelse också straffbart att olovligen ändra eller utplåna eller i register (kan nu sägas motsvara begrepp som databastabeller, kataloger och filer) föra in upptagning för automatisk databehandling. Även om tillgången till en upptagning är lovlig är det alltså straffbart att olovligen ändra i eller utplåna en sådan upptagning. Både den information som behandlas och de program som styr behandlingen omfattas av det straffrättsliga skyddet. Det gäller oavsett om effekten av ändringen är tillfällig eller bestående. Att installera programvaror i form av virusprogram, snifferprogram (används för att fånga upp t.ex. lösenord) och crackprogram (används för att åstadkomma skada) kan också omfattas av uttrycket att i register föra in upptagning för automatisk databehandling. Med upptagning avses i paragrafen även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Det innebär bl.a. att om information förs över från en terminal till en dator, i vilken informationen bearbetas och lagras på ett datamedium, är det straffbart att olovligen bereda sig tillgång till sådan information under överföringen.

Straffskyddet beträffande dataintrång omfattar alla upptagningar för automatisk databehandling, oavsett om dessa innehåller personuppgifter eller inte. För straffansvar krävs inte heller att personen faktiskt tagit del av innehållet. Bestämmelsen om dataintrång är subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar (4 kap. 8 och 9 §§ BrB). Det innebär bl.a. att det inte är straffbart som dataintrång att via en på obehörigt sätt införskaffad kod ta del av telemeddelanden som finns lagrade på en server. En sådan gärning bedöms i stället enligt bestämmelserna i 4 kap. 8 och 9 §§ BrB. Dataöverföringar som sker med hjälp av ”det allmänna telenätet” skyddas av bestämmelsen om brytande av telehemlighet. Även försök och förberedelse till dataintrång som inte är ringa är straffbelagt (4 kap. 10 § BrB). Att på måfå testa olika användarnamn och lösenord har ansetts inte utgöra straffbart försök, eftersom sannolikheten att lyckas är alltför liten, dvs. det har inte förelegat en tillräcklig fara för att dataintrång skall fullbordas (se 23 kap. 1 § BrB). I samband med dataintrång förekommer det ofta att gärningsmannen före själva intrånget kartlägger måldatorn genom s.k. portscanning för att avgöra bl.a. vilket operativsystem som finns i måldatorn och vilka andra program som finns installerade. Med hjälp av den informationen genomförs sedermera dataintrånget. Eftersom även immateriella objekt kan utgöra ”hjälpmedel” vid förberedelse till brott enligt 23 kap. 2 § BrB kan innehav av programvaror för portscanning utgöra förberedelse till dataintrång liksom innehav av programvaror för skapande av exempelvis datavirus.

2.8.5 Rättegångsbalken m.m.

Regleringen i rättegångsbalken av förundersökningsförfarandet och tvångsmedelsanvändning innehåller en mängd bestämmelser och rekvisit som på olika sätt skall skydda den enskilde från integritetsintrång och ge honom vad som kan kallas rättsskyddsgarantier. Där finns bl.a. regler om beslutsordningen vid tvångsmedel (t.ex. domstolsprövningen enligt 27 kap. 21 § första stycket RB), om tillståndstiden (t.ex. vid hemlig teleavlyssning och hemlig teleövervakning enligt 27 kap. 21 § andra stycket RB), om offentliga ombud i vissa fall (27 kap. 26-30 §§ RB) och regler som tillförsäkrar den misstänkte och hans försvarare en viss insyn i utredningen. Rätten till insyn regleras av bestämmelserna i 23 kap. RB (SOU 1998:46 s. 90 ff. och SOU 2003:74 s. 187 ff.).

I 23 kap. 18 § RB föreskrivs att, när förundersökning har kommit så långt att någon skäligen kan misstänkas för brott, han skall när han hörs underrättas om misstanken. Efter denna tidpunkt har den misstänkte och hans försvarare enligt samma paragraf rätt att fortlöpande, i den mån det kan ske utan men för utredningen, ta del av vad som har förekommit under förundersökningen. De har också rätt att begära att utredningen kompletteras. Åtal får inte väckas förrän de har fått möjlighet att ta del av allt material i utredningen och fått skäligt rådrum att begära komplettering. Det har ansetts att det inte går att undanhålla den misstänkte information om något material i detta skede (se SOU 1999:53 s. 393 f. samt JO 1964 s. 214 och 1965 s. 198 samt Ds Ju 1979:15 s. 113, jfr dock prop. 1986/87:89 s. 145). Rätten till insyn gäller inte bara sådana uppgifter som har tagits in i protokollet utan även andra uppgifter (sådana uppgifter som finns i den s.k. slasken, dvs. uppgifter utanför förundersökningsprotokollet).

Bestämmelsen i 23 kap. 18 § RB ger den misstänkte och hans försvarare rätt till insyn men inte automatiskt rätt till handlingar som upprättats under förundersökningen. En sådan rätt uppkommer först när åtal har beslutats. Rätten till insyn omfattar även handlingar som inte är allmänna. Förundersökningsprotokoll anses inte bli allmänna handlingar förrän de är färdigställda (JO 1971 s. 88 och 1980/81 s. 124), eller om ärendet avslutas utan att fullständigt protokoll har upprättats, när ärendet arkiveras. Hos åklagaren blir förundersökningsmaterialet allmän handling när beslut fattas i åtalsfrågan, oavsett om det är fråga om ett färdigställt protokoll eller inte (SOU 1999:53 s. 394).

När åtal har väckts har den misstänkte och hans försvarare enligt 23 kap. 21 § RB rätt att på begäran få en utskrift av förundersökningsprotokollet, som skall innehålla det för den kommande domstolsprocessen relevanta materialet. Om en förundersökning inte föranleder åtal (s.k. negativt åtalsbeslut), föreligger inte någon ovillkorlig rätt för den misstänkte att få en utskrift av protokoll eller anteckningar. I stället blir 5 kap. 1 § sekretesslagen tillämplig (SOU 1998:46 s. 112 och 1999:53 s. 394, Gärde m.fl. Nya rättegångsbalken s. 314 samt prop. 1986/87:89 s. 148). Regeringsrätten har i praxis tillerkänt den misstänkte en sådan rätt (Regeringsrättens Årsbok 1995 referat 28).

Beslut om hemliga tvångsmedel fattas utan att den misstänkte själv är närvarande. Att inte den misstänkte kallas till en sådan prövning är självklart, eftersom avsikten är att han inte skall känna till att tvångsmedel används. Från och med den 1 oktober 2004 in-

fördes ett system med offentliga ombud i ärenden om hemlig teleavlyssning och hemlig kameraövervakning. Dessa ombud är motparter till åklagaren vid sammanträden inför domstol. Det offentliga ombudet har till uppgift att bevaka enskildas rätt och integritetsintressen i allmänhet och skall lyfta fram alla aspekter, även t.ex. skydd för tredje mans integritet. Det offentliga ombudet skall också bevaka att de grundläggande principerna för tvångsmedelsanvändning följs och får överklaga domstolens beslut. Syftet med systemet är bl.a. att stärka den enskildes rättsskydd och att, utöver att det är domstol som prövar ansökan om tillstånd, skapa ytterligare rättssäkerhetsgarantier redan vid tillståndsprövningen (se bl.a. Skr. 2004/05:36 s. 13).

För ytterligare uppgifter om den misstänktes partsbefogenheter, som partsinsynen och rätten att överklaga beslut om hemlig teleavlyssning och hemlig teleövervakning, hänvisar vi till Buggningsutredningens redogörelse i SOU 1998:46 s. 90 ff.

2.8.6 Polislagen

I polisens brottsbekämpande verksamhet skall bl.a. de allmänna principer beaktas som finns fastslagna i 8 § polislagen (1984:387). Enligt den bestämmelsen skall en polisman, när han verkställer en tjänsteuppgift, iaktta vad som föreskrivs i lagar eller andra författningar och ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Om polismannen måste använda tvång, får det ske bara i den form och den utsträckning som behövs för att det avsedda resultatet skall uppnås. Paragrafen ger därmed uttryck för bl.a. behovs- och proportionalitetsprinciperna (se avsnitt 2.8.2).

I förarbetena till polislagen fördes en diskussion om s.k. okonventionella spaningsmetoder (SOU 1982:63 s. 129 ff. och prop. 1983/84:111 s. 44 ff.). De metoder som nämndes där var bl.a. provokation, infiltration, agentverksamhet, desinformation och hemlig avlyssning. Dessutom definierades några principer som anses gälla för okonventionella spaningsmetoder men som har giltighet även i övrigt i polisarbetet. Polisen får enligt dessa principer aldrig

1. själv begå en kriminaliserad handling för att kunna efterforska eller avslöja brott,

2. provocera eller förmå någon att inleda en brottslig aktivitet (som personen annars inte skulle ha gjort), eller

3. underlåta att vidta föreskrivna åtgärder mot brott eller mot en person som misstänks för brott.

Departementschefen ansåg att principerna inryms i den allmänna regeln i 8 § polislagen och att det därför inte behövdes någon särskild lagreglering av okonventionella spaningsmetoder.

2.8.7 Lagen om elektronisk kommunikation

Även lagen om elektronisk kommunikation innehåller bestämmelser om integritetsskydd (särskilt 6 kap.). Förutom de bestämmelser som nämndes tidigare om tystnadsplikten kan nämnas att reglerna omfattar bl.a. skydd av personuppgifter och skydd mot obehörig avlyssning. Exempelvis anges i 6 kap. 3 § LEK att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst skall vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas och att den som tillhandahåller ett allmänt kommunikationsnät skall vidta de åtgärder som är nödvändiga för att upprätthålla skydd i nätet. Den säkerhet som avses är skydd mot olovlig avlyssning och liknande integritetskränkande handlingar. Åtgärderna skall vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärden, är anpassad till risken för integritetsintrång.

I 6 kap. 17 § LEK finns bestämmelser om förbud mot avlyssning. I princip finns ett totalt förbud mot att ta del av eller på annat sätt behandla uppgifter i ett elektroniskt meddelande som överförs i ett allmänt kommunikationsnät eller med en allmänt tillgänglig elektronisk kommunikationstjänst, eller trafikuppgifter som hör till meddelandet, om inte en av användarna har samtyckt till åtgärden. Ett av undantagen från bestämmelsen rör den situationen att man genom radiomottagare avlyssnar ett radiobefordrat elektroniskt meddelande som inte är avsett för den som avlyssnar eller allmänheten. Undantaget motiveras av att det är allas rätt att inneha en radiomottagare och att det inte är lämpligt att sanktionera själva avlyssnandet. Det har många gånger uttalats att ”etern är fri” och att var och en därmed kan avlyssna vad som transporteras radiobefordrat. Däremot får den som har avlyssnat eller på annat sätt fått tillgång till innehållet i ett sådant radiobefordrat meddelande inte obehörigen föra det vidare. Den tystnadsplikten, som föreskrivs i 6 kap. 23 § LEK, är straffsanktionerad i 7 kap. 15 § LEK.

På andra ställen i detta betänkande redovisas flera av de övriga bestämmelserna i 6 kap. LEK om integritetsskydd.

2.9 Parlamentarisk kontroll

En parlamentarisk kontroll över tillämpningen av bestämmelserna i rättegångsbalken om hemlig teleavlyssning och hemlig teleövervakning samt av bestämmelserna i lagen om hemlig kameraövervakning utövas av riksdagen på grundval av årliga uppgifter från regeringen. Regeringen får uppgifter om tillämpningen från Åklagarmyndigheten och Rikspolisstyrelsen. Den senaste redovisningen, som avser år 2003, gjordes i regeringens skrivelse 2004/05:36. Där framkommer bl.a. följande uppgifter rörande hemlig teleavlyssning och hemlig teleövervakning.

Under år 2003 meddelade domstol totalt 631 tillstånd om hemlig teleavlyssning. Av dessa avsåg 446 tillstånd narkotikarelaterad brottslighet (grovt narkotikabrott och grov narkotikasmuggling). I övriga fall var det fråga om förundersökningar rörande främst mord och grova rån. I enstaka fall rörde förundersökningarna människorov, grov mordbrand, allmänfarlig ödeläggelse, grov penningförfalskning, grov våldtäkt och människohandel för sexuella ändamål. Den tid den totala avlyssningen pågick varierade kraftigt, från en dag till nästan åtta månader. Avlyssningen hade betydelse för förundersökningen beträffande den misstänkte i 46 procent av fallen under året. I 14 procent av fallen kunde avlyssning inte ske i önskad omfattning på grund av t.ex. tekniska problem, att den misstänkte reste utomlands, abonnemanget upphörde eller den misstänkte greps för annat brott. I sex procent av fallen kunde ingripande ske endast mot andra än den misstänkte. I drygt 33 procent av fallen lades förundersökningen ned på grund av att brott inte kunde styrkas. Under året förekom det i sex fall att ansökan om hemlig teleavlyssning avslogs av domstol och i tolv fall meddelades tillstånd efter begäran om rättslig hjälp från annat land.

Det lämnades tillstånd i 645 fall under år 2003 till hemlig teleövervakning. I så gott som samtliga fall där hemlig teleavlyssning beviljades meddelades tillstånd även till hemlig teleövervakning. Av tillstånden till hemlig teleövervakning avsåg 450 fall grovt narkotikabrott eller grov narkotikasmuggling. De övriga fallen avsåg främst förundersökningar rörande mord, grovt rån, människorov, grov mordbrand, allmänfarlig ödeläggelse, grov penningförfalskning, grov våldtäkt, människohandel för sexuella ändamål, grovt barnpornografibrott, grov varusmuggling, grov stöld, grovt bedrägeri, grovt penninghäleri, grov urkundsförfalskning, grovt bokföringsbrott, grovt skattebrott och grovt miljöbrott. Liksom för hemlig teleavlyssning varierade den totala övervakningstiden från

en dag till nästan åtta månader. Övervakningen hade betydelse för förundersökningen i knappt 46 procent av fallen. I 14 procent av fallen avbröts övervakningen i förtid på grund av t.ex. tekniska problem, att den misstänkte reste utomlands, abonnemanget upphörde eller den misstänkte greps för annat brott. I sex procent av fallen kunde tillslag ske endast mot andra än den misstänkte. I knappt 34 procent av fallen lades förundersökningen ned på grund av att brott inte kunde styrkas. Under året förekom det i sju fall att ansökan om hemlig teleövervakning avslogs av domstol och i tolv fall meddelades tillstånd efter begäran om rättslig hjälp från annat land.

Av regeringens slutsatser i skrivelsen framgår att tvångsmedlen användes främst vid förundersökningar där det funnits misstankar om organiserad eller annars omfattande narkotikabrottslighet där huvudsyftet med åtgärderna var att avslöja den mera omfattande narkotikasmugglingen till Sverige och narkotikaförsäljningen inom landet. Regeringen kommenterade också det något ökade antalet tillståndsärenden och angav då att den omständigheten berodde på att polisen hade fått bättre tekniska möjligheter till avlyssning och kan avlyssna nya typer av telefoner. Regeringen påpekade också att den grova brottsligheten i dag har en mer organiserad struktur, att det är vanligt att större grupperingar, ofta med internationella förgreningar, deltar i planeringen och utförandet av brott och att detta medför att ett stort antal tillstånd kan komma att meddelas inom ramen för en och samma förundersökning.

3 Rättegångsbalkens terminologi

3.1 Sammanfattning av bedömningar och förslag

– Terminologin i bestämmelserna som rör hemlig teleavlyssning och hemlig teleövervakning behöver anpassas till ny lagstiftning och moderniseras.
– Två grundläggande utgångspunkter bör då vara dels att skilda lösningar för olika typer av elektronisk kommunikation skall undvikas, dels att regleringen i största möjliga utsträckning skall göras oberoende av den snabba tekniska utvecklingen och alltså kunna stå sig över tiden.
– Begreppet telemeddelande skall mönstras ut ur lagtexten och ersättas med begreppet meddelande.
– Det meddelande som skall avlyssnas eller övervakas skall befordras eller ha befordrats i ett elektroniskt kommunikationsnät. Begreppet elektroniskt kommunikationsnät skall ha samma innebörd som i lagen om elektronisk kommunikation, med den inskränkningen att det inte skall avse sådant nät som enbart är avsett för utsändning av program i ljudradio eller television.
– Begreppet teleadress skall mönstras ut ur lagtexten. I stället skall bestämmelserna anknytas till begreppet tekniskt hjälpmedel.
– Begreppen hemlig teleavlyssning och hemlig teleövervakning skall mönstras ut ur lagtexten.

3.2 Utgångspunkter för en översyn av rättegångsbalkens terminologi

Bedömning: Terminologin i bestämmelserna som rör hemlig teleavlyssning och hemlig teleövervakning behöver anpassas till ny lagstiftning och moderniseras.

Två grundläggande utgångspunkter bör då vara dels att skilda lösningar för olika typer av elektronisk kommunikation skall undvikas, dels att regleringen i största möjliga utsträckning skall göras oberoende av den snabba tekniska utvecklingen och alltså kunna stå sig över tiden.

Av våra direktiv (Dir. 2003:145, se *bilaga 2*) framgår att det i översynen av regelverket som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation ingår att överväga en anpassning och modernisering av rättegångsbalkens terminologi. Målsättningen för vårt arbete skall enligt direktiven vara att skapa en enhetlig reglering som, särskilt med hänsyn till den snabba tekniska utvecklingen, kan stå sig över tiden.

Lagen om elektronisk kommunikation ersatte i juli 2003 telelagen och lagen om radiokommunikation. I den nya lagen genomfördes flera EG-direktiv. Begreppet elektronisk kommunikation är inte definierat i lagstiftningen men med begreppet bör enligt förarbetena menas överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier (prop. 2002/03:110 s. 111). Tillämpningsområdet för lagen om elektronisk kommunikation är vidare än telelagens (jfr prop. 2002/03:110 s. 113). Elektronisk kommunikation omfattar telefoni och datakommunikation men till skillnad från telelagen även utsändningar till allmänheten genom radio och TV.

Bestämmelser om telefonavlyssning har sedan rättegångsbalkens ikraftträdande år 1948 funnits i balken. Terminologin när det gäller hemlig teleavlyssning och hemlig teleövervakning är i dagsläget i mångt och mycket anknuten till den numera upphävda telelagens begrepp och uttryckssätt. Det rör exempelvis uttrycken hemlig teleavlyssning (rubriken till 27 kap. RB och 27 kap. 18, 20-26 och 28 §§ RB), hemlig teleövervakning (27 kap. 19-21, 23 och 25 §§ RB), telemeddelande (27 kap. 18-20 och 22 §§ RB), telefonnummer, kod och teleadress (27 kap. 18-21 §§ RB), telefonsamtal (27 kap. 22 § RB) och telenät (27 kap. 20-21 §§ RB). En del av begreppen finns även i andra författningar.

Bl.a. mot bakgrund av att tillämpningsområdet för lagen om elektronisk kommunikation är vidare än telelagens, har de begrepp som tidigare fanns i telelagen i princip inte förts över till lagen om elektronisk kommunikation. I den senare lagen finns i stället andra begrepp som inte korresponderar mot telelagens eller rättegångsbalkens. Det är med andra ord uppenbart att det bl.a. som en följd av att telelagen har upphävts och ersatts av lagen om elektronisk kommunikation behöver ske en anpassning och modernisering av terminologin.

E-komutredningen konstaterade att lagen om elektronisk kommunikation rör ett mycket dynamiskt område där utvecklingen av ny teknik för elektronisk överföring och för elektronisk kommunikation går med rasande fart. Utredningen uttalade också att det är svårt att se vad som kommer att hända längre fram i tiden än något år och att det finns en risk för en utveckling som innebär att reglerna inte till fullo korresponderar med den nya teknik som växer fram om de görs allt för konkreta (SOU 2002:60 s. 286).

Vi har inte underlag för att göra någon annan bedömning än den som e-komutredningen gjorde. Att binda tvångsmedelsreglerna till vissa typer av kommunikation eller vissa typer av teknik är direkt olämpligt. I stället bör man så långt som möjligt bygga vidare på nuvarande regler. Två grundläggande utgångspunkter även i vårt arbete måste därför vara dels att skilda lösningar för olika typer av elektronisk kommunikation skall undvikas, dels att regleringen om tillgång till elektronisk kommunikation i brottsbekämpningen i största möjliga utsträckning skall göras oberoende av den snabba tekniska utvecklingen. Regleringen skall med andra ord kunna stå sig över tiden. Det kräver att bestämmelserna ges en något mer generell utformning i jämförelse med dagens regler för att inte riskera att dessa snabbt blir överspelade av utvecklingen, samtidigt som avsikten med ändringarna i det avseendet inte skall vara att i dagsläget utvidga tillämpningsområdet. Det främjar varken effektiviteten eller rättssäkerheten i brottsutredningsverksamheten att regler på tvångsmedelsområdet, kanske kort tid efter ikraftträdandet, får en oklar innebörd som en följd av den tekniska utvecklingen på området.

Bestämmelserna i 27 kap. 18 och 19 §§ RB kan sägas innefatta definitioner av hemlig teleavlyssning och hemlig teleövervakning. Paragrafernas första stycken har följande lydelser.

> Hemlig teleavlyssning innebär att telemeddelanden, som befordras eller har befordrats till eller från ett telefonnummer,

en kod eller annan teleadress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.

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.

Som framgår finns vissa grundläggande begrepp i bestämmelserna som mot bakgrund av vad vi nyss har sagt behöver förändras. Det rör framför allt telemeddelande, telefonnummer, kod, teleadress men även begreppen teleavlyssning och teleövervakning. Målsättningen skall vara att skapa regler som i så stor utsträckning som möjligt är oberoende av den tekniska utvecklingen samtidigt som reglerna också skall vara teknikneutrala i den bemärkelsen att tvångsmedlen måste omfatta meddelanden som förmedlas med många typer av tekniska hjälpmedel. Tvångsmedlen skall med andra ord kunna tillämpas oavsett om det är fråga om t.ex. telefon, telefax, e-posttrafik eller Internet.

3.3 Begreppet telemeddelande

Förslag: Begreppet telemeddelande skall mönstras ut ur lagtexten och ersättas med begreppet meddelande.

I 1 § telelagen definierades telemeddelande som ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskild anordnad ledare. I stort sett all information som går genom ett s.k. elektroniskt kommunikationsnät utgör telemeddelanden enligt den definitionen. I prop. 1992/93:200 (s. 301) anges att begreppet telemeddelande innefattar att det är någon form av information som överförs. Där sägs också att överföringsmedium kan bestå av radiovågor och i ljus eller elektromagnetiska svängningar, varvid särskilt anordnad ledare används. Det sistnämnda innebär att mobiltelefoni som förmedlas endast med radio i och för sig anses som telemeddelande.

Genom att telemeddelande definieras på det sättet är det alltså möjligt att enligt 27 kap. 18-19 §§ RB avlyssna respektive övervaka telefon- och telefaxtrafik, e-posttrafik, överföring av datafiler med

hjälp av t.ex. FTP (File Transport Protocol), liksom överföring från hemsidor, nyhetsgrupper och chatkanaler.

Även straffbestämmelsen i 4 kap. 8 § BrB om brytande av telehemlighet utgår från begreppet telemeddelande. I paragrafen anges att det är straffbart att olovligen bereda sig tillgång till ett telemeddelande som förmedlas. Det kan då i och för sig vara svårt att förstå den slutsats som anges t.ex. i lagrådsremissen den 6 april 2000 rörande Buggningsutredningens förslag (s. 29), att det inte är straffbart att lyssna på telemeddelanden som befordras endast med radio, t.ex. mobiltelefoni som inte sker via kabel. Tolkad efter ordalydelsen omfattar 4 kap. 8 § BrB nämligen även avlyssning av telemeddelanden som överförs på det sättet. Vid brottsbalkens tillkomst utgick man dock från att straffbudet inte omfattade meddelanden som befordrades via radio. Av förarbetena framgår att det inte synes ha varit statsmakternas avsikt att vid införandet av telelagen utsträcka tillämpningsområdet för 4 kap. 8 § BrB till att också omfatta radiobefordrade telemeddelanden (prop. 1992/93:200 s. 166 f.). Avlyssning av telemeddelanden som befordras via radio torde således inte vara straffbart som brytande av telehemlighet. I 6 kap. 23 § LEK finns dock ett straffsanktionerat förbud (7 kap. 15 § LEK) för den som i radiomottagare har avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett radiobefordrat meddelande, som inte är avsett för honom själv eller för allmänheten, att obehörigen föra det vidare (se SOU 1998:46 s. 55).

I förarbetena till lagen om elektronisk kommunikation anges följande när det gäller begreppet telemeddelande (prop. 2002/03:110 s. 269).

> I bl.a. 4 kap. brottsbalken och 27 kap. rättegångsbalken används begreppet telemeddelande. I telelagen finns en definition av detta begrepp. Med telemeddelande avses därvid ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare. Begreppet används inte i EG:s regelverk för elektronisk kommunikation och skulle därför inte behövas i övrigt i lagen om elektronisk kommunikation. Som framgår av avsnitt 19.2 föreslås ett särskilt begrepp, elektroniskt meddelande, med avseende på bestämmelserna om integritetsskydd. I avvaktan på sådan ytterligare utredning som nämnts ovan anser regeringen att det, för att inte skapa rättsosäkerhet i fråga om tillämpningen av de författningar som innehåller begreppet telemeddelande, är

> lämpligt att såsom en övergångslösning använda detta begrepp även i den nya lagen såvitt avser anpassningsskyldigheten. Begreppet bör också definieras i bestämmelsen i enlighet med vad som anges i telelagen.

I lagen om elektronisk kommunikation används inte begreppet telemeddelande annat än att begreppet definieras i 6 kap. 19 § tredje stycket i enlighet med telelagens definition, som en övergångslösning i avvaktan på våra förslag.

Det är inte lämpligt att ha kvar begreppet telemeddelande i rättegångsbalken. Frågan blir då om begreppet elektroniskt meddelande kan användas i stället.

I lagen om elektronisk kommunikation används begreppet elektroniskt meddelande med avseende på bestämmelserna om integritetsskydd. Elektroniskt meddelande definieras i 6 kap. 1 § LEK som all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och TV-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om denna information inte kan sättas i samband med den enskilde abonnenten eller användaren av informationen.

I prop. 2002/03:110 (s. 389) anges något om bakgrunden till och innebörden av begreppet elektroniskt meddelande. Där sägs bl.a. följande.

> Definitionen av elektroniskt meddelande motsvarar definitionen för "kommunikation" i artikel 2 i direktivet om integritet och elektronisk kommunikation. En annan term har valts för att undvika sammanblandning med elektronisk kommunikation som ingår i andra definitioner. Definitionen av elektroniskt meddelande är sådan att den bara kan gälla för 6 kap. Den gäller nämligen bara information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Elektroniskt meddelande omfattar vidare information som överförs som del av en sändningstjänst för ljudradio eller TV till allmänheten via ett elektroniskt kommunikationsnät endast om informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen. Ett exempel kan vara betal-TV-tjänster. Även tjänster med villkorad tillgång kan falla in under definitionen på grund av att åtkomstkon-

trollen medger identifiering av abonnenten. En ytterligare förutsättning för att det skall vara fråga om ett elektroniskt meddelande är dock att den överförda informationen kan sättas i samband med abonnemanget.

Begreppet elektroniskt meddelande omfattar alltså bl.a. information som överförs som en del av sändningstjänst för ljudradio eller TV till allmänheten, om informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen. Ett exempel kan vara betal-TV-tjänster.

Begreppet användare i 6 kap. LEK är inskränkt till användare som är fysisk person (prop. 2002/03:110 s. 250). Dessutom knyter definitionen av elektroniskt meddelande an till en allmänt tillgänglig elektronisk kommunikationstjänst, alltså till en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (1 kap. 7 § LEK). I avsnitt 3.4.3 tar vi upp begreppet allmänt kommunikationsnät och utvecklar i samband därmed de begränsningar som begreppet elektronisk kommunikationstjänst innefattar i förhållande till de aktuella tvångsmedelsbestämmelserna.

Det går att konstatera att begreppet telemeddelande inte är möjligt att byta ut mot elektroniskt meddelande i rättegångsbalken. Bestämmelserna i 27 kap. 18 och 19 §§ RB utgår från avlyssning eller övervakning av information vid överföring av denna. Enligt vår mening bör det som får avlyssnas respektive övervakas enligt bestämmelserna anges med det teknikneutrala begreppet meddelande. För att avgränsa de meddelanden som omfattas av tvångsmedlen och för att på så sätt även avgränsa tvångsmedlen i sig, bör det i bestämmelserna anges var meddelandet får avlyssnas eller övervakas. Frågan blir då vilken typ av nät som bör avses.

3.4 Begreppet telenät

Förslag: Det meddelande som skall avlyssnas eller övervakas skall befordras eller ha befordrats i ett elektroniskt kommunikationsnät. Begreppet elektroniskt kommunikationsnät skall ha samma innebörd som i lagen om elektronisk kommunikation, med den inskränkningen att det inte skall avse sådant nät som enbart är avsett för utsändning av program i ljudradio eller television.

3.4.1 Telenät

Enligt 27 kap. 20 § andra stycket RB får hemlig teleavlyssning och hemlig teleövervakning 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. Därmed avses bl.a. system för snabbtelefoner, porttelefoner, PC-nät och liknande utrustning inom eller intill en bostad, hörslingor för hörselskadade eller interna system för personsökning i form av fasta installationer. Även interna telekommunikationer på mindre arbetsplatser via t.ex. PC-nät utgör telenät av mindre betydelse. Motsatsen gäller vanligtvis beträffande sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät eller större företagsnät. Detsamma gäller fristående datorer som är försedda med modem och datorer i t.ex. små interna nätverk som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem. Om kommunikationen endast sker internt inom ett slutet nät bör det krävas att nätet är av större omfattning för att en tvångsåtgärd skall få äga rum. Frågan om ett telenät skall anses vara av mindre betydelse prövas utifrån en samlad bedömning av de olika omständigheter som rör ett telenäts betydelse från allmän kommunikationssynpunkt. Då kan bl.a. antalet anslutningar, geografisk spridning och hur utrustningen fungerar och används ha betydelse (prop. 1994/95:227 s. 27 och 31 och Fitger, Rättegångsbalken 2 s. 27:41).

I domstolens tillstånd till åtgärden skall det enligt 27 kap. 21 § tredje stycket RB särskilt anges om tvångsmedlet får verkställas utanför ett allmänt tillgängligt telenät.

I telelagen användes begreppet allmänt tillgängligt telenät i en mängd bestämmelser. I den lagrådsremiss som föregick telelagen fanns en definition av det begreppet. Efter Lagrådets yttrande utgick emellertid definitionen ur lagförslaget såsom inte erforderligt. Detta skall enligt propositionen om en telelag och en förändrad verksamhetsform för Televerket, m.m. (prop. 1992/93:200 s. 302) ses mot bakgrund av de svårigheter som med hänsyn till regleringen inom EG finns att skapa en sådan svensk definition. Däremot definierades begreppet telenät som anläggning som är avsedd för förmedling av telemeddelanden (1 § telelagen). Det anges dock i telelagens förarbeten att ett kännetecken på att ett telenät är allmänt tillgängligt bör vara att det står öppet för en vid krets av an-

vändare att ansluta sig till nätet (prop. 1992/93:200 särskilt s. 88, 91 f. och 99).

Begreppet allmän kommunikationssynpunkt användes inte i telelagen.

Det är en självklar utgångspunkt att tvångsmedlen även i fortsättningen skall träffa enbart meddelanden som befordras eller har befordrats i nät. Vi har kommit fram till att det är lämpligt att detta anges i 27 kap. 18 och 19 §§ RB. Frågan blir då vilken typ av nät som bestämmelserna skall ta sikte på.

I lagen om elektronisk kommunikation definieras tre olika nät, nämligen elektroniskt kommunikationsnät, allmänt telefonnät och allmänt kommunikationsnät. Av definitionerna framgår att elektroniskt kommunikationsnät är det ”överordnade” begreppet medan de två övriga näten är olika typer av elektroniska kommunikationsnät. Vid en bedömning av om något av dessa begrepp kan användas i bestämmelserna i rättegångsbalken måste följande beaktas.

3.4.2 Allmänt telefonnät

Allmänt telefonnät definieras i lagen om elektronisk kommunikation som ett elektroniskt kommunikationsnät som används för att tillhandahålla allmänt tillgängliga telefonitjänster och som möjliggör överföring av tal, telefaxmeddelanden, datakommunikation och andra former av kommunikation mellan nätanslutningspunkter. *Telefonitjänst* definieras i sin tur som en elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan, inklusive nödsamtal. Begreppet telefonitjänst utgår från samtal, som i sin tur definieras som en förbindelse för överföring av tal som medger tvåvägskommunikation i vad som av användaren uppfattas som realtid (1 kap. 7 § LEK).

Allmänt telefonnät är med andra ord nät som typiskt sett är anpassade för överföring av tal. I förarbetena anges att det kan vara flera faktorer som tillsammans gör att denna förutsättning är uppfylld. Såväl det fysiska nätet som den logiska uppbyggnaden avgör om ett nät betraktas som ett allmänt telefonnät. Även överföringskapaciteten i en förbindelse och möjlighet att få tillgång till alarmerings- och räddningstjänst är sådana faktorer (prop. 2002/03:110 s. 357 f.).

Mot bakgrund av att allmänt telefonnät och telefonitjänst tar sikte just på samtal skulle en användning av det förstnämnda be-

greppet i 27 kap. RB kunna innebära en inskränkning i tvångsmedlens tillämpningsområde. Bl.a. skulle det inte längre vara självklart att tillämpningsområdet omfattar vissa former av IP-telefoni (jfr prop. 2002/03:110 s. 270 och 357 ff.). Det är således olämpligt att knyta tvångsmedlen till meddelanden som befordras eller har befordrats i allmänna telefonnät.

3.4.3 Allmänt kommunikationsnät

I lagen om elektronisk kommunikation används även begreppet *allmänt kommunikationsnät*. Det är då fråga om ett elektroniskt kommunikationsnät som huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster. *Elektroniska kommunikationstjänster* är tjänster som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (1 kap. 7 § LEK). För att avgöra om kommunikationsnätet är allmänt får enligt förarbetena (prop. 2002/03:110 s. 120) vägledning hämtas från telelagens begrepp ”allmänt tillgängligt”, dvs. det står öppet för en vid krets av användare att ansluta sig till nätet (prop. 1992/93:200 särskilt 88, 91 f. och 99).

Begreppet elektroniska kommunikationstjänster anges i förarbetena inte omfatta de av informationssamhällets tjänster som anges i artikel 1 i Europaparlamentets och rådets direktiv 98/34/EG om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, som inte helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (prop. 2002/03:110 s. 116 f.).

Vi har bedömt att inte heller begreppet allmänt kommunikationsnät är lämpligt att använda i rättegångsbalken. Begreppets innebörd är beroende av begreppet elektroniska kommunikationstjänster som i sin tur är avsett att urskilja sådana tjänster som innebär ett kommersiellt tillhandahållande av tjänster till andra. Sker tillhandahållandet på rent ideell basis omfattas däremot tjänsten inte av begreppet. Det framstår som att en del av den kommunikation som i dag kan omfattas av hemlig teleavlyssning och hemlig teleövervakning skulle, om begreppet allmänt kommunikationsnät användes för att avgränsa tvångsmedlen, kunna falla utanför tillämpningsområdet. Det gäller t.ex. vissa av de tjänster som tillhan-

dahålls på Internet (se prop. 2002/03:110 s. 95 och SOU 2002:60 s. 579).

3.4.4 Elektroniskt kommunikationsnät

Ett grundläggande begrepp i lagen om elektronisk kommunikation är *elektroniskt kommunikationsnät*. I 1 kap. 7 § LEK är elektroniskt kommunikationsnät definierat som system för överföring och i tilllämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs. Begreppet omfattar enligt förarbetena (prop. 2002/03:110 s. 357) alla typer av telenät enligt telelagens definition. Telelagens tillämpningsområde avsåg enligt 1 § telelagen televerksamhet och abonnentupplysning. Med televerksamhet avsågs enligt samma lagrum inte utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket första meningen yttrandefrihetsgrundlagen. Någon motsvarande begränsning finns inte i lagen om elektronisk kommunikation. Detta medför att utöver de nät som omfattas av telenät enligt telelagen omfattar elektroniskt kommunikationsnät även nät som används för utsändning av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen.

Yttrandefrihetsgrundlagen är tillämplig bl.a. på radio- och TV-sändningar samt på vissa andra överföringar av ljud, bild och text som sker med hjälp av elektromagnetiska vågor. I lagtexten används uttrycket radioprogram som sammanfattande beteckning på de olika typer av överföringar till allmänheten som nu avses. Gemensamt för dem alla är att överföringen sker med hjälp av elektromagnetiska vågor (1 kap. 1 § tredje stycket). Enligt yttrandefrihetsgrundlagens förarbeten (prop. 1990/91:64 s. 108) ingår i det sistnämnda uttrycket bl.a. överföringar av information till allmänheten genom telefax.

Enligt huvudregeln om radioprogram skall sändningar av programmen vara riktade till allmänheten och avsedda att tas emot med tekniska hjälpmedel för att omfattas av grundlagsskyddet (1 kap. 6 §). Det är således en förutsättning för grundlagens tillämplighet att det är fråga om radioprogram och att dessa är riktade till allmänheten, dvs. sändaren riktar sändningen av ett program till vem som helst som önskar ta emot den utan att denne begärt det

(SOU 2002:60 s. 204, prop. 1986/87:151 s. 164 och prop. 2002:03:110 s. 81). Tillhandahållandet av direktsända och inspelade program ur en databas (via Internet) inkluderas.

Gemensamt för de sändningar som enligt huvudregeln om radioprogram omfattas av yttrandefrihetsgrundlagen är alltså att de startas av sändaren och inte på beställning av mottagaren. Det innebär att sådan informationsförmedling som sker genom att den som önskar ta del av informationen själv tar kontakt med informationsförmedlaren och begär viss information som regel inte omfattas av yttrandefrihetsgrundlagen.

Viss användning av interaktiva medier, dvs. sådana där både sändare och mottagare kan påverka sändningen, skyddas dock genom den s.k. databasregeln (1 kap. 9 §). Enligt denna är yttrandefrihetsgrundlagen även tillämplig när tidningsredaktioner, nyhetsbyråer och andra särskilt angivna massmedieföretag på särskild begäran tillhandahåller allmänheten upplysningar direkt ur en databas vars innehåll kan ändras endast av den som driver verksamheten. Sedan den 1 januari 2003 är grundlagsskyddet enligt databasregeln utvidgat till att gälla vissa nya tekniker, bland annat s.k. print on demand, som innebär framställning på kundens begäran av enstaka exemplar av skrifter, bilder och upptagningar genom överföring av information ur en databas. Dessutom har till gruppen massmedieföretag lagts företag för yrkesmässig framställning av tryckta och därmed jämställda skrifter, t.ex. bokförlag och tryckerier. Sådana företag erhåller därmed automatiskt grundlagsskydd för samma användning av databaser som tidigare nämnda massmedieföretag. Därutöver kan numera andra aktörer än massmedieföretag få ett frivilligt grundlagsskydd för motsvarande verksamheter. Fysiska och juridiska personer som yttrar sig via Internet kan på frivillig väg omfattas av grundlagsbestämmelserna. Detta fordrar att en ansvarig utgivare utsetts samt att utgivningsbevis beviljats efter ansökan.

Internet kan användas på olika sätt och för olika ändamål. Olika användningar måste från grundlagsskyddssynpunkt ses och bedömas för sig. Om innehållet i en tryckt periodisk skrift helt eller delvis återges även på Internet kan den vara grundlagsskyddad enligt den s.k. bilageregeln i 1 kap. 7 § andra stycket tryckfrihetsförordningen. Elektroniska tidningar som publiceras på nätet kan alltså under vissa förutsättningar skyddas av antingen databasregeln eller bilageregeln. Om sändningar av ljudradio sker i realtid över Internet kan de vara grundlagsskyddade enligt yttrandefrihetsgrundlagens huvudregel om radioprogram.

Vi kom tidigare fram till att det skulle kunna innebära begränsningar av det nuvarande tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning om begreppen allmänt telefonnät eller allmänt kommunikationsnät användes i rättegångsbalken för att beskriva det nät inom vilka de meddelanden befordras som kan bli föremål för tvångsmedlen. Frågan blir då om det mer överordnade begreppet elektroniskt kommunikationsnät kan användas i stället.

Som har framgått tidigare är tillämpningsområdet för lagen om elektronisk kommunikation vidare än telelagens, bl.a. genom att det omfattar utsändningar till allmänheten genom radio och TV. Begreppet elektroniskt kommunikationsnät är det överordnade, samlade begreppet, som omfattar både telenät enligt telelagen och sådana nät som används för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen. Enligt vår mening är det inte ändamålsenligt att för tvångsmedelsregleringen skapa ett nytt begrepp rörande nät vid sidan av de som förekommer i lagen om elektronisk kommunikation. I stället är det lämpligt att använda sig av elektroniskt kommunikationsnät i den betydelse begreppet har i lagen om elektronisk kommunikation men samtidigt föreskriva begränsningar rörande vissa typer av sådana nät.

En begränsning som innebär att tvångsmedlen blev tillämpliga på meddelanden i elektroniska kommunikationsnät med undantag av de nät som används för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen skulle medföra en inskränkning i tillämpningsområdet i förhållande till dagens regler. Som framgick ovan omfattas t.ex. viss telefaxtrafik och viss användning av Internet i de utsändningar som avses i yttrandefrihetsgrundlagen. Även i fortsättningen måste exempelvis telefaxtrafik och överföringar från hemsidor omfattas av tvångsmedlen.

Vad som däremot i princip inte behöver omfattas av tillämpningsområdet är nät som är avsedda för utsändning till allmänheten av program i ljudradio eller television. Problemet är dock att samma nät samtidigt kan användas för exempelvis telefoni, Internet och interaktiva teletjänster. Vi har därför kommit fram till att de nät som bör avses i tvångsmedelsbestämmelserna är elektroniska kommunikationsnät med undantag för nät som *enbart* är avsett för utsändning av program i ljudradio eller television.

Även i fortsättningen bör det finnas en begränsning som motsvarar bestämmelsen i 27 kap. 20 § andra stycket RB, dvs. avlyss-

ning eller övervakning skall inte få avse meddelanden som befordras eller har befordrats i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt. Dessutom skall det i tillståndet anges om avlyssningen eller övervakningen får verkställas utanför ett allmänt tillgängligt elektroniskt kommunikationsnät (27 kap. 21 § tredje stycket RB).

3.5 Begreppet teleadress

Förslag: Begreppet teleadress skall mönstras ut ur lagtexten. I stället skall bestämmelserna anknytas till begreppet tekniskt hjälpmedel.

I rättegångsbalken används begreppet teleadress som en gemensam beteckning för olika identifieringsmetoder. Med teleadress avses en identifiering av den icke fysiska adress som ett telemeddelande skickas till eller från, t.ex. ett abonnemang, en enskild anknytning, adressen för elektronisk post, en kod eller någon annan motsvarande tillförlitlig identifieringsmetod. Begreppet teleadress användes tidigare även i 50 § telelagen, som reglerade undantag från skyldigheten att utplåna eller avidentifiera uppgifter om telemeddelanden.

I lagstiftningen fanns tidigare begreppet teleanläggning. Den 1 januari 1996 ersattes det begreppet med teleadress i rättegångsbalken. Regeringen uttalade då följande om den tekniska utvecklingen som bakgrund till förslaget (prop. 1994/95:227 s. 18).

> Utvecklingen på teleområdet har inneburit att de beskrivna närmast fysiska avgränsningarna som bygger på teleanläggningar och telenät inte kan tillämpas konsekvent. Ett samband mellan den misstänkte och viss plats, ledning och telefon var tidigare en naturlig och närmast självklar utgångspunkt för en tydlig avgränsning av tvångsmedlen på teleområdet. Nya IT-baserade rutiner har emellertid fört med sig att förutsättningarna förändrats. Numera kan det vanligtvis inte förutsägas vilken typ av teleanläggning – telefax, telefon, modem, etc. – som ansluts till en viss telelinje. Kombinationer har blivit vanliga, t.ex. att telefon, telefax och telefonsvarare ansluts till samma abonnentledning. Vidare har sambandet mellan abonnentnummer och abonnentledning delvis

suddats ut. Telemeddelanden kan t.ex. kopplas vidare och flyttas med. Sådana omdirigeringar av telemeddelanden sker redan i teleoperatörens växel så att telemeddelandena aldrig når ursprungligen avsedd abonnentledning. Andra exempel på frikoppling från viss teleanläggning kan hämtas från mobil telefoni och moderna företagsväxlar. Alla telemeddelanden till ett visst mobilteleabonnemang styrs direkt i teleoperatörens växel till den radiosändare inom vilkens räckvidd mottagaren befinner sig. Är abonnemanget GSM-baserat kan valfri telefon användas under förutsättning att den har försetts med mottagarens personliga kort. På motsvarande sätt ger vissa televäxlar möjligheter att – efter en indikation via t.ex. personsökare – ta emot ett samtal vid den fysiska anknytning där mottagaren för tillfället befinner sig. Mottagaren anger en kod genom vilken meddelandet dirigeras till den aktuella telefonapparaten. Ett annat exempel där t.ex. telefonapparater inte fysiskt knyts till viss plats är televäxlar som nu börjat marknadsföras vilka knyter telefonapparaten till televäxeln via radiokommunikation.

En fysisk gränsdragning i de nu beskrivna fallen medför närmast slumpvis att vissa, men inte andra, av de telemeddelanden som befordras via televäxeln till eller från den misstänkte kan tas upp. Traditionella gränser har i allt högre grad suddats ut och vedertagna rutiner för att knyta telemeddelanden till viss teleanläggning har ersatts av flexibla IT-baserade rutiner som inte är beroende av vilken telefonapparat, telelinje eller annan teleanläggning som används i det enskilda fallet. Följden blir – som på andra områden där IT-rutiner genomförs och de traditionella, närmast fysiska avgränsningarna faller bort – att kvar finns endast sådana avgränsningar som följer av ändamål, funktioner och tekniska strukturer som byggs upp.

I bestämmelsen om hemlig teleavlyssning i 27 kap. 18 § RB används begreppen telefonnummer, kod eller annan teleadress. Det sistnämnda begreppet används också vid hemlig teleövervakning enligt 27 kap. 19 § RB. Begreppet är inte definierat i lagstiftningen. Hemlig teleavlyssning och hemlig teleövervakning får ske endast om någon är skäligen misstänkt för brott av viss svårhetsgrad. Beslutet får bara avse 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. Exempel

på det sistnämnda kan beroende på omständigheterna vara en teleadress som innehas av en sambo till en misstänkt, en teleadress på den misstänktes arbetsplats eller teleadressen till en telefonkiosk som den misstänkte regelbundet använder. 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 (27 kap. 20 § första stycket RB).

De beslut om hemlig teleavlyssning och hemlig teleövervakning som domstolarna fattar begränsas med andra ord dels till en namngiven skäligen misstänkt person, dels till vissa klart angivna teleadresser.

Åklagare och polis har påtalat vissa oklarheter rörande innebörden av begreppet teleadress. En typ av uppgifter som kan erhållas vid hemlig teleövervakning är det s.k. IMEI-numret (International Mobile Equipment Identification). Som namnet antyder rör det sig om ett unikt nummer som identifierar utrustningen eller hårdvaran, exempelvis själva mobiltelefonen. Det har sagts att domstolarnas bedömning varierar över landet i frågan om IMEI-numret skall anses vara en teleadress eller inte.

Från åklagar- och polishåll har vi också fått beskrivningar av de effektivitetsförluster som uppkommer i det brottsutredande arbetet genom att tvångsmedlen i varje enskilt fall behöver knytas till en klart angiven identifierad teleadress (se även slutrapporten från juni 2004 ”Organiserad kriminalitet, grov narkotikabrottslighet” av den nationella narkotikapolitiska samordningen Mobilisering mot narkotika, S 2002:03, s. 96).

Vi återkommer i avsnitt 4.5 till det mycket stora problemet för de brottsutredande myndigheterna att identifiera vissa teleadresser och i avsnitt 4.3 till frågan om domstolens beslut skall ange särskilt identifierade adresser. Redan här skall dock sägas att det i dagsläget är mycket vanligt att mobiltelefoner på olika sätt används vid brottslig verksamhet. Det är då i princip uteslutande fråga om s.k. anonyma kontantkort, där teleadresserna är okända för de brottsutredande myndigheterna, vilket innebär att tvångsmedlen heller inte kan verkställas. De kriminella personerna försvårar också myndigheternas arbete genom att ständigt byta kontantkort och mobiltelefoner. Därigenom byts även teleadressen.

Teleadress finns inte definierat i lagstiftningen. Förutom i rättegångsbalken fanns begreppet tidigare i 50 § telelagen, som reglerade undantag från skyldigheten att i televerksamhet utplåna eller avidentifiera uppgifter som telemeddelanden. Begreppet är förknippat

med den terminologi som användes i telelagen och som numera saknar motsvarighet i lagen om elektronisk kommunikation. Vi menar att i den anpassning och modernisering av bestämmelserna som skall ske bör begreppet teleadress mönstras ut ur rättegångsbalken. Tvångsmedelsbestämmelserna bör alltså inte innehålla uttrycket teleadress.

Begreppet teleadress är grundläggande för många av bestämmelserna rörande hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken. Exempelvis anges som sagt i 27 kap. 20 § första stycket RB att tvångsmedlen endast får avse teleadresser med viss närmare anknytning till den misstänkte, antingen så att teleadressen innehas/har innehafts av denne eller så att det finns synnerlig anledning att anta att den misstänkte kommer att kontakta/har kontaktat teleadressen. Det står därför enligt vår mening klart att teleadress behöver ersättas med något annat begrepp, inte minst för att göra lagstiftningen mer oberoende av den tekniska utvecklingen.

Vid övervägandena är det enligt vår mening även nödvändigt att beakta de mycket stora effektivitetsproblem som har påtalats från åklagare och polis och som bottnar i att tvångsmedlen behöver knytas inte enbart till den skäligen misstänkte personen utan även till vissa specifika teleadresser. Att kriminella, särskilt sådana personer som är inblandade i brott av organiserad eller annan allvarlig karaktär, har satt i system att byta SIM-kort och att byta mobiltelefoner har inget annat syfte än att försvåra utredning av brottsligheten och visar tydligt att myndigheternas svårigheter att snabbt anpassa tvångsmedelsanvändningen till den faktiska verkligheten utnyttjas i kriminella sammanhang. Detta framstår som ytterligt otillfredsställande.

I dagsläget skall domstolen i tillståndet till hemlig teleavlyssning och hemlig teleövervakning ange dels den skäligen misstänkte personen, dels de specifika teleadresser som tillståndet omfattar. Vad som är av intresse är emellertid inte en sådan metod för identifiering av en speciellt identifierad icke fysisk adress som teleadressen utgör, utan information om den misstänktes kommunikation som sådan, oavsett identifieringsmetoder för kommunikationen. Därför och mot bakgrund av vad som anges i avsnitt 4.3 och 4.5 bedömer vi, främst med tanke på effektiviteten i brottsbekämpningen, att knytningen av besluten till vissa i förväg angivna teleadresser eller liknande behöver göras mindre strikt och ersättas med knytning till annat begrepp.

För att sända eller ta emot meddelanden i ett elektroniskt kommunikationsnät används olika former av tekniska hjälpmedel som är konstruerade för just detta ändamål. Begreppet tekniskt hjälpmedel används också i 27 kap. 25 § första stycket RB, som anger att myndigheterna får använda de tekniska hjälpmedel som behövs när domstolen har lämnat tillstånd till hemlig teleavlyssning respektive hemlig teleövervakning och är således introducerat inom det rättsområde som nu är föremål för överväganden. Begreppet är teknikneutralt och kan avse exempelvis fast telefon, mobiltelefon, telefax, modem, Internetterminal och mjukvara utan att tillämpningsområdet samtidigt är begränsat till dessa hjälpmedel.

Det är lämpligt att anknyta rätten till avlyssning och övervakning till detta begrepp, som bör ha samma innebörd som enligt bestämmelsen i 27 kap. 25 § första stycket RB. Rätten till avlyssning och övervakning bör alltså anknytas till tekniskt hjälpmedel som används, har använts eller kan förväntas bli använda av den misstänkte eller, i förekommande fall, kan förväntas ha anknytning till brottet innan någon misstänkt har identifierats (se avsnitt 4.3).

När tekniska hjälpmedel är avsedda att användas av dem som deltar i en kommunikation för att sända eller ta emot ett meddelande brukar hjälpmedlet benämnas terminalutrustning eller slutanvändarutrustning. Sådan utrustning kan också användas för avlyssning. Regler om terminalutrustning finns i lagen (2000:121) om radio- och teleterminalutrustning. Det bör särskilt observeras att begreppet tekniskt hjälpmedel är mer vidsträckt än begreppet terminalutrustning. Exempelvis ingår terminalutrustning definitionsmässigt inte i ett elektroniskt kommunikationsnät, utan ansluts till detta i en s.k. nätanslutningspunkt, vilken definitionsmässigt utgör nätets gräns mot användaren.

3.6 Begreppen hemlig teleavlyssning och hemlig teleövervakning m.m.

Förslag: Begreppen hemlig teleavlyssning och hemlig teleövervakning skall mönstras ut ur lagtexten.

Som framgått utgjorde telelagens tillämpningsområde enbart en del av tillämpningsområdet för lagen om elektronisk kommunikation. Som en följd av det och mot bakgrund av det behov som finns av en reglering som i största möjliga utsträckning är oberoende av den tekniska utvecklingen, har vi kommit fram till att de begrepp som

innehåller uttrycket tele i de aktuella tvångsmedelsbestämmelserna bör ersättas med andra begrepp. Då är det heller inte ändamålsenligt att benämna tvångsmedlen teleavlyssning respektive teleövervakning. Dessa begrepp bör alltså mönstras ut ur lagtexten. Enligt vår mening bör lagtexten utformas utan att nya särskilda benämningar på tvångsmedlen införs. Det är fullt tillräckligt att innebörden av och förutsättningarna för åtgärderna beskrivs där. Detta hindrar inte att begreppen avlyssning respektive övervakning används i andra författningar som hänvisar till tvångsmedlen i 27 kap. 18 eller 19 § RB.

Vi vill samtidigt för tydlighetens skull påpeka att det finns en mängd författningar som innehåller begreppet tele i någon form, t.ex. televerksamhet, telenät, telefonsamtal, telefonnummer, teleoperatör och telebefordringsföretag. Författningarna ändrades inte i samband med att lagen om elektronisk kommunikation trädde i kraft och telelagen upphörde att gälla. Flera av begreppen kommer säkert att mönstras ut ur lagtexten efter hand. Det ankommer inte på oss att utreda om några förändringar behövs av dessa begrepp i författningarna, annat än då det finns en direkt koppling till vårt arbete. Som exempel på det sistnämnda kan nämnas 9 kap. 8 § andra stycket sekretesslagen, som i samband med begreppet telemeddelande innehåller uttrycket ”myndighet som driver televerksamhet”.

4 En samlad reglering i rättegångsbalken

4.1 Sammanfattning av förslagen

– Bestämmelserna i 6 kap. 22 § första stycket 3 LEK och 14 kap. 2 § fjärde och femte styckena sekretesslagen som innebär skyldighet för operatörer att i vissa fall lämna ut uppgifter som angår ett särskilt elektroniskt meddelande respektive telemeddelande till brottsutredande myndighet skall upphävas. De brottsutredande myndigheternas tillgång till uppgifterna skall uteslutande regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning.
– Vid förundersökning angående brott som är så allvarliga att de kan ligga till grund för beslut om avlyssning, skall övervakning få användas även om det inte finns någon som är skäligen misstänkt för brottet.
– Någon motsvarighet till det krav som finns i dag på att det i ett beslut om hemlig teleavlyssning eller hemlig teleövervakning skall anges vilken teleadress tillståndet gäller skall inte finnas i lagtexten.
– I rättegångsbalken skall det införas en möjlighet för åklagare att i brådskande fall fatta interimistiska beslut i fråga om övervakning enligt 27 kap. 19 § RB. Beslutet skall genast skriftligen anmälas hos rätten, som skyndsamt skall pröva frågan.
– Av bestämmelserna om övervakning i rättegångsbalken skall det uttryckligen framgå att tvångsmedlet får användas för att hämta in uppgifter för lokalisering. Med uppgifter för lokalisering skall avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits (oavsett om det tekniska hjälpmedlet används eller har använts för samtal eller inte).

forts.

– Övervakning enligt 27 kap. 19 § RB skall i fortsättningen även innebära att uppgifter i hemlighet får hämtas in för identifiering av tekniska hjälpmedel. Med uppgifter för identifiering skall avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden.
– Övervakning i syfte att identifiera tekniska hjälpmedel skall få avse sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte.
– Har tillstånd givits till avlyssning skall även övervakningsuppgifter (uppgifter om meddelanden och för lokalisering eller identifiering av tekniska hjälpmedel) få hämtas in med stöd av tillståndet och meddelanden hindras från att nå fram till eller lämna ett visst tekniskt hjälpmedel.

4.2 Upphävande av vissa bestämmelser i lagen om elektronisk kommunikation och sekretesslagen

4.2.1 Nuvarande bestämmelser

Rättegångsbalken och lagen om elektronisk kommunikation

Sedan den 1 oktober 2004 innebär hemlig teleövervakning enligt 27 kap. 19 § RB att uppgifter i hemlighet hämtas in om telemeddelanden som befordras och som *har befordrats*. Det sistnämnda betyder att det numera är möjligt för de brottsutredande myndigheterna att få även historiska uppgifter vid hemlig teleövervakning, alltså inte enbart framtida uppgifter (uppgifter i s.k. realtid). Tidigare var de historiska uppgifterna möjliga att få enbart genom utlämnande från operatörerna enligt 47 § telelagen och sedermera 6 kap. 22 § LEK (jfr dock vad som sägs nedan om sekretesslagen).

I dagsläget är det alltså möjligt för de brottsutredande myndigheterna att få historiska uppgifter om telemeddelanden såväl enligt rättegångsbalkens regler om hemlig teleövervakning som genom utlämnande från operatörerna enligt 6 kap. 22 § första stycket 3 LEK.

De typer av uppgifter som myndigheterna erhåller är desamma i båda fallen. Däremot skiljer sig förutsättningarna för att få uppgifterna åt i några avseenden.

Vid *hemlig teleövervakning* krävs enligt 27 kap. 19-21 §§ RB

- ✓ att någon är *skäligen misstänkt* för brott,
- ✓ att det för brottet inte är föreskrivet lindrigare *straff* än fängelse i sex månader eller att det är fråga om dataintrång, barnpornografibrott som inte är att anse som ringa, narkotikabrott, narkotikasmuggling eller straffbara fall av försök, förberedelse eller stämplig till sådana brott,
- ✓ att åtgärden är av *synnerlig vikt* för utredningen,
- ✓ att åtgärden antingen avser 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 avser 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,
- ✓ att telemeddelandena inte befordras eller har befordrats endast inom *telenät* som får anses vara av mindre betydelse från allmän kommunikationssynpunkt, och
- ✓ att *domstolen*, på ansökan av *åklagaren*, ger tillstånd till åtgärden och anger bl.a. under vilken tid tillståndet avser, vilket får vara högst en månad för framtida uppgifter (för historiska uppgifter finns ingen bestämd gräns bakåt i tiden).

Detta skall jämföras med förutsättningarna för de brottsutredande myndigheterna att under förundersökning få historiska uppgifter som angår särskilda elektroniska meddelanden enligt *lagen om elektronisk kommunikation* (6 kap. 22 § första stycket 3). Det krav som ställs upp då är att det för brottet inte är föreskrivet lindrigare *straff* än fängelse i två år. Det innebär bl.a. att inga försöks- och förberedelsebrott omfattas av regleringen (23 kap. 1-2 §§ BrB).

Beträffande straffskalan ställer alltså lagen om elektronisk kommunikation strängare krav för tillgång till uppgifterna än rättegångsbalken vid hemlig teleövervakning. Däremot saknas krav på att det skall finnas en skäligen misstänkt person i förundersökningen och att åtgärden skall vara av synnerlig vikt för utredningen. I lagen om elektronisk kommunikation saknas också sådana be-

gränsningar som finns vid hemlig teleövervakning när det gäller vilka teleadresser och telenät som får omfattas av åtgärden. Dessutom är det inte domstolen som fattar beslut enligt lagen. Det är i stället tillräckligt med en begäran till operatören direkt från polis- eller åklagarmyndighet eller annan myndighet som skall ingripa mot brottet. Liksom för de historiska uppgifterna vid hemlig teleövervakning finns det ingen bestämd tidsgräns bakåt för hur gamla uppgifterna får vara vid utlämnande enligt lagen om elektronisk kommunikation. Skyldigheten för operatörerna att utplåna eller avidentifiera uppgifterna sätter dock i praktiken en gräns för vilka historiska uppgifter de brottsutredande myndigheterna erhåller såväl vid hemlig teleövervakning som enligt lagen om elektronisk kommunikation (6 kap. 5 § LEK). Givetvis har även anpassningsskyldigheten för operatörerna och skyldigheten att medverka betydelse för myndigheternas möjligheter att över huvud taget få tillgång till uppgifter och få besluten verkställda. Vi återkommer till de sistnämnda frågorna i avsnitt 6-8.

Sekretesslagen

I sekretesslagen finns bestämmelser som gäller för myndigheter som driver televerksamhet. Enligt 6 kap. 2 § tredje stycket LEK skall 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.

Buggningsutredningen uttalade att reglerna i sekretesslagen rörande tystnadsplikt för telemeddelanden i praktiken inte är tillämpliga sedan Televerket som myndighet upphörde att bedriva verksamhet (SOU 1998:46 s. 367 f.). I den lagrådsremiss som följde på Buggningsutredningens förslag anges att bestämmelserna för närvarande inte torde vara tillämpliga i något fall, då det sannolikt inte finns någon myndighet som driver televerksamhet (s. 32).

Vi har under vårt arbete fått uppgifter från PTS om att det finns kommuner som tillhandahåller IP-telefoni och att allting tyder på en ökning av sådan verksamhet hos myndigheter. Det kan också nämnas att tanken bakom det blivande nationella gemensamma radiokommunikationssystemet för skydd och säkerhet är, som vi har uppfattat det, att systemet skall drivas genom en myndighets försorg (se betänkandet Trygga medborgare – säker kommunikation, SOU 2003:10, från kommittén Radiokommunikation för effektiv ledning [RAKEL]). Bestämmelsen i 9 kap. 8 § andra stycket sekre-

tesslagen om sekretess hos myndigheter som driver televerksamhet för uppgift som angår ett särskilt telefonsamtal eller annat telemeddelande kan med andra ord fortfarande aktualiseras.

Sekretess hindrar inte att uppgift som angår misstanke om brott lämnas till åklagarmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet, om fängelse är föreskrivet för brottet och detta kan antas föranleda annan påföljd än böter (14 kap. 2 § fjärde stycket sekretesslagen). För uppgift som omfattas av sekretess enligt bl.a. 9 kap. 8 § andra stycket sekretesslagen gäller detta dock endast vid misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år (14 kap. 2 § femte stycket sekretesslagen). De uppgifter som avses torde vara såväl innehållet i ett telemeddelande (jfr hemlig teleavlyssning) som t.ex. när och mellan vilka abonnemang som ett telemeddelande har utväxlats (jfr SOU 1992:70 s. 328 och prop. 1992/93:200 s. 311). Frågan om förutsättningarna för att lämna ut uppgifter är uppfyllda prövas av den utlämnande myndigheten.

Liksom 6 kap. 22 § första stycket 3 LEK innebär 14 kap. 2 § fjärde och femte stycket sekretesslagen att uppgifter lämnas ut om elektronisk kommunikation med koppling såväl till personer som är misstänkta för brott som till andra än misstänkta (se bl.a. prop. 1983/84:142 s. 17). Det enda krav som ställs är att uppgiften angår misstanke om vissa allvarligare brott.

4.2.2 Buggningsutredningen

Buggningsutredningen hade bl.a. i uppdrag att se över tillämpningsområdet för hemlig teleövervakning och, om arbetet gav anledning till det, lämna förslag till ändringar innebärande att tvångsmedlet kunde användas såväl för en fortlöpande insamling av uppgifter som för att hämta in uppgifter om telemeddelanden bakåt i tiden. Utredningen skulle också se över de regler i rättegångsbalken, telelagen och sekretesslagen som tog sikte på de brottsutredande myndigheternas möjligheter att hämta in uppgifter om telemeddelanden. I direktiven angavs att förutom att förutsättningarna för att få tillgång till uppgifter om telemeddelanden skiljer sig åt mellan olika författningar är gränserna mellan tillämpningsområdena för de olika reglerna inte helt klara. I direktiven angavs också att beslutsordningarna har stora olikheter och att tillämpningen av ifrågavarande bestämmelser i rättegångsbalken är föremål för parlamentarisk kontroll medan detta inte är fallet med telelags- och

sekretesslagsreglerna. Utredningen fick i uppdrag att lämna förslag på en samlad reglering av dessa bestämmelser i rättegångsbalken (Dir. 1996:64).

Buggningsutredningen lade fram sina förslag i betänkandet Om buggning och andra hemliga tvångsmedel (SOU 1998:46). Buggningsutredningen föreslog bl.a. att hemlig teleövervakning skulle omfatta även historiska uppgifter, alltså inte bara en fortlöpande insamling av uppgifter utan även inhämtande av redan tillgängliga uppgifter. Som nyss nämndes är förslaget sedan den 1 oktober 2004 genomfört i den delen genom att tvångsmedlet även omfattar uppgifter om telemeddelanden som *har befordrats*. Buggningsutredningen konstaterade i det sammanhanget att det med förslaget inte längre fanns samma behov av att ha kvar telelagens och sekretesslagens regler på området och fortsatte enligt följande (s. 368 ff.).

> Det finns emellertid även andra skäl som talar för att man bör överväga att avskaffa dessa regler. Ett sådant skäl är att det med hänsyn till Europadomstolens avgörande i fallet Kruslin mot Frankrike (Europadomstolens dom den 24 april 1990, 176-A) kan ifrågasättas om inte en tillämpning av reglerna 14 kap. 2 § femte stycket sekretesslagen och 27 § 3 */sedermera 47 § 3/* telelagen står i strid med artikel 8 i Europakonventionen. Omständigheterna var följande. I en förundersökning om mord på en bankir, Jean Baron, natten mellan den 7 och 8 juni 1982, gav förundersökningsdomaren den 14 juni 1982 polisen instruktioner att avlyssna en misstänkt persons telefon, Dominique Terrieux. Jean Kruslin var vid tiden för avlyssningsbeslutet bosatt hos denne. Från den 15 till den 17 juni avlyssnade polisen sammanlagt 17 telefonsamtal, av vilka Jean Kruslin, som också använde telefonen, deltagit i flera. I anslutning till *ett* av Jean Kruslins telefonsamtal den 17 juni anhölls han som misstänkt för bl.a. mord. Misstanken kom emellertid att avse ett annat mord än det som föranlett telefonavlyssningen, nämligen ett mord på en juveleranställd, det s.k. Gerbe d'Or-fallet. Det rörde sig följaktligen om överskottsinformation. I den rättegång som följde yrkade Jean Kruslin att telefonsamtalet inte skulle tillåtas som bevisning, eftersom det hade tagits upp med anledning av ett ärende som inte berörde honom, det s.k. Baron-fallet. Detta yrkande ogillades dock av domstolarna och Jean Kruslin dömdes sedermera för väpnat rån och försök till väpnat rån till fängelse i 15 år. Åtalet för mord ogillades. Det bör vidare

nämnas att Jean Kruslin i ett annat mål dömdes till livstids fängelse för mord på Jean Baron. Det klagomål som Jean Kruslin framförde till Europakommissionen och som sedan blev föremål för Europadomstolens prövning i detta mål, avsåg dock endast den telefonavlyssning, vars resultat användes i det s.k. Gerbe d'Or-fallet.

Av rättsfallet framgår bl.a. följande beträffande fransk lagstiftning och rättspraxis på området. Den skrivna franska lagen gav inte något uttryckligt stöd för en förundersökningsdomare att ge polisen tillstånd till telefonavlyssning. Straffprocesslagen innehöll emellertid föreskrifter som berättigade en förundersökningsdomare att vidta samtliga de lagliga undersökningsåtgärder han bedömde som nödvändiga för att utreda sanningen och i rättspraxis ansågs telefonavlyssning vara en sådan tillåten åtgärd. Den närmare tillämpningen av telefonavlyssning bestämdes vid tiden för Europadomstolens dom av ett antal domar från de franska överrätterna. I Europadomstolens avgörande påpekades dock att de flesta av de rättsfall som åberopats inför domstolen hänförde sig till tiden efter den i målet relevanta tidpunkten, juni 1982. Av rättsfallen framgick bl.a. *att* en förundersökningsdomare kunde ge tillstånd till telefonavlyssning endast om det fanns skäl att misstänka att ett visst brott hade begåtts och utredningen gällde det brottet, *att* telefonavlyssningen fick avse endast vissa personer, nämligen den som anklagats för brott, den som var misstänkt för brott samt även en tredje person, t.ex. ett vittne, under förutsättning att det fanns skäl att tro att denne hade kunskap om för utredningen relevant information, *att* telefonsamtal mellan den misstänkte och hans försvarare inte fick avlyssnas och *att* den misstänkte eller tilltalade i ett brottmål och hans försvarare hade rätt att ta del av det vid en telefonavlyssning upptagna materialet och utskrifterna av materialet. I rättspraxis ställdes dock inga krav på brottets svårhet och ett beslut om telefonavlyssning behövde inte begränsas i tiden.

Jean Kruslin hävdade vid Europadomstolen av avlyssningen och upptagningen av hans telefonsamtal den 17 juni 1982 stod i strid med artikel 8 i Europakonventionen. Den franska regeringen bestred att så var fallet.

Domstolen antecknade som ostridigt mellan parterna, att avlyssningen av Dominique Terrieux telefon innebar ett intrång av en offentlig myndighet (”interference by a public

authority”) i Jean Kruslins rätt till skydd för sin korrespondens och sitt privatliv, eftersom avlyssningen innebar att även de samtal som denne deltog i avlyssnades.

Domstolen antecknade vidare att ett sådant intrång står i strid med artikel 8 om det inte är fråga om en inskränkning enligt artikel 8:2, dvs. en inskränkning som är lagenlig (”in accordance with the law”) och nödvändig i ett demokratiskt samhälle för att tillgodose något av de i artikeln uppräknade allmänna eller enskilda intressena.

Domstolen övergick härefter till att pröva om intrånget varit lagenligt (”in accordance with the law”). Domstolen uttalade därvid att kravet på lagenlighet innebär i första hand att åtgärden måste ha visst stöd i inhemsk lag (”should have some basis in domestic law”) och vidare att lagen måste uppfylla vissa kvalitetskrav. Den måste vara tillgänglig (”accessible”) för de personer som berörs och det skall vidare vara möjligt för den enskilde att kunna förutse dess konsekvenser (”foreseeable”).

Vid sin prövning fann Europadomstolen att åtgärden hade stöd i fransk lag. Domstolen beaktade därvid förekomsten inte bara av skriven lag utan även av en stadgad praxis. Domstolen fann vidare att reglerna om telefonavlyssning uppfyllde kravet på tillgänglighet. När det sedan gällde frågan om reglernas förutsebarhet (”the law´s foreseeability”) fann domstolen däremot – efter att ha framhållit nödvändigheten av att ett så allvarligt intrång som telefonavlyssning och andra former av registrering av telefonsamtal (”tapping and other forms of interception of telephone conversations”) regleras genom klara och detaljerade bestämmelser – att den nationella lagstiftningen inte hade varit tillräckligt tydlig i fråga om tillämpningsområdet för och sättet att utöva berörda myndigheters diskretionära prövning och att en kränkning av artikel 8 därför förelåg. Det sagda gällde enligt domstolen i än högre grad vid den i målet relevanta tidpunkten, juni 1982. Domstolen konstaterade att reglerna framför allt inte innebar tillräckliga garantier mot missbruk. Domstolen nämnde därvid bl.a. att den personkrets som kunde bli föremål för telefonavlyssning och de brott för vilka telefonavlyssning kunde beslutas inte hade definierats och att det inte hade funnits något krav på att ett beslut om telefonavlyssning begränsades i tiden. Jean Kruslin hade alltså, enligt

domstolen, inte åtnjutit det minimum av rättssäkerhet som en medborgare i ett demokratiskt samhälle har rätt att kräva.

I ett beslut av JO den 18 november 1996 (JO:s ämbetsberättelse 1997/98 s. 47 ff.), som avsåg ett initiativärende rörande en framställning om editionsföreläggande, redogjorde JO för fallet Kruslin samt uttalade att det kan ifrågasättas om reglerna i telelagen och sekretesslagen till fullo uppfyller de krav på klarhet och förutsebarhet som Europakonventionen ställer på regler om intrång i skyddet för privatliv och korrespondens. JO pekade därvid bl.a. på att reglerna i 14 kap. 2 § sekretesslagen och 27 § 3 telelagen inte innehåller några begränsningar av innebörd exempelvis att endast uppgifter hänförliga till misstänkta personer kan komma ifråga och att de inte innehåller någon begränsning till tiden av den information som får inhämtas.

Enligt utredningens mening är det mycket som talar för att de berörda bestämmelserna i sekretesslagen och telelagen inte uppfyller de krav som ställs upp i artikel 8 i Europakonventionen. Som tidigare har berörts finns det – efter de ändringar i fråga om hemlig teleavlyssning och hemlig teleövervakning som utredningen föreslår – inte samma behov av den angivna regleringen. Det behov som kan kvarstå torde vidare till stor del bli tillgodosett genom den variant av bestämmelsen i 27 § 3 telelagen som enligt vad utredningen föreslår bör finnas kvar. Det rör sig därvid huvudsakligen om fall där de brottsutredande myndigheterna av olika skäl har behov av att få uppgifter om telekommunikation till eller från en teleadress som innehas eller kan antas ha använts av en *målsägande*. En sådan regel bör föras in i rättegångsbalken.

Sammanfattningsvis anser utredningen att regleringen i 14 kap. 2 § fjärde och femte styckena – såvitt den avser särskilda telemeddelanden – och 27 § 3 telelagen bör upphävas.

En annan fråga som Buggningsutredningen berörde var om det bör gälla samma förutsättningar för att hämta in uppgifter som avser förfluten tid som uppgifter som avser framtiden eller om rekvisiten i ett eller flera avseenden bör vara lindrigare för att genom hemlig teleövervakning hämta in uppgifter som redan finns tillgängliga. Buggningsutredningen angav att det ibland hävdas att risken för integritetsintrång blir mindre vid inhämtning av historiskt material och fortsatte sina överväganden på följande sätt (SOU 1998:46 s. 387).

När det gäller frågan om vilka brott som bör föranleda hemlig teleövervakning för förfluten tid har en överväldigande majoritet av de myndigheter som har besvarat utredningens enkätundersökning angett att tillämpningsområdet bör bestämmas på samma sätt som vid hemlig teleövervakning som avser framtida uppgifter. Två av myndigheterna redovisade emellertid en annan uppfattning. Den ena myndigheten ansåg att hemlig teleövervakning som avser förfluten tid bör kunna beslutas när fängelse är föreskrivet för brottet och den andra myndigheten ansåg att det bör vara tillräckligt att det är föreskrivet fängelse i ett år eller däröver.

Enligt utredningens uppfattning torde integritetsriskerna vid hemlig teleövervakning för förfluten tid vara i allt väsentligt desamma som vid hemlig teleövervakning som avser framtida uppgifter. Det saknas därför anledning att göra åtskillnad mellan dessa fall när det gäller de brott som bör föranleda en användning av tvångsmedlet.

4.2.3 Lagrådsremissen den 6 april 2000

I den lagrådsremiss som följde på Buggningsutredningens betänkande instämde regeringen i utredningens bedömning att telelagens och sekretesslagens bestämmelser om skyldighet att lämna ut uppgifter som angår telemeddelanden borde upphävas. Regeringen uttryckte följande (s. 77).

De nuvarande reglerna i telelagen tar sikte på uppgifter som ligger bakåt i tiden, medan bestämmelserna om hemlig teleövervakning avser framtida uppgifter. Det är emellertid samma slags uppgifter som de båda regelverken avser. På samma sätt tar reglerna i sekretesslagen sikte på dels uppgifter som ligger bakåt i tiden, dels uppgifter i realtid, medan regleringen i rättegångsbalken om hemlig teleavlyssning och hemlig teleövervakning avser framtida uppgifter. Redan det förhållandet talar för att regleringen bör finnas samlad.

Den nuvarande ordningen med två parallella system har också nackdelen att de skiljer sig åt i beslutsordning; i det ena fallet (telelagen och sekretesslagen) krävs inte i första hand domstolsbeslut om att uppgifterna skall lämnas ut, medan en

förutsättning för utlämnande enligt rättegångsbalkens regler är att domstol lämnat tillstånd till åtgärden. Det är otidsenligt och mindre förenligt med Europakonventionens syften och krav att utlämnande av sådana integritetskänsliga uppgifter som det här är fråga om inte kräver beslut av ett offentligt organ. Såsom utredningen föreslagit bör därför regelsystemen föras samman. Det blir lagtekniskt mest logiskt och framför allt för den enskilde mest fördelaktigt att frågorna uteslutande hanteras enligt rättegångsbalkens regler och att följaktligen de aktuella lagrummen i telelagen och sekretesslagen upphävs.

Förändringen innebär en förstärkning av integritetsskyddet genom att de brottsutredande myndigheterna inte direkt hos teleoperatörerna får begära att få ut uppgifter om telemeddelanden. Det ankommer således alltid på domstol att fatta beslut i dessa frågor. Den av utredningen föreslagna förändringen bör därför genomföras.

I lagrådsremissen redovisade regeringen också samma uppfattning som Buggningsutredningen, att integritetsintrånget vid hemlig teleövervakning för förfluten tid är i allt väsentligt detsamma som vid hemlig teleövervakning som avser framtida uppgifter, och kom därför till slutsatsen att samma förutsättningar som gällde för att inhämta uppgifter i realtid vid hemlig teleövervakning även skulle gälla för redan befordrade telemeddelanden (s. 72 f.).

Lagrådet uttalade sig inte särskilt över frågan om att samla regleringen i rättegångsbalken och därmed upphäva de aktuella bestämmelserna i telelagen och sekretesslagen. Däremot föreslog Lagrådet vissa justeringar av lagteknisk karaktär.

4.2.4 Propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74)

Som framgick tidigare ändrades bl.a. bestämmelserna om hemlig teleövervakning den 1 oktober 2004. Numera är det möjligt att få även historiska uppgifter vid hemlig teleövervakning genom att regleringen omfattar uppgifter om telemeddelanden som *har befordrats*. I dagsläget är det alltså möjligt för de brottsutredande myndigheterna att få historiska uppgifter om telemeddelanden såväl enligt rättegångsbalkens regler om hemlig teleövervakning som ge-

nom utlämnande från operatörerna enligt 6 kap. 22 § första stycket 3 LEK och enligt sekretesslagen, även om utlämnande enligt den sistnämnda lagstiftningen förmodligen inte förekommer i praktiken.

Regeringen påpekade i den nu aktuella propositionen (prop. 2002/03:74 s. 40) att förslaget till ändring av bestämmelserna i rättegångsbalken inte påverkade tillämpningen av de bestämmelser i andra lagar som ger de brottsutredande myndigheterna möjlighet att inhämta historiska uppgifter om telemeddelanden. Regeringen hänvisade i det sammanhanget till att frågan om att avskaffa möjligheten för brottsutredande myndigheter att inhämta uppgifter om telemeddelanden direkt från teleoperatör skulle bli föremål för ytterligare överväganden. Det är alltså den frågan som regeringen därefter genom tilläggsdirektiven (Dir. 2003:145) gav oss i uppdrag att utreda.

Det kan tilläggas att regeringen i propositionen avstod från att behandla vissa frågor rörande hemlig teleavlyssning och hemlig teleövervakning som Buggningsutredningen tidigare hade tagit upp. Det rörde dels ett utvidgat förbud mot att avlyssna vissa samtal (jfr undantaget från vittnesplikten i 36 kap. 5 § RB), dels hanteringen av inhämtad information (jfr 27 kap. 22 och 24 §§ RB). Regeringen angav i dessa delar att frågorna hänger samman med en eventuell lagstiftning om hemlig avlyssning (buggning) och om hanteringen av överskottsinformation. För att inte föregripa beredningen av dessa frågor (se bl.a. departementspromemorian Överskottsinformation, Ds 2003:13) avstod regeringen från att lägga fram några förslag i det sammanhanget (prop. 2002/03:74 s. 12). Regeringen har nyligen lagt fram ett förslag till reglering av överskottsinformation vid användning av hemliga tvångsmedel (prop. 2004/05:143). Vi har utgått från utformningen av det förslaget i våra överväganden (se bl.a. avsnitt 9.4.11).

4.2.5 Våra överväganden

Förslag: Bestämmelserna i 6 kap. 22 § första stycket 3 LEK och 14 kap. 2 § fjärde och femte styckena sekretesslagen som innebär skyldighet för operatörer att i vissa fall lämna ut uppgifter som angår ett särskilt elektroniskt meddelande respektive telemeddelande till brottsutredande myndighet skall upphävas. De brottsutredande myndigheternas tillgång till uppgifterna skall uteslutande regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning.

Som framgått är det numera såväl vid hemlig teleövervakning som vid utlämnande enligt 6 kap. 22 § första stycket 3 LEK möjligt för de brottsutredande myndigheterna att erhålla uppgifter om telemeddelanden, eller, som det anges i lagen om elektronisk kommunikation, uppgifter som angår ett särskilt elektroniskt meddelande, som har befordrats, alltså *historiska* uppgifter. Dessutom är det i båda fallen fråga om *samma typ* av uppgifter som myndigheterna får tillgång till. Det kan vara uppgifter om meddelandets ursprung, destination, färdväg, datum, tid, storlek, varaktighet eller typ av tjänst. Som exempel kan nämnas uppgift om

- ✓ uppringt nummer/kontaktad IP-adress
- ✓ uppringande nummer/kontaktande IP-adress
- ✓ omstyrt nummer (vid vidarekoppling eller medflyttning)
- ✓ starttid
- ✓ sluttid
- ✓ antalet ringsignaler
- ✓ IMEI-numret (International Mobile Equipment Identification)
- ✓ IMSI-numret (International Mobile Subscriber Identification), och
- ✓ lokaliseringsuppgifter vad gäller mobiltelefon.

Som också har framgått skiljer sig förutsättningarna åt när det gäller möjligheten för myndigheterna att kunna utnyttja de båda metoderna i brottsutredningar. Ett utlämnande enligt lagen om elektronisk kommunikation kräver att det för brottet som utreds inte är föreskrivet lindrigare straff än fängelse i två år, vilket skall jämföras med kravet på minst sex månaders fängelse vid hemlig teleövervakning. I så måtto kan kravet i lagen om elektronisk kommunikation sägas vara strängare än enligt rättegångsbalken för att få ut historiska uppgifter. Däremot saknas motsvarigheter till rättegångsbalkens övriga krav i lagen om elektronisk kommunikation. Det rör kraven på att det skall finnas en skäligen misstänkt person, att åtgärden skall bedömas ha synnerlig vikt för utredningen, att åtgärden enbart får avse vissa teleadresser och telenät och att åtgärden kräver tillstånd av domstol.

Sekretesslagens bestämmelse i 14 kap. 2 § är även den en slags dubbelreglering i förhållande till såväl rättegångsbalken som lagen om elektronisk kommunikation. Visserligen kanske bestämmelsen i dag saknar praktisk betydelse men den tar sikte på såväl historiska uppgifter som uppgifter i realtid. Den torde dessutom ge möjlighet

för de brottsutredande myndigheterna att få tillgång till innehållet i ett telemeddelande, vilket i andra fall kräver beslut om hemlig teleavlyssning.

Redan av direktiven till Buggningsutredningen framgår att den splittrade regleringen rörande de brottsutredande myndigheternas möjlighet att hämta in uppgifter om telemeddelanden inte var ändamålsenlig utan att det i stället behövdes en samlad reglering i rättegångsbalken. Regeringen påpekade i det sammanhanget att förutsättningarna för att få tillgång till uppgifterna skilde sig åt, att gränserna mellan tillämpningsområdena för de olika författningarna inte var helt klara, att beslutsordningarna hade stora olikheter och att den parlamentariska kontrollen enbart omfattade rättegångsbalkens reglering.

Buggningsutredningens förslag om att hemlig teleövervakning även skulle omfatta historiska uppgifter trädde i kraft den 1 oktober 2004. Däremot är utredningens och den därpå följande lagrådsremissens förslag om att samtidigt upphäva bestämmelsen som numera motsvarar 6 kap. 22 § första stycket 3 LEK respektive bestämmelsen i 14 kap. 2 § fjärde och femte styckena sekretesslagen ännu inte genomförda. Orsaken till det sistnämnda förhållandet är att regeringen ville invänta resultatet av vår utredning (prop. 2003/03:74 s. 40).

Som synes har såväl Buggningsutredningen som regeringen vid flera tillfällen uttalat att den reglering som finns rörande tillgång till framför allt de historiska uppgifterna av flera skäl inte framstår som ändamålsenligt utformad. Ett sådant påpekande har fått större giltighet sedan det för en tid sedan blev möjligt för de brottsutredande myndigheterna att få tillgång till historiska uppgifter genom hemlig teleövervakning. Behovet för myndigheterna att utnyttja den rätt som lagen om elektronisk kommunikation ger minskade då.

En självklar och grundläggande utgångspunkt i samband med övervägandena om regelsystemen skall föras samman är att den brottsutredande verksamheten inte får förlora i effektivitet genom ett sådant förslag. De brottsutredande myndigheterna har t.ex. ett mycket stort behov av att få tillgång till de historiska uppgifterna (se bl.a. avsnitt 4.3.5 och 7.5.2). Uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt.

Vi instämmer i den slutsats som såväl Buggningsutredningen som regeringen tidigare har kommit fram till, nämligen att regelsy-

stemen skall föras samman i rättegångsbalken och att det blir det lagtekniskt mest logiska. För den enskilde innebär det, som påpekats tidigare, en förstärkning av integritetsskyddet bl.a. genom att det som huvudregel kommer att krävas domstolsbeslut för att övervakning enligt 27 kap. RB skall få genomföras (jfr nedan om åklagarens intermistiska beslutanderätt). Dessutom är användningen av tvångsmedlet föremål för parlamentarisk kontroll. Mot bakgrund av hur vi i övrigt har utformat förslagen i betänkandet (se särskilt möjligheten att använda övervakning utan misstänkt gärningsman, avsnitt 4.3.5), bedömer vi att effektiviteten i det brottsutredande arbetet, trots förslaget om att den aktuella bestämmelsen i lagen om elektronisk kommunikation skall upphävas, kan hållas på samma nivå som tidigare.

Det kan nämnas att det saknas statistik om i hur många fall årligen som de brottsutredande myndigheterna begär uppgifter som angår särskilda elektroniska meddelanden från operatörerna, alltså uppgifter enligt lagen om elektronisk kommunikation. Vid hemlig teleavlyssning och hemlig teleövervakning sköter Säkerhetspolisen all kontakt med operatörerna medan begäran enligt lagen om elektronisk kommunikation görs ”mer formlöst” av Säkerhetspolisen, Rikskriminalpolisen och varje polismyndighet för sig. Enligt en grov uppskattning gjord av Säkerhetspolisen kan det röra sig om drygt 4000 fall årligen. Särskilt som det är så att gränsen vad gäller straffskalan är strängare vid utlämnande enligt lagen om elektronisk kommunikation än vid hemlig teleövervakning, är det alltså en ansenlig mängd ärenden som i fortsättningen får hanteras av domstolarna, med den ökning av integritetsskyddet som detta innebär.

Som följer redan av den nuvarande regleringen av hemlig teleövervakning saknas det skäl att föreskriva skilda förutsättningar för tvångsmedlet beroende på om det är historiska uppgifter eller realtidsuppgifter som de brottsutredande myndigheterna vill få tillgång till. Integritetsintrånget är allmänt sett detsamma i båda fallen.

Bestämmelserna i 6 kap. 22 § första stycket 3 LEK och 14 kap. 2 § fjärde och femte styckena sekretesslagen som innebär skyldighet för operatörer att i vissa fall lämna ut uppgifter som angår ett särskilt elektroniskt meddelande respektive telemeddelande till brottsutredande myndighet bör alltså upphävas.

Vi vill påpeka att det nu sagda inte avser möjligheten för de brottsutredande myndigheterna att enligt 6 kap. 22 § första stycket 2 LEK få uppgift om abonnemang från operatörerna vid brott som enligt myndighetens bedömning kan föranleda annan påföljd än böter. Det är orimligt att polisens tillgång till uppgifter om abon-

nemang, alltså rena ”kataloguppgifter”, som namn, titel, adress och abonnentnummer, skall kräva domstolsbeslut om övervakning enligt 27 kap. RB. Vi återkommer till den bestämmelsen i avsnitt 5.4.

Det skall också sägas att särskilt på grund av den snabba tekniska utvecklingen är det direkt olämpligt att i lagtext ange precis vilka typer av uppgifter som skall lämnas ut vid övervakning. Vi instämmer där med Buggningsutredningen som uttalade följande (SOU 1998:46 s. 365).

> Av lagtexten till bestämmelsen om hemlig teleövervakning framgår vidare inte vilken information som tvångsmedlet ger åtkomst till, vilket naturligtvis inte heller är nödvändigt under förutsättning att det rör sig om uppgifter som på ett någorlunda naturligt sätt kan anses falla under definitionen av hemlig teleövervakning.

Vi vill samtidigt nämna att frågan om interimistisk beslutanderätt för åklagaren behandlas i avsnitt 4.3.5.

4.3 Övervakning även utan misstänkt gärningsman m.m.

4.3.1 Nuvarande bestämmelser

Hemlig teleavlyssning och hemlig teleövervakning får ske endast om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Dessutom får åtgärden enligt 27 kap. 20 § första stycket RB enbart avse vissa teleadresser, nämligen

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.

Enligt gällande rätt är det alltså en förutsättning för att hemlig teleövervakning skall få användas att det går att peka ut en person som skäligen misstänkt för ett brott. Något sådant krav gäller dock inte för att de brottsutredande myndigheterna med stöd av 6 kap.

22 § första stycket 3 LEK skall få ut motsvarande uppgifter från operatörerna, alltså uppgifter som angår särskilda elektroniska meddelanden.

Vi föreslog i avsnitt 4.2.5 att bl.a. sistnämnda bestämmelse om skyldighet för operatörer att lämna ut uppgifter till brottsutredande myndigheter skulle upphävas. De brottsutredande myndigheternas tillgång till uppgifterna skulle uteslutande regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning Det finns därför skäl att överväga om det även fortsättningsvis i samtliga fall skall krävas en skäligen misstänkt person vid användning av det tvångsmedlet.

I samband med de övervägandena måste det också bedömas om kravet i 27 kap. 21 § andra stycket RB skall finnas kvar om att det i domstolens beslut att tillåta hemlig teleavlyssning eller hemlig teleövervakning skall anges vilken teleadress (tekniskt hjälpmedel) tillståndet avser.

Ytterligare en fråga som aktualiseras i detta sammanhang är om det är lämpligt att åklagare fattar interimistiska beslut om övervakning. Rättegångsbalken tillåter i dag inte att åklagare i avvaktan på domstolsprövning fattar interimistiska beslut om användning av hemlig teleavlyssning och hemlig teleövervakning. Däremot finns det i 1952 års tvångsmedelslag och i 1988 års lag om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. en sådan beslutanderätt för åklagaren.

Enligt 1952 års lag (5 § andra stycket) gäller att ett sådant förordnande får meddelas om det kan befaras att inhämtande av rättens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. I 1988 års lag ställs det upp samma förutsättningar för ett interimistiskt beslut (28 § första stycket). I båda fallen gäller att beslutet skall anmälas skriftligen till rätten, som snabbt skall pröva frågan (6 § i 1952 års lag och 28 § andra stycket i 1988 års lag).

4.3.2 Buggningsutredningen

Mot bakgrund av att Buggningsutredningen menade att den dåvarande regleringen i sekretesslagen och telelagen (numera lagen om elektronisk kommunikation) skulle upphävas, ansåg utredningen att det i några situationer behövdes undantag från huvudregeln om kravet på brottsmisstanke mot viss person vid hemlig teleövervak-

ning. Enligt Buggningsutredningen fanns det två olika situationer där det från effektivitetssynpunkt framstår som angeläget och från integritetssynpunkt som godtagbart att de brottsutredande myndigheterna kan hämta in uppgifter genom teleövervakning utan att det finns en skäligen misstänkt person. Buggningsutredningen anförde följande (SOU 1998:46 s. 403 f.).

> Den första situationen är när det i en brottsutredning saknas en skäligen misstänkt person men det finns uppgifter om att någon har ringt eller blivit uppringd i området kring en brottsplats. Det sagda torde i princip gälla enbart vid mobiltelefonsamtal. I stort sett samtliga brottsutredande myndigheter som utredningen har varit i kontakt med har ansett att det finns ett stort behov av en undantagsregel i en situation som den nämnda och myndigheterna har lämnat ett flertal praktiska exempel på behovet. Ett exempel som därvid har nämnts är att ett vittne i samband med ett bankrån har sett en maskerad gärningsman ringa ett mobiltelefonsamtal. Myndigheterna har därvid framhållit att teleövervakningsuppgifter, som enligt gällande rätt kan inhämtas med stöd av telelagen, i ett sådant fall kan vara de enda konkreta uppgifter som utredningspersonalen har att gå efter då de söker en tänkbar gärningsman. En begränsning som dock bör gälla beträffande en sådan inhämtning är att teleövervakningsuppgifterna får avse endast de teleadresser som använts i anslutning till den plats där brottet har begåtts. Vad det i praktiken kommer att handla om är att uppgifter hämtas in från den eller de basstationer som – vid tidpunkten för brottet – kan antas har berörts av ett sådant mobiltelefonsamtal.
>
> Den andra situationen där undantag bör göras från kravet på att åtgärden får avse endast en teleadress som innehas eller kan antas ha använts av den misstänkte, är vissa fall där målsägandens teleadress kan ge uppgifter som leder till att ett brott klaras upp. De flesta av myndigheterna har framhållit att det vid bl.a. mordutredningar där det saknas misstanke mot viss person kan vara av avgörande betydelse för utredningen att man får reda på vem offret talat med i telefon den närmaste tiden före brottet för att därigenom kunna identifiera tänkbara gärningsmän. Myndigheterna har påtalat att ett krav på skälig misstanke mot viss person i dessa fall i praktiken skulle kunna förstöra möjligheterna att utreda brottet.

> En polismyndighet nämnde att sådana fall förekommit vid tre tillfällen under sex månaders tid.
>
> En förutsättning för åtgärden bör dock vara att målsäganden har lämnat sitt samtycke till åtgärden. Utredningen menar nämligen att det ur integritetssynpunkt skulle leda allt för långt att införa en regel som innebär att de brottsutredande myndigheterna mot målsägandens vilja kan hämta in uppgifter som rör hans teleadresser. För att åtgärden skall vara till praktisk nytta i det polisiära arbetet bör emellertid uppgifterna få inhämtas även i de fall målsägandens samtycke inte kan inhämtas, t.ex. på grund av att målsäganden har avlidit genom brottet. Andra exempel är där målsäganden är medvetslös eller försvunnen. Enligt utredningens uppfattning får det anses ligga i sakens natur att målsäganden vill att brottet mot honom utreds och beivras.

I frågan om interimistisk beslutanderätt för åklagare skrev Buggningsutredningen följande (SOU 1998:46 s. 415 ff.).

> Inledningsvis kan nämnas att det utomlands är förhållandevis vanligt att det vid hemlig teleavlyssning m.fl. tvångsmedel finns någon form av interimistisk beslutanderätt i avvaktan på den domstolsprövning som annars i princip är det normala.
>
> ---
>
> Frågan om att i rättegångsbalken införa en interimistisk beslutanderätt för åklagaren vid användning av hemlig teleavlyssning m.fl. tvångsmedel är inte ny. Den diskuterades bl.a. i 1989 års lagstiftningsärende om vissa tvångsmedelsfrågor (prop. 1988/89:124 s. 51 f.). Departementschefen redovisade där uppfattningen att en sådan befogenhet för åklagare inte borde införas, om inte tvingande praktiska behov talade för det. Hon menade att en sådan möjlighet endast bör vara en utväg i särskilt kritiska lägen. Departementschefen uttalade att det som förekommit i lagstiftningsärendet inte övertygat henne om att det förelåg något sådant påtagligt behov utan att man i de situationer där det varit nödvändigt att snabbt få ett beslut också har gått att utverka detta inom rimlig tid utan att några mer väsentliga effektivitetsförluster uppstått. Under sådana omständigheter, menade departementschefen, var hon inte beredd att då förorda att åklagare får möjlighet att besluta intermistiskt. Även i propositionen om hemlig

kameraövervakning (prop. 1995/96:85 s. 33 f.) berördes frågan om interimistiska beslut. Regeringen uttalade att det saknades tillräckliga skäl för att införa en generell möjlighet till sådana beslut avseende användningen av dolda övervakningskameror.

När det först gäller hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning finns det, vilket framgår av det tidigare redovisade, ett visst behov av en befogenhet för åklagaren att fatta interimistiska beslut. Behovet av snabba beslut vid hemlig teleavlyssning och hemlig teleövervakning har sannolikt ökat under de senaste åren, vilket hänger samman bl.a. med teknikutvecklingen. Det kan nämligen numera gå mycket snabbt att verkställa ett beslut om hemlig teleavlyssning och hemlig teleövervakning. Även det sätt som de kriminella använder den moderna teletekniken har gjort att behovet av snabba beslut har ökat. T.ex. förekommer det – särskilt vid mobiltelefoni – att den misstänkte ofta byter teleadress. Det är dessutom troligt att en ordning med ett offentligt ombud för den misstänkte kan ytterligare öka behovet av snabba beslut.

Enligt utredningens uppfattning utgör det som framkommit tillräckliga skäl för att föreslå att det i rättegångsbalken införs en generell möjlighet för åklagaren att fatta interimistiska beslut avseende hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Det förhållandet att det hittills, i de flesta fall där det har varit nödvändigt att få ett snabbt beslut, varit möjligt att utverka detta inom rimlig tid utan några mer väsentliga effektivitetsförluster, förändrar inte denna bedömning. Det är nämligen, menar utredningen, inte tillfredsställande att en fråga om t.ex. hemlig teleavlyssning skall kunna användas i en förundersökning rörande ett allvarligt brott på en kväll eller en helg blir beroende av om polis och åklagare lyckas får tag i en domare som kan fatta beslut.

Eftersom det vid dessa tvångsmedel finns starka integritetsintressen bör det emellertid vara en förutsättning för ett interimistiskt beslut att ändamålet med åtgärden går förlorat om man väntar med att företa åtgärden, dvs. att befogenheten får användas endast i brådskande fall. Av rättssäkerhets- och kontrollskäl bör man dessutom ha en obligatorisk domstolsprövning av ett interimistiskt beslut, dvs. domstolen skall pröva frågan också i de fall åtgärden – vid tiden för

domstolsprövningen – redan har upphört. Med en sådan ordning anser utredningen att det finns tillräckliga garantier för att den interimistiska beslutanderätten kommer att användas endast i de fall där det verkligen är befogat.

4.3.3 Lagrådsremissen den 6 april 2000

I lagrådsremissen tog regeringen också upp frågan om hemlig teleövervakning utan känd gärningsman och menade att även om det inte finns någon som är skäligen misstänkt för ett begånget brott, bör hemlig teleövervakning tillåtas i vissa fall. Regeringen skrev följande (s. 78 f.).

> Utredningen har ansett att det bör göras undantag från regeln i rättegångsbalken att det alltid skall finnas en person som är misstänkt för brott när det gäller s.k. historiska teleövervakningsuppgifter. Enligt utredningens bedömning finns det annars en risk för att avsaknaden av de bestämmelser i telelagen och sekretesslagen som enligt gällande rätt ger en möjlighet att hämta in sådana uppgifter kan få allvarliga konsekvenser för det polisiära arbetet. Samtidigt har utredningen framhållit att sekretesslagens och telelagens bestämmelser inte uppfyller de krav som bör ställas på bestämmelser av det slag som nu är ifråga, bl.a. mot bakgrund av att bestämmelserna inte alls knyter an till den misstänkte.
>
> Utredningen tar upp två typsituationer där det ur effektivitetssynpunkt är angeläget och ur integritetssynpunkt godtagbart att det görs undantag från kravet på att det skall finnas en misstänkt person. Den ena situationen är att det i en brottsutredning finns uppgifter om att någon har ringt eller blivit uppringd i området kring en brottsplats. Ett exempel på ett sådant fall är att ett vittne vid ett bankrån sett en maskerad gärningsman ringa ett mobiltelefonsamtal. Ett annat exempel är att en målsägandes teleadress kan ge uppgifter som leder till att ett brott klaras upp, men det inte går att få målsägandens samtycke till att få del av uppgifter om vilka teleadresser målsäganden haft kontakt med strax före det att brottet begicks. Är målsäganden avliden bör dödsboet kunna lämna motsvarande samtycke. Är däremot målsäganden försvunnen och finns det särskild anledning anta att ett brott

har begåtts gentemot den personen, bör det ligga i målsägandens intresse att brottet mot honom utreds och beivras.

Regeringen anser att undantag från huvudregeln vid fall motsvarande de av utredningen angivna exemplen framstår som angelägna ur såväl effektivitetssynpunkt som av hänsyn till brottsoffret. Regeringen konstaterar också att det i vissa brottsutredningar har varit av största betydelse att uppgifter av detta slag har kunnat hämtas in enligt telelagen. I klarhetens intresse kan framhållas att regeringen inte här avser situationer där målsäganden kan men inte vill samtycka till att uppgiften lämnas ut. Det är möjligt att utforma en bestämmelse som är tillräckligt snäv för att vara acceptabel ur integritetssynpunkt, samtidigt som den medger utlämnande av de uppgifter som polisen kan behöva i de avsedda situationerna. Utredningens förslag bör därför genomföras. Det ankommer dock givetvis på åklagare och domstol att se till att tillståndet medger minsta möjliga intrång i för utredningen ovidkommande personers privatliv. Därutöver skall också gälla att åtgärden skall vara av synnerlig betydelse för utredningen.

Lagrådet lämnade synpunkter enbart av lagteknisk karaktär på förslaget i denna del.

När det gäller interimistisk beslutanderätt för åklagare i fråga om hemliga tvångsmedel gjorde regeringen den bedömningen i lagrådsremissen att det inte borde införas någon sådan rätt i rättegångsbalken och anförde följande (s. 94).

Interimistiska beslut som institut används när det är särskilt brådskande ärenden och där det inte finns tid att avvakta den normala handläggningsordningen. Enligt 1952 års tvångsmedelslag har åklagaren en interimistisk beslutanderätt i fråga om de tvångsmedel som särskilt regleras där. Åklagarens beslut skall därefter underställas domstolen som skall besluta om tillståndet skall bestå eller inte.

De tvångsmedel vi nu talar om bör omgärdas av särskilda rättssäkerhetsgarantier. En sådan garanti är den obligatoriska domstolsprövningen. Avsteg därifrån bör ske endast om det kan antas att syftet med regleringen inte annars kan uppnås.

Varken av utredningen eller av remissvaren framkommer att det har funnits ett större behov av en särskild handläggningsordning för brådskande ärenden. Visserligen kan antalet ärenden om hemliga tvångsmedel antas att öka eftersom te-

leövervakning uteslutande skall handläggas vid domstol, men det torde knappast innebära att det blir ett betydligt större antal ärenden som är brådskande eller annars kräver prövning på annan tid än kontorstid. Regeringen anser således att det inte har framkommit sådana starka skäl som krävs för att införa ett system där integritetskänsliga hemlig tvångsmedel som följer rättegångsbalkens regler får verkställas utan rättens tillstånd. Regeringen anser därför inte att utredningens förslag i denna del bör genomföras.

4.3.4 Propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74)

I den aktuella propositionen gjorde regeringen samma bedömning som tidigare och upprepade skälen i lagrådsremissen mot att införa en interimistisk beslutanderätt för åklagare i fråga om hemliga tvångsmedel. Regeringen tillade att den har för avsikt att noga följa utvecklingen och vid behov pröva frågan på nytt (s. 42 f.).

4.3.5 Våra överväganden

Frågan om övervakning även utan misstänkt gärningsman

Förslag: Vid förundersökning angående brott som är så allvarliga att de kan ligga till grund för beslut om avlyssning, skall övervakning få användas även om det inte finns någon som är skäligen misstänkt för brottet.

Den aktuella regleringen i lagen om elektronisk kommunikation tillåter att de brottsutredande myndigheterna hämtar in uppgifter som angår särskilda elektroniska meddelanden, oavsett om det finns en skäligen misstänkt person i förundersökningen eller inte. Vi föreslog i avsnitt 4.2.5 att den regleringen skulle upphävas. Det är uppenbart att det främst av effektivitetsskäl och av hänsyn till brottsoffren i ett sådant läge måste övervägas vilka möjligheter som skall finnas för de brottsutredande myndigheterna att använda

övervakning enligt 27 kap. RB, särskilt i fall där det saknas en skäligen misstänkt person.

Buggningsutredningens betänkande och lagrådsremissens förslag innehöll en begränsning i förhållande till bestämmelsen i telelagen (numera lagen om elektronisk kommunikation). När det saknas en skäligen misstänkt person skulle de brottsutredande myndigheterna enligt förslaget kunna få uppgifter genom hemlig teleövervakning enbart avseende de teleadresser som har använts i anslutning till tiden och platsen för ett brott samt uppgifter om telemeddelanden som har befordrats till eller från en teleadress som innehas av eller av särskild anledning kan antas ha använts av en målsägande som inte kan samtycka till åtgärden.

Ofta är övervakningsuppgifter, däribland uppgifter om positionen hos mobiltelefoner den absolut viktigaste nyckeln till att utredningar rörande grövre brott kan föras framåt (se även förslaget i avsnitt 4.5 rörande identifiering av tekniska hjälpmedel). Övervakningsuppgifterna används mycket ofta i utredningar, exempelvis rörande 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, som terroristbrott. Särskilt i de inledande skedena av sådana förundersökningar kan det många gånger saknas en skäligen misstänkt person. I utredningsarbetet kan polisen i sådana fall på olika sätt ”lägga pussel” med övervakningsuppgifterna, 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, är det alltså möjligt att klarlägga hur gärningsmännen har agerat och vilka personer som har varit inblandade i brottsligheten. Dessutom kan övervakningsuppgifterna 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 övervakningsuppgifter 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. Övervakningsuppgifterna 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. All information som erhålls på detta sätt ligger därefter till grund för det vidare utredningsarbetet.

Arbetet med att utreda brottslighet av den karaktär som nu är aktuell inleds ofta med en kontroll av de övervakningsuppgifter som har genererats i anslutning till en brottsplats. 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. Arbetet fortsätter sedan med en kartläggning av sambandet mellan en intressant teleadress och andra adresser, allt för att få fram de upplysningar som beskrevs ovan. I Buggningsutredningen och i lagrådsremissen föreslogs en begränsning i myndigheternas möjligheter att få tillgång till övervakningsuppgifter i de fall det saknas en skäligen misstänkt person. Det skulle enligt förslagen bli möjligt att inhämta uppgifter enbart rörande de teleadresser som använts i anslutning till tiden och platsen för brottet. Den kan dock nämnas att platsen för brottet i flera fall kan vara svår att ange, t.ex. när datorer har använts, och att det inträffar att själva brottet begås utomlands medan de förberedande åtgärderna har skett i Sverige, dit gärningsmännen dessutom återvänder efter brottet. Likaså kan tidpunkten för t.ex. förberedelsebrott vara i princip omöjlig att ange innan övervakningsuppgifterna har erhållits.

Mot den bakgrund som nyss beskrevs skulle en sådan begränsning enligt vår bedömning och enligt samstämmiga uppgifter från polis och åklagare innebära en *kraftig* försämring av effektiviteten i utredningar rörande grova brott. Begränsningen kan, just när det gäller övervakningsuppgifter, inte motiveras vid en avvägning mot hänsyn till skyddet för personlig integritet. Enligt vår mening skulle begränsningen innebära en helt oacceptabel följd av att den aktuella bestämmelsen i lagen om elektronisk kommunikation föreslås bli upphävd. En grundläggande utgångspunkt måste vara att den brottsutredande verksamheten inte får förlora i effektivitet över huvud taget genom förslaget om en samlad reglering i rättegångsbalken.

En lämplig lösning är enligt vår mening att övervakning enligt rättegångsbalken skall få användas under vissa förutsättningar även om det inte finns någon som är skäligen misstänkt för brottet. Bl.a. på det sättet kommer ordningen inte att avvika i allt för stor om-

fattning från de möjligheter som lagen om elektronisk kommunikation ger, vilket är helt nödvändigt för att upprätthålla effektiviteten i den brottsutredande verksamheten. I ett sådant förslag finns inte begränsningen till tiden och platsen för brottet. Dessutom täcks den situationen som nämndes i tidigare förslag in, att myndigheterna behöver få uppgifter om telemeddelanden som har befordrats till eller från en teleadress som innehas av eller av särskild anledning kan antas ha använts av en målsägande som inte kan samtycka till åtgärden. Det är också en godtagbar lösning vad gäller intrånget i personlig integritet i samband med tillgång till övervakningsuppgifter.

I dagsläget är möjligheten för de brottsutredande myndigheterna att använda lagen om elektronisk kommunikation för att få uppgifter som angår elektroniska meddelanden inte begränsad till situationer när det saknas en skäligen misstänkt person. Åtgärden kan användas även när någon är skäligen misstänkt och också för att hämta in historiska uppgifter samtidigt med en pågående hemlig teleövervakning, om brottet är tillräckligt allvarligt. Den brottslighet som nämndes tidigare är i de flesta fall sådan att flera personer på olika sätt är inblandade. Skulle någon av de inblandade ha identifierats som skäligen misstänkt måste utredningen trots detta kunna fortsätta att drivas framåt genom framtagande och bearbetning av övervakningsuppgifter. Möjligheten att använda övervakning skall alltså inte vara begränsad till situationer när det saknas en skäligen misstänkt person utan måste kunna användas i utredningar även efter det att någon har bedömts vara skäligen misstänkt. En motsatt ordning skulle innebära en allt för stor begränsning av effektiviteten i förhållande till nuvarande bestämmelser.

Som framgått tidigare krävs vid hemlig teleövervakning, med vissa undantag, att det för brottet inte är föreskrivet lindrigare straff än fängelse i sex månader. För att myndigheterna skall få ut samma typ av uppgifter krävs enligt lagen om elektronisk kommunikation minst två års fängelse i straffskalan. Det sistnämnda innebär bl.a. att inga försöks- eller förberedelsebrott omfattas (23 kap. 1-2 §§ BrB). Dessutom är hemlig teleövervakning begränsad till att avse vissa teleadresser, nämligen sådana som har innehafts eller kan antas ha använts av den misstänkte samt teleadresser som det finns synnerlig anledning att anta att det misstänkte har kontaktat.

Frågan inställer sig då om det bör föreskrivas strängare krav i förhållande till andra fall när det gäller brottsligheten för att få hämta in uppgifter i nu aktuella fall.

Det skall först sägas att det inte finns anledning att göra undantag från kraven i 27 kap. 20 § RB vad gäller att åtgärden skall vara av synnerlig vikt för utredningen och enbart får avse meddelanden som befordras eller har befordrats i vissa elektroniska kommunikationsnät. Dessutom skall det som huvudregel vara domstolen som ger tillstånd (jfr nedan om åklagarens interimistiska beslutanderätt). På det sättet uppkommer ett ökat skydd mot intrång i den personliga integriteten i förhållande till ordningen enligt lagen om elektronisk kommunikation.

Rekvisitet ”synnerlig vikt för utredningen” innebär stora krav på de brottsutredande myndigheterna att presentera ett tillräckligt gott underlag för domstolens ställningstagande. Som uttalades i den tidigare lagrådsremissen ankommer det på domstolen att se till att tillståndet bl.a. medger minsta möjliga intrång i för utredningen ovidkommande personers privatliv. Det kan t.ex. ske genom begränsningar av integritetsskäl i domstolens beslut, t.ex. till viss tidsperiod, visst geografiskt område, vissa basstationer eller vissa telefoner (SOU 1998:46 s. 497). Polis och åklagare har även skyldighet att hela tiden väga intresset av att brottsutredningen bedrivs effektivt mot skyddet för personlig integritet.

Vi inser att det finns en hel del situationer där det saknas en skäligen misstänkt person och där övervakning enligt 27 kap. RB säkerligen skulle vara av stort värde i utredningar rörande brott där minst sex månader eller ett års fängelse är föreskrivet. Även de fallen kan röra brott av mer eller mindre organiserat slag med flera gärningsmän inblandade, t.ex. fall av grov misshandel, grova stölder vid inbrott i villor eller på andra platser samt personrån och s.k. åldringsbrott. Av integritetsskäl menar vi dock att övervakningsuppgifterna skall få hämtas in enbart när brottsligheten är sådan att den kan ligga till grund för avlyssning enligt 27 kap. 18 § RB. Det rör alltså brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, försök, förberedelse eller stämpling i de fallen samt andra brott om straffvärdet överstiger fängelse i två år. I det avseendet kommer regleringen att likna den som nu finns i lagen om elektronisk kommunikation.

Det finns givetvis en möjlighet att straffvärdet för de brott som nyligen nämndes, t.ex. grov misshandel, är så högt att det överstiger fängelse i två år. I de fallen kan givetvis övervakning i den nu aktuella situationen användas. För övrigt kan sägas att utan en liknande bestämmelse skulle de begränsningar i tvångsmedlet som nu finns i 27 kap. 20 § första stycket RB vad gäller vilka teleadresser

(tekniska hjälpmedel) som åtgärden får omfatta i princip komma att sakna praktisk betydelse.

Frågan om angivande av identifierade tekniska hjälpmedel i domstolens beslut

Förslag: Någon motsvarighet till det krav som finns i dag på att det i ett beslut om hemlig teleavlyssning eller hemlig teleövervakning skall anges vilken teleadress tillståndet gäller skall inte finnas i lagtexten.

I avsnitt 3.5 kom vi fram till att begreppet teleadress skulle mönstras ut ur lagtexten i rättegångsbalken. I stället skulle bestämmelserna anknytas till begreppet tekniskt hjälpmedel. I dagsläget finns ett krav i 27 kap. 21 § andra stycket RB om att den teleadress som tillståndet gäller skall anges i beslutet om hemlig teleavlyssning och hemlig teleövervakning.

Ett motsvarande krav kan givetvis inte finnas kvar för det fall övervakning tillåts när det saknas en skäligen misstänkt person och vetskap om det tekniska hjälpmedlet. Till detta kommer de mycket stora effektivitetsproblem som användningen s.k. anonyma kontantkort skapar i det brottsutredande arbetet och som vi utvecklar i avsnitt 4.5 och 5.6. Vi upprepar inte detta här utan konstaterar att vad som kommer fram i de avsnitten och vårt förslag till lösning på problemet också talar med stor styrka för att inte ha ett krav på att identifierade tekniska hjälpmedel skall anges i domstolens beslut. Det är nödvändigt för effektiviteten i myndigheternas arbete att knytningen av tvångsmedelsbesluten som rör en skäligen misstänkt person görs mindre strikt när det gäller en exakt identitet på det tekniska hjälpmedel som personen använder. Enligt uppgift från Rikskriminalpolisen inträffar det i i stort sett samtliga ärenden att domstolen ständigt måste ha nya förhandlingar för att nya telefonnummer (teleadresser) blir aktuella för tvångsmedlen rörande samma person.

Mot den bakgrunden menar vi att det i fortsättningen inte bör finnas något krav i lagtexten på att vissa identifierade tekniska hjälpmedel skall anges i domstolens beslut. Däremot skall det givetvis fortfarande vara så att för en skäligen misstänkt person skall lagstiftningen ställa krav på att hemlig teleavlyssning och hemlig teleövervakning avser

1. sådana tekniska hjälpmedel 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. sådana tekniska hjälpmedel 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.

En annan sak är att det behöver finnas metoder för att identifiera sådana tekniska hjälpmedel. Vi återkommer till den frågan i avsnitt 4.5.

Visserligen uttalade regeringen i samband med att begreppet teleanläggning ersattes av teleadress i lagstiftningen att den ansåg att det inte var möjligt att reglera tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning endast genom att låta åtgärden avse telemeddelanden med viss anknytning till den misstänkte. Det är nödvändigt, ansåg regeringen, inte minst från integritetssynpunkt, att en bestämmelse om vad som får avlyssnas eller övervakas är så utformad att domstolen kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Regeringen fortsatte med att säga att det dock framför allt från tillämpningssynpunkt är ett oeftergivligt krav att ett beslut om hemlig teleavlyssning och hemlig teleövervakning kan konkretiseras så att beslutet blir praktiskt verkställbart (prop. 1994/95:227 s. 20 f.).

Enligt vår mening har den oerhört snabba tekniska utvecklingen under de senaste åren och de metoder som de kriminella personerna numera använder för att undgå tvångsmedlen och därmed försvåra eller helt omöjliggöra det brottsutredande arbetet gjort att regeringens tidigare uttalanden måste omprövas. Det är enligt vår mening fullt tillräckligt att undersökningsledaren, efter domstolens beslut om att tillåta tvångsmedlen i förundersökningen, får avgöra, utifrån vad lagstiftningen tillåter, t.ex. vilka identifierade enskilda telefonnummer eller e-postadresser som skall omfattas av verkställigheten. Verkställighet av tvångsmedelsbeslutet kan därefter begäras hos operatören. Enligt vår bedömning kommer domstolarna ändå att inför beslut om tvångsmedlen få all den information som är nödvändig från åklagaren och i förekommande fall från det offentliga ombudet och kunna göra en fullödig bedömning i tillståndsfrågan, bl.a. av det integritetsintrång som skulle uppkomma om tillstånd ges (se i det sammanhanget 27 kap. 1 § tredje stycket RB). Det ankommer också på domstolen att se till att tillståndet medger minsta möjliga intrång i för utredningen ovidkommande personers privatliv. Det kan t.ex. ske genom begränsande villkor i

domstolens beslut, t.ex. till viss tidsperiod, visst geografiskt område eller vissa basstationer (SOU 1998:46 s. 497). De villkor som domstolen ställer upp skulle också kunna röra vissa typer av tekniska hjälpmedel och vissa särskilt identifierade hjälpmedel, som att avlyssning får avse en viss telefon enbart under viss tid. Det kan samtidigt erinras om att de brottsutredande myndigheterna genom proportionalitetsprincipen har en skyldighet att under hela verkställigheten se till att tvångsåtgärderna står i rimlig proportion till vad som står att vinna med dessa.

Frågan om interimistisk beslutanderätt för åklagare

Förslag: I rättegångsbalken skall det införas en möjlighet för åklagare att i brådskande fall fatta interimistiska beslut i fråga om övervakning enligt 27 kap. 19 § RB. Beslutet skall genast skriftligen anmälas hos rätten, som skyndsamt skall pröva frågan.

I avsnitt 4.2.5 föreslog vi bl.a. att bestämmelsen i 6 kap. 22 § första stycket 3 LEK om skyldighet för operatörer att i vissa fall lämna ut uppgifter som angår särskilda elektroniska meddelanden till brottsutredande myndigheter skulle upphävas. Den bestämmelsen har som framgått inneburit en möjlighet för polis och åklagare att snabbt fatta beslut om att inhämta historiska övervakningsuppgifter och få dessa utlämnade till sig.

När den nämnda paragrafen upphävs och möjligheten för de brottsutredande myndigheterna att få sådana uppgifter i stället regleras genom tvångsmedlet övervakning i 27 kap. 19 § RB, innebär det som framgått att de flera tusen fallen varje år först behöver prövas av domstol innan utlämnande kan ske. Det ligger ett stort värde i att det sker en sådan prövning, särskilt som det kommer att innebära en förstärkning av integritetsskyddet.

Det är självklart att en domstolsprövning av frågan leder till en fördröjning av besluten och till att de brottsutredande myndigheterna inte i samma omfattning kommer att kunna få uppgifterna från operatörerna med lika stor snabbhet som i dag. Myndigheterna har sagt sig vara klart bekymrade över detta och pekat på att just snabbheten i dagens system vid många tillfällen lett till att grövre brott har kunnat klaras upp. Vi har fått flera exempel på verkliga fall där just snabbheten i förfarandet med att få fram uppgifter, särskilt om positionen hos mobiltelefoner, har varit av avgörande betydelse. Exempelvis har rånarligor kunnat gripas tack vare att poli-

sen fått övervakningsuppgifter i akuta skeden i samband med att gärningsmännen har rekognoserat eller varit i färd med att begå själva rånet. Dessutom finns exempel på fall där en mycket snabb tillgång till uppgifterna lett till att gärningsmän till människorov har kunnat gripas kort efter brottet. Det har skett efter att övervakningsuppgifter blivit kända som avslöjade åt vilket håll målsägande och gärningsmän färdats i bil. Ett annat fall av människorov som har nämnts är när en målsägande sattes i en container som sedan lokaliserades innan den hann fraktas bort, tack vare att gärningsmännen använde mobiltelefon vid containern.

Det som nu har sagts aktualiserar frågan om det behövs en möjlighet att fatta interimistiska beslut om övervakning i sådana fall där saken är av så brådskande natur att ett domstolsbeslut inte kan inväntas. I den referensgrupp som är knuten till beredningen har flertalet ledamöter ansett att det behövs en sådan rätt att fatta interimistiska beslut, medan några ledamöter har menat att frågan om övervakning alltid bör prövas av domstol.

Vi framhöll tidigare att en grundläggande utgångspunkt måste vara att den brottsutredande verksamheten inte får förlora i effektivitet genom att möjligheten för myndigheterna att få del av övervakningsuppgifter samlas i rättegångsbalken. Mot bakgrund av de redogörelser vi har fått för hur tillgången till uppgifterna varit av helt avgörande betydelse i akuta skeden vid grova brott, har vi blivit övertygade om att domstolens beslutanderätt om övervakning enligt 27 kap. 19 § RB behöver kompletteras med en interimistisk rätt för åklagare att besluta i brådskande fall. Det kan med andra ord vara helt nödvändigt för ett framgångsrikt utredningsarbete att beslut fattas snabbare än som är möjligt vid en domstolsprövning. Där inkluderas även en prövning som sker vid domstolarnas jourorganisation. På så sätt kan effektiviteten i den brottsbekämpande verksamheten hållas uppe.

Buggningsutredningen kom fram till att det finns ett behov av interimistisk beslutanderätt för åklagare vid tvångsmedlen hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Som regeringen framhåller i lagrådsremissen som följde på Buggningsutredningens förslag, är det självklart att de tvångsmedlen bör omgärdas av särskilda rättssäkerhetsgarantier och att avsteg från detta bör ske endast om det kan antas att syftet med regleringen inte annars kan uppnås.

Vi har valt att lägga fram ett förslag om interimistisk beslutanderätt för åklagare när det gäller övervakning enligt 27 kap. 19 § RB. Av de nyss nämnda tvångsmedlen är det övervakning som är det

minst integritetskänsliga. Det rör sig inte om tillgång till uppgifter om innehållet i meddelanden, alltså t.ex. om tal, och inte heller om dold inspelning med kamera. I stället är det frågan om tillgång till uppgifter rörande t.ex. telefonnummer och lokalisering av mobiltelefon till området för en viss basstation. Mot bakgrund av det stora behov från effektivitetssynpunkt som har framkommit rörande interimistisk beslutanderätt i akuta skeden vid grova brott och med hänsyn till det aktuella tvångsmedlets karaktär, bör det allmänt sett förhållandevis lindriga integritetsintrång som uppstår i sådana relativt få fall inte hindra att åklagare får rätt att fatta beslut i brådskande fall.

Uttrycket i brådskande fall är avsett att i sak innebära detsamma som uttrycket fara i dröjsmål, som diskuterades ingående i Polisrättsutredningens slutbetänkande Tvångsmedel enligt 27 och 28 kap. RB samt polislagen (SOU 1995:47 s. 165 f.). I allmänna termer kan saken uttryckas så att det skall vara så bråttom att ändamålet med en åtgärd kan antas gå förlorat om man väntar med att företa den. Motsvarande uttryck i 1952 års tvångsmedelslag är att det kan befaras att inhämtande av rättens tillstånd till åtgärden skulle medföra fördröjning eller annan olägenhet av väsentlig betydelse för utredningen.

Som Buggningsutredningen föreslog bör det av rättssäkerhets- och kontrollskäl finnas en obligatorisk domstolsprövning av ett interimistiskt beslut. Det bör gälla även i de fall när åtgärden har upphört vid tiden för prövningen. Därmed skapas det också garantier för att beslutanderätten används enbart när det verkligen är befogat.

4.4 Lokalisering av tekniskt hjälpmedel

4.4.1 Nuvarande bestämmelser

Enligt 27 kap. 19 § RB innebär hemlig teleövervakning 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. Uppgifterna skall med andra ord röra telemeddelanden (”uppgifter om telemeddelanden”).

Bland de uppgifter om telemeddelanden som de brottsutredande myndigheterna får tillgång till vid hemlig teleövervakning finns lo-

kaliseringsuppgifter för mobiltelefon, dvs. uppgifter om från vilket geografiskt område ett samtal rings eller tas emot.

Historiska uppgifter rörande positionen hos mobiltelefoner vid samtal har de brottsutredande myndigheterna möjlighet att i dagsläget få från operatörer även genom bestämmelsen i 6 kap. 22 § första stycket 3 LEK. Lokaliseringsuppgifterna utgör det som i 6 kap. 20 § första stycket 3 LEK benämns annan uppgift som angår ett särskilt elektroniskt meddelande. Operatörerna skall enligt gällande regler lämna ut sådana uppgifter som angår ett särskilt elektroniskt meddelande om misstanken rör brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år.

I vårt tidigare betänkande Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74) föreslog vi en bestämmelse i polislagen om användning av vissa tekniska hjälpmedel (10 b § polislagen). Enligt bestämmelsen får en polisman, för att förhindra, avslöja eller utreda brott, vidta vilseledande eller dolda åtgärder genom att använda bl.a. utrustning för positionsbestämning, ofta kallat pejling. Med sådan positionsbestämning avsåg vi metoden att spåra ett föremål genom att en elektronisk utrustning placeras på detta. Metoden används i relativt stor utsträckning inom polisen framför allt vad gäller fordon och containers. Det har hittills skett utan uttryckligt lagstöd. För en närmare beskrivning av innehållet i vårt tidigare förslag hänvisar vi till det nämnda betänkandet. Vi angav där att metoden att lokalisera personer med hjälp av signaler från mobiltelefoner inte avsågs i det sammanhanget (s. 90 f.).

För att de brottsutredande myndigheterna skall vara säkra på att få tillgång till uppgifter från operatörer om positionen hos en mobiltelefon krävs alltså i dag att uppgifterna kan sägas antingen *avse ett telemeddelande* (historiska uppgifter och realtidsuppgifter vid hemlig teleövervakning) eller *angå ett särskilt elektroniskt meddelande* (historiska uppgifter vid utlämnande enligt lagen om elektronisk kommunikation). Det kan som en följd av detta inte uteslutas att det finns en viss osäkerhet om lagstiftningen omfattar lokaliseringsuppgifter rörande en mobiltelefon som är påslagen utan att det samtidigt pågår ett samtal. Skulle sådana lokaliseringsuppgifter inte anses avse ett telemeddelande eller angå ett särskilt elektronisk meddelande, omfattas sådana uppgifter inte av tvångsmedlet hemlig teleövervakning eller av operatörens tystnadsplikt enligt 6 kap. 20 § LEK, vilket innebär att det bör stå operatören fritt att välja att lämna ut historiska uppgifter eller inte till de brottsutredande myndigheterna. Uppgifterna träffas med andra ord då inte heller av utlämnandeskyldigheten för operatörerna i 6 kap. 22 § första stycket 3

LEK. De brottsutredande myndigheterna har i praktiken svårigheter med att få tillgång till lokaliseringsuppgifter rörande mobiltelefoner där det samtidigt inte pågår eller har pågått ett samtal (jfr PTS yttrande den 8 februari 2001, ref 01-88/23).

4.4.2 Buggningsutredningen

Buggningsutredningen tog bl.a. upp frågan om innebörden av tvångsmedlet hemlig teleövervakning i betänkandet Om buggning och andra hemliga tvångsmedel (SOU 1998:46 s. 365 f. och 477 f.). Den definition av tvångsmedlet som Buggningsutredningen föreslog innebar bl.a. att uppgifter i hemlighet fick hämtas in om

1. telemeddelanden som befordras eller har befordrats till eller från en viss teleadress, eller
2. lokaliseringen av en viss teleadress.

Av den föreslagna bestämmelsen framgår att hemlig teleövervakning enligt Buggningsutredningen även uttryckligen skulle omfatta lokaliseringen av en viss teleadress, även utan att det samtidigt t.ex. rings ett samtal. Buggningsutredningen motiverade förslaget på följande sätt (SOU 1998:46 s. 365 f.).

> Av lagtexten till bestämmelsen om hemlig teleövervakning framgår vidare inte vilken information som tvångsmedlet ger åtkomst till, vilket naturligtvis inte heller är nödvändigt under förutsättning att det rör sig om uppgifter som på ett någorlunda naturligt sätt kan anses falla under definitionen av hemlig teleövervakning. Som framgått på en rad olika ställen i betänkandet, bl.a. i avsnitt 2.5.2, innebär emellertid den nuvarande tekniken att det är möjligt att – såvitt avser samtal till eller från en mobiltelefon – ta reda på från vilket geografiskt område ett telefonsamtal rings och var mottagaren av samtalet befinner sig. När en mobiltelefon är påslagen är det vidare möjligt att – utan att något samtal rings – lokalisera i vilket geografiskt område den finns. Det är, menar utredningen, inte klart att denna information, en slags pejling, kan anses rymmas i den nuvarande definitionen av hemlig teleövervakning. Eftersom det tveklöst finns ett stort behov av att få fram sådana uppgifter, och då det ur integritetssynpunkt inte kan anses möta något hinder, anser utredningen att definitionen av hemlig teleövervakning bör ändras så att

det klart framgår att tvångsmedlet får användas även för att lokalisera en viss teleadress.

4.4.3 Lagrådsremissen den 6 april 2000

I den lagrådsremiss som följde på Buggningsutredningens förslag behandlade regeringen frågan om lokaliseringsuppgifter och föreslog att det i definitionen av hemlig teleövervakning uttryckligen skulle framgå att uppgifter i hemlighet kunde hämtas in om var en viss teleadress är lokaliserad. Regeringen anförde följande skäl för förslaget (s. 79 f.).

> Det är i dag möjligt att ta reda på i vilket geografiskt område en mobiltelefon som används eller som endast är påslagen är lokaliserad. De brottsutredande myndigheterna får i dag ofta sådana uppgifter som avses i 45 § första stycket 3 telelagen */6 kap. 20 § första stycket 3 LEK/* och som teleoperatören är skyldig att lämna ut om det för det misstänkta brottet inte är föreskrivet lindrigare straff än fängelse i två år. Som framgår av tidigare avsnitt föreslås att den bestämmelsen upphävs. Eftersom s.k. lokaliseringsuppgifter kan vara av stor betydelse i brottsutredningar bör polisens möjligheter att inhämta sådana uppgifter föras över till rättegångsbalkens regler om hemlig teleövervakning.
>
> Förslaget innebär ett utökat integritetsskydd för andra än den misstänkte; som tidigare framkommit innebär telelagens bestämmelser att uppgifter kan lämnas ut även för andra än de som är misstänkta för brott. Enligt regeringens förslag skall även en teleadress som det finns synnerlig anledning anta att den misstänkte kommer att ringa till eller på annat sätt kontakta kunna omfattas av hemlig teleövervakning. Regeringen anser emellertid inte att utvidgningen skall få genomslag på frågan om samtalslokalisering. Det finns inget behov av att få ut lokaliseringsuppgifter beträffande en teleadress som den misstänkte kan antas kontakta. En sådan möjlighet bör därför inte heller införas.

Lagrådet uttalade sig inte särskilt över frågan om positionsbestämning annat än att man lämnade förslag på vissa justeringar av lagteknisk karaktär.

4.4.4 Våra överväganden

Förslag: Av bestämmelserna om övervakning i rättegångsbalken skall det uttryckligen framgå att tvångsmedlet får användas för att hämta in uppgifter för lokalisering. Med uppgifter för lokalisering skall avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits (oavsett om det tekniska hjälpmedlet används eller har använts för samtal eller inte).

Som har framgått rör lokaliseringsfrågan tillgång till uppgifter rörande positioner hos mobiltelefoner. Lokaliseringsuppgifterna genereras såväl vid samtal som när mobiltelefonen enbart är påslagen utan att det samtidigt pågår ett samtal. Uppgifterna kommer av den kontakt som mobiltelefonen har med basstationerna. Den kontakten ”registreras” och ger, om uppgifterna lämnas ut, möjlighet för de brottsutredande myndigheterna att få reda på inom vilket område en mobiltelefon har befunnit sig vid en viss tidpunkt. Hur precisa uppgifterna är beror främst på vilken yta basstationen täcker. Områdena kan sträcka sig från några hundra meter i stadsmiljö till flera mil ut från basstationerna på landsbygden. Inom den aktuella ytan är det däremot inte möjligt att med exakthet avgöra var mobiltelefonen finns eller har funnits. Något mer exakta uppgifter kan fås i det fallet att en mobiltelefon bryter kontakten med en basstation för att därefter få kontakt med en annan. I det sammanhanget är det möjligt att sluta sig till i vilken riktning mobiltelefonen har rörts.

Som även framgår av avsnitt 4.3.5 och 7.5 kan uppgifter för lokalisering många gånger vara oerhört värdefulla vid utredning av framför allt allvarlig brottslighet, som mord, människorov, grovt rån och grovt narkotikabrott samt den brottslighet som faller inom Säkerhetspolisens område, som olika former av terroristbrott. Från polis- och åklagarhåll har det även framhållits att lokaliseringsuppgifterna vid många tillfällen har bidragit till att misstankar mot personer har kunnat avskrivas.

Det är uppenbart att uppgifter om positionen hos mobiltelefoner, vare sig de genereras vid pågående samtal eller inte, kan ha mycket stor betydelse i effektivitetshänseende, särskilt vid utredning av grova brott (se t.ex. slutrapporten från juni 2004 ”Organiserad kriminalitet, grov narkotikabrottslighet” av den nationella narkotikapolitiska samordningen Mobilisering mot narkotika, S 2002:03, s. 96).

Det finns tveklöst ett mycket stort behov av att få tillgång till sådana uppgifter i förundersökningar. Genom bestämmelserna om hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation får myndigheterna lokaliseringsuppgifter redan i dag, i vart fall uppgifter som genereras i samband med att samtal pågår.

Såväl av Buggningsutredningens betänkande som av den följande lagrådsremissen framgår att det bör uttryckligen klargöras i lagstiftningen att hemlig teleövervakning får användas för att lokalisera en teleadress, oavsett om uppgifterna har samband med ett samtal eller inte. Vi instämmer i den bedömningen och i konstaterandet att ett sådant klargörande inte kan möta några avgörande hinder från integritetssynpunkt. Som en följd av förslaget att upphäva bestämmelsen om utlämnande enligt 6 kap. 22 § första stycket 3 LEK kommer i fortsättningen myndigheterna att få lokaliseringsuppgifter enbart genom reglerna om övervakning i rättegångsbalken. Som konstaterades i lagrådsremissen kommer detta i sig att innebära ett utökat integritetsskydd. Till detta kommer också den betydelse lokaliseringsuppgifterna har när det gäller att avföra oskyldiga personer från misstankar om brott.

Sedan den 1 oktober 2004 gäller enligt 27 kap. 20 § första stycket RB att hemlig teleövervakning får avse även en teleadress som det finns synnerlig anledning anta att den misstänkte har ringt till eller kontaktat (historiska uppgifter) respektive kommer att ringa till eller kontakta (realtidsuppgifter). Tillstånd kan med andra ord ges till hemlig teleövervakning av andra teleadresser än sådana som den misstänkte själv innehar eller har innehaft respektive använder eller har använt sig av.

Frågan är om det skall vara möjligt att positionsbestämma även andra personers mobiltelefoner, alltså tekniska hjälpmedel som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta. Förslaget i den tidigare lagrådsremissen var att sådana lokaliseringsuppgifter inte skulle få inhämtas. Regeringen motiverade detta med att det inte finns något behov för de brottsutredande myndigheterna av att få tillgång till sådana uppgifter (s. 80).

I avsnitt 4.3.5 behandlade vi frågan om övervakning utan misstänkt gärningsman och kom fram till att det vid förundersökning rörande brott som är så allvarliga att de kan ligga till grund för beslut om avlyssning, skall övervakning få användas även om det inte finns någon som är skäligen misstänkt för brottet. Vi redogjorde något i avsnittet för hur arbetet med historiska uppgifter bedrivs i

brottsutredningar. Det gällde bl.a. lokaliseringsuppgifter rörande mobiltelefoner inhämtade med stöd av lagen om elektronisk kommunikation. Vid grövre brott och särskilt i samband med att skäligen misstänkta personer saknas i utredningen kan polisen genom sådana uppgifter kartlägga hur brotten planerats, genomförts och vad gärningsmännen gjort därefter och på så sätt även identifiera misstänkta gärningsmän och klarlägga gärningsmännens agerande. Vi upprepar inte ytterligare vad som nämndes i det tidigare avsnittet utan kan konstatera att det finns ett uppenbart behov hos de brottsutredande myndigheterna att kunna inhämta särskilt historiska lokaliseringsuppgifter rörande mobiltelefoner utan de begränsningar till vissa tekniska hjälpmedel som nämndes tidigare.

Från polishåll har det framförts att det föreligger ett behov av sådana uppgifter även i andra fall. Det är framför allt kopplat till olika smugglingssituationer, t.ex. rörande narkotika. Ett vanligt agerande är då att den kurir som tar godset över gränsen har order om att i ett visst läge ringa ett telefonnummer, vilket polis och tull på annat sätt har identifierat. Vem som innehar den telefonen är däremot oftast okänt för de brottsutredande myndigheterna. För att kunna utreda brottsligheten på ett effektivt sätt menar myndigheterna att det är viktigt att de ges möjlighet att få positionsuppgifter avseende detta tekniska hjälpmedel. Vi instämmer i den bedömningen och föreslår inte någon begränsning i det avseendet.

4.5 Identifiering av tekniskt hjälpmedel

4.5.1 Nuvarande bestämmelser

Hemlig teleavlyssning och hemlig teleövervakning får ske endast om någon är skäligen misstänkt för ett brott av viss svårhetsgrad och åtgärden är av synnerlig vikt för utredningen. Dessutom får åtgärden enligt 27 kap. 20 § första stycket RB enbart avse vissa teleadresser, nämligen

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.

Enligt 27 kap. 21 § andra stycket RB skall det i domstolens beslut att tillåta hemlig teleavlyssning eller hemlig teleövervakning anges bl.a. vilken teleadress tillståndet gäller.

4.5.2 Problem som skapas genom användning av anonyma kontantkort

Det har under lång tid skett en stadig ökning av antalet mobiltelefonabonnemang i Sverige. Det totala antalet abonnemang per capita uppgick den 31 december 2003 till nära 981 abonnemang per 1000 invånare, vilket är en ökning med drygt nio procent jämfört med motsvarande tidpunkt ett år tidigare (PTS rapport Svensk telemarknad 2003 s. 33 ff.).

Det finns en tydlig tendens bland mobiltelefonkunder att använda s.k. kontantkort i stället för att teckna kontraktsabonnemang. Från att i stort sett inte ha förekommit år 1996 uppgick antalet aktiva kontantkort den 31 december 2003 till 5 003 000 stycken, eller närmare 58 procent av samtliga GSM-abonnemang (se den angivna rapporten från PTS). Operatörer har ofta behov av att hålla register med uppgifter över sina abonnenter, kanske främst för att kunna sköta sin fakturering. Innehavarna av kontantkorten med förutbetalda tjänster förblir dock i regel anonyma för operatören, om inte innehavaren själv väljer att lämna abonnemangsuppgifter till denne.

I dagsläget är det mycket vanligt att mobiltelefoner på olika sätt används vid brottslig verksamhet. Det är ofta ett problem för de brottsutredande myndigheterna att kriminella personer har fullt klart för sig vilka gränser som finns för myndigheternas operativa möjligheter och utnyttjar den kunskapen i sin brottsliga verksamhet. Den anonymitet som kontantkorten ger och fördelarna med anonymiteten är enligt uppgifter från polisen helt känd i kriminella kretsar ”ner på lägsta nivå” och utnyttjas av personer vid all typ av brottslighet i syfte att försvåra eller omöjliggöra de brottsutredande myndigheternas arbete. Allt sker givetvis mot bakgrund av att det ofta ligger ett högt bevisvärde i den information hemlig teleavlyssning och hemlig teleövervakning kan ge.

Som framgår krävs det i dag enligt rättegångsbalken att det finns en skäligen misstänkt person för att hemlig teleavlyssning och hemlig teleövervakning skall kunna komma i fråga. Dessutom krävs

att det finns identifierade teleadresser som dessutom skall anges i domstolens beslut. I det föreliggande betänkandet lägger vi fram förslag som kommer att effektivisera brottsutredningsarbetet i olika avseenden. På liknande sätt som det i dag föreskrivs i lagen om elektronisk kommunikation skall det enligt vårt förslag i fortsättningen i vissa fall inte krävas att det finns en skäligen misstänkt person för att övervakning skall få användas. När det finns en skäligen misstänkt person skall tvångsmedlen avseende den personen även fortsättningsvis inte få avse andra identifierade tekniska hjälpmedel (teleadresser) än som i dag framgår av 27 kap. 20 § första stycket RB, men hjälpmedlet skall inte behöva anges i domstolens beslut (se avsnitt 4.3.5).

Ett stort effektivitetsproblem är även att verkställigheten av tvångsmedelsbesluten, oavsett hur lagstiftningen ser ut, måste knytas till identifierade teleadresser i förhållande till operatörerna. Med undantag i vart fall för s.k. basstationstömning (se avsnitt 2.6) är en förutsättning för att tvångsmedelsbesluten över huvud taget skall kunna verkställas att de brottsutredande myndigheterna har identifierat en teleadress som skall omfattas av avlyssningen eller övervakningen och att operatörerna för sina åtgärder vid verkställigheten får den uppgiften av myndigheterna. För att besluten i praktiken skall kunna verkställas måste alltså operatörerna, oavsett vilka krav lagstiftningen i övrigt ställer, få uppgift av de brottsutredande myndigheterna om vissa angivna teleadresser.

När de brottsutredande myndigheterna har identifierat en skäligen misstänkt person innebär det givetvis inte att myndigheterna även har klart för sig vilka teleadresser som den personen disponerar eller t.ex. kan komma att kontakta. Det är där problemet med de anonyma kontantkorten finns. Det är i stort sett undantagslöst så att de kriminella personerna köper, byter och slänger mobiltelefoner och/eller anonyma kontantkort mycket frekvent. Därigenom ändras också de teleadresser som används. Dessutom används flera telefoner och flera kort parallellt av samma person.

Företrädare för Säkerhetspolisen, Rikskriminalpolisen och länskriminalpolisen i Stockholm har alla uttryckt för oss att anonyma kontantkort utgör ett av de absolut största effektivitetshindren vid utredning av grova brott. De anonyma kontantkorten och kravet på att teleadresser skall vara identifierade för att tvångsmedlen skall kunna beslutas och verkställas skapar så stora problem i brottsutredningarna att polisen uttrycker det som ”en utredningsmässig, tidsmässig och resursmässig katastrof”. Det sägs att det läggs ned ”fruktansvärt stora resurser” på att på olika sätt ändå identifiera de

teleadresser som används av brottslingarna. Vi beskriver inte här hur det arbetet går till annat än att ange 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 en uppenbar risk för att arbetet med att identifiera teleadresserna blir resultatlöst, vilket innebär att hemlig teleavlyssning och hemlig teleövervakning över huvud taget inte kan användas i arbetet med att utreda grova brott.

Rikspolisstyrelsen har givit in en skrivelse till oss rörande anonyma kontantkort och begärt att det skall föreskrivas en skyldighet för operatörer att registrera uppgifter om abonnemang för kontantkort och uppgifter som visar var och när kortet köptes (RÄS-000-5200/04). Vi behandlar den frågan i avsnitt 5.6. Det måste dock redan här sägas att vi kommer fram till att det finns effektivitetsproblem med den ordning Rikspolisstyrelsen föreslår. Bl.a. skulle det vara allt för lätt för de kriminella personerna att komma runt ”kontrollen” genom att t.ex. anlita bulvaner vid köpen. I avsaknad av bl.a. en utvärdering av den lagstiftning som finns på området i andra länder framstår en sådan ordning inte som tillräckligt effektiv. Rikspolisstyrelsens förslag om skyldighet att registrera abonnemangsuppgifter till kontantkort bör enligt vår mening inte genomföras nu.

Rikspolisstyrelsen berör i sin skrivelse även svårigheten för de brottsutredande myndigheterna att över huvud taget identifiera en teleadress och anger bl.a. följande.

> Den anonymitet som kontantkort ger är i dag väl känd i kriminella kretsar och korten används i hög grad för att försvåra Polisens arbete. Den närmast explosionsartade ökningen av mobiltelefonabonnemang och intresset för kontantkort har emellertid medfört att mobiltelefoner med kontantkortabonnemang i dag är vanliga i alla typer av utredningar.
>
> När det gäller den mer organiserade brottsligheten har utvecklingen gått så långt att det i exempelvis utredningar av narkotikabrott endast i undantagsfall förekommer mobiltelefoner med kontraktsabonnemang. Likaså är det i dag mycket vanligt att mobiltelefoner med kontantkortsabonnemang används i sådan brottslighet som ligger inom Säkerhetspolisens kompetensområde.
>
> Polisens möjligheter att få tillgång till abonnemangsuppgifter är ofta avgörande för om en brottsutredning skall vara

framgångsrik. Om exempelvis en person är skäligen misstänkt för ett allvarligt brott, kan brottsutredande myndigheter vilja använda hemlig teleavlyssning och hemlig teleövervakning i det fortsatta utredningsarbetet. En förutsättning för tvångsmedlet är emellertid att det går att identifiera en teleadress, exempelvis telefonnummer, som den misstänkte innehar eller annars kan komma att använda. När det saknas abonnentförteckningar måste polisen emellertid helt förlita sig på andra spaningsmetoder för att fastställa vilket mobiltelefonnummer det är fråga om. Viktig tid går härigenom förlorad. Det finns givetvis också en överhängande risk för att Polisen aldrig kan identifiera den aktuella mobiltelefonen.

4.5.3 Våra överväganden

Förslag: Övervakning enligt 27 kap. 19 § RB skall i fortsättningen även innebära att uppgifter i hemlighet får hämtas in för identifiering av tekniska hjälpmedel.

Med uppgifter för identifiering skall avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden.

Övervakning i syfte att identifiera tekniska hjälpmedel skall få avse sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte.

Användningen av anonyma kontantkort i brottslig verksamhet innebär ett allvarligt effektivitetsproblem för de brottsutredande myndigheterna. Det är ytterligt otillfredsställande att personer som sysslar med grov brottslighet genom så relativt enkla åtgärder som det är frågan om kan undvika en verkställighet av tvångsmedel i de fall där detta är av synnerlig betydelse för det brottsutredande arbetet. Om inget görs för att förhindra detta, kommer den grova brottsligheten att i många fall ha ett försprång framför de brottsutredande myndigheterna. Det är uppenbart att i flertalet sådana fall kommer brottsligheten inte att avslöjas. I andra fall kommer avslöjandet inte att kunna ske utan att betydande resurser förbrukas.

Då inställer sig frågan vad som kan göras åt problemet. Enligt uppgifter från Säkerhetspolisen finns det möjligheter att med hjälp av en speciell typ av tekniskt hjälpmedel, som används i vissa närliggande länder, identifiera andra tekniska hjälpmedel, dvs. de teleadresser som är aktuella och som används av en viss person. Meto-

den ger på ett relativt enkelt sätt uppgift om vilka tekniska hjälpmedel som finns inom ett begränsat geografiskt område. Den ger alltså uppgift om vilka telefonnummer, koder eller andra teleadresser som används inom området. De brottsutredande myndigheterna får genom metoden kännedom inte enbart om det tekniska hjälpmedel som är intressant för myndigheterna utan även om andra som används i närheten. Allt efter omständigheterna kräver då detta att något fler än en enda ”sökning” sker i området kring en misstänkt person för att ett visst tekniskt hjälpmedel skall kunna ”ringas in”. Det sker genom en jämförelse mellan uppgifterna från de olika platserna. Det geografiska området i vilka de korta sökningarna sker (någon enstaka sekund) kan begränsas genom att utrustningens räckvidd justeras efter de enskilda förhållandena. Utgångspunkten är då att man genom fysisk spaning har klart för sig var inom ett klart begränsat område det tekniska hjälpmedel finns som man vill ha uppgift om. I stadsmiljö kan det i praktiken röra sig om en radie på högst ett hundratal meter. Därigenom begränsas också avsevärt de uppgifter som ges om vilka tekniska hjälpmedel som används i övrigt på platsen. För tydlighetens skull måste nämnas att det alltså inte är fråga om att avlyssna innehållet i meddelanden utan enbart att få fram uppgifter som identifierar de tekniska hjälpmedlen, alltså det som i nuvarande bestämmelser i 27 kap. RB benämns teleadresser.

Vi ser ingen anledning att ifrågasätta Säkerhetspolisens bedömning av att utrustningen i sig skulle fungera mycket effektivt och att en användning av den i brottsutredningssammanhang på många sätt skulle innebära en kraftfull effektivitetshöjning för myndigheterna. Säkerhetspolisen har för övrigt tillagt att den teknik det är fråga om bygger på samma princip som den som används av operatörerna för att ge de brottsutredande myndigheterna uppgifter för lokalisering.

Vi har alltså konstaterat att det finns ett påtagligt behov i det brottsutredande arbetet av att kunna identifiera tekniska hjälpmedel. Dessutom framstår den metod som Säkerhetspolisen har redogjort för som effektiv. Under förutsättning att inga avgörande hinder möter från integritetssynpunkt, menar vi därför att de brottsutredande myndigheterna genom lagstiftning bör ges rätt att använda sig av en sådan metod vid förundersökningar.

Det är ofta en svår uppgift att avväga integritetsintresset mot nödvändigheten av att myndigheterna har effektiva metoder för bl.a. brottsutredning. Det ligger i sakens natur att sådana metoder ofta innefattar ett integritetsintrång. Samtidigt måste beaktas att

detta intrång ofta är blygsamt i jämförelse med den kränkning som offren för den allvarliga brottsligheten måste utstå. Ju allvarligare och ju mer svårutredd som brottsligheten blir, desto mer tvingas statsmakterna tillåta i form av tvångsåtgärder i brottsbekämpningen. Det kan aldrig accepteras att brottsligheten tar överhanden och att statsmakterna kapitulerar inför utvecklingen av en allt mer avancerad och förslagen brottslighet.

Vid användning av den nu aktuella metoden får som sagt de brottsutredande myndigheterna inte uppgifter om innehållet i ett meddelande, alltså om innehållet i kommunikationen (jfr avlyssning enligt 27 kap. 18 § RB), utan uppgifter om vilka tekniska hjälpmedel som används på en viss plats. Det uppstår då ett visst integritetsintrång hos den person som åtgärden riktar sig mot. För det fall tredje man använder en mobiltelefon inom det geografiska område som undersöks, uppstår ett intrång även hos denne. Det måste dock framhållas att uppgifterna som avser tredje man ofta i praktiken kommer att avse anonyma kontantkort. De brottsutredande myndigheterna kommer i stort sett aldrig att knyta de uppgifterna till namngivna personer.

Att metoden ger uppgifter om tekniska hjälpmedel innebär att den i praktiken har stora likheter med övervakning enligt 27 kap. 19 § RB. Enligt den bestämmelsen i dess nuvarande lydelse innebär hemlig teleövervakning 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. Uppgifterna skall med andra ord röra telemeddelanden (”uppgifter om telemeddelanden”). Som vi har nämnt på flera håll i betänkandet kan uppgifter om telemeddelanden vara exempelvis uppringt nummer, uppringande nummer och IMEI-numret. Även lokaliseringsuppgifter vad gäller mobiltelefon omfattas av tvångsmedlet.

Genom vårt förslag till förändring av paragrafen som framgår av avsnitt 3 och 4.4 skulle övervakning komma att innebära att uppgifter i hemlighet fick hämtas in om meddelanden som befordras eller har befordrats med tekniskt hjälpmedel till eller från ett elektroniskt kommunikationsnät och även för lokalisering av ett sådant tekniskt hjälpmedel. Meddelanden skulle även få hindras från att nå fram till eller lämna ett sådant tekniskt hjälpmedel.

Liksom i andra fall kan det vara svårt att generellt ange omfattningen av det integritetsintrång som skulle blir följden av en användning av metoden att identifiera tekniska hjälpmedel. I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte

kommer att bli större än vid hemlig teleövervakning. Mot bakgrund av vad som tidigare nämndes om behovet av metoden, där en identifiering av de tekniska hjälpmedlen ofta utgör en förutsättning för att över huvud taget kunna använda tvångsmedlen vid grov brottslighet, och om effektiviteten, kan det förhållandevis ringa integritetsintrång som typiskt sett uppkommer inte utgöra tillräckliga skäl för att avstå från en lagstiftning på området. Det är alltså inte försvarligt att avstå från den vinst som metoden skulle ge vid bekämpningen av särskilt den grova brottsligheten.

Lagstiftningen kan givetvis utformas på olika sätt. Det är exempelvis möjligt att se metoden som en slags verkställighetsåtgärd till ett fattat beslut om avlyssning eller övervakning.

Det är dock självklart att en reglering av metoden skall omgärdas av tillräckliga rättssäkerhetsgarantier bl.a. så att bestämmelserna inte kan missbrukas, att allmänheten kan acceptera bestämmelserna och ha tilltro till myndigheterna och så att integritetsintrånget hos den misstänkte och andra begränsas eller till och med undviks. Detta uppfylls enligt vår mening bäst om identifieringen av tekniska hjälpmedel blir en del av tvångsmedlet övervakning enligt 27 kap. 19 § RB.

Genom den ordningen kommer de rättssäkerhetsgarantier och andra krav som omgärdar tvångsmedlet även att gälla för den nu aktuella metoden. Det betyder att någon skall vara skäligen misstänkt för ett brott som det enligt huvudregeln inte är föreskrivet lindrigare straff än fängelse i sex månader för. Åtgärden skall också vara av synnerlig vikt för utredningen och skall, om det inte är fråga om brådskande fall, prövas av rätten på ansökan av åklagaren. I tillståndet, som får gälla i högst en månad åt gången, får rätten föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när. Sådana villkor kan gälla platsen för användningen av metoden och avståndet mellan polisens utrustning och det tekniska hjälpmedel som skall identifieras. Det är också självfallet så att de principer som i övrigt gäller vid all tvångsmedelsanvändning skall beaktas av myndigheterna (se t.ex. proportionalitetsprincipen i 27 kap. 1 § tredje stycket RB och 8 § polislagen).

Vi föreslår med andra ord att övervakning enligt 27 kap. 19 § RB i fortsättningen även skall innebära att uppgifter i hemlighet får hämtas in för identifiering av tekniska hjälpmedel. Med uppgifter för identifiering skall avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden. Övervakning i syfte att identifiera tekniska hjälpmedel skall få avse sådana tekniska hjälpmedel som kan antas användas

eller komma att användas för meddelanden till eller från den misstänkte. Genom att lagstiftningen utformas på det viset kommer metoden att kunna användas för att identifiera de tekniska hjälpmedel som anges i 27 kap. 20 § första stycket RB, nämligen

1. sådana tekniska hjälpmedel 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. sådana tekniska hjälpmedel 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.

Beroende på omständigheterna kan exempel på de sistnämnda tekniska hjälpmedlen vara sådana som innehas av medlemmar i samma kriminella gäng som den misstänkte tillhör.

I 27 kap. 25 § första stycket RB anges att när rätten har lämnat tillstånd till avlyssning och övervakning får de tekniska hjälpmedel som behövs för åtgärden användas.

4.6 Övervakningsuppgifter vid avlyssning

4.6.1 Nuvarande bestämmelser

Hemlig teleavlyssning innebär att innehållet i ett telemeddelande blir tillgängligt för de brottsutredande myndigheterna. Vid hemlig teleövervakning får myndigheten i stället ”uppgifter om telemeddelanden” och myndigheten kan också hindra telemeddelanden från att nå fram (27 kap. 18-19 §§ RB).

Regeringen påpekade i skrivelsen till riksdagen om tillämpningen av bestämmelserna i rättegångsbalken om hemlig teleavlyssning och hemlig teleövervakning (Skr. 2004/05:36), att antalet tillstånd till hemlig teleövervakning hade ökat kraftigt sedan år 1996. Det kunde enligt regeringen till stor del förklaras av att utvecklingen varit den att ansökningar om tillstånd till hemlig teleavlyssning regelmässigt kombineras med ansökan om tillstånd till hemlig teleövervakning.

Även av de uppgifter vi har inhämtat framgår att det i dag, i princip alltid, tillämpas den ordningen att ett tillstånd till hemlig teleavlyssning kombineras med ett tillstånd till hemlig teleövervakning. Orsaken är främst att hemlig teleavlyssning ger de brottsut-

redande myndigheterna åtkomst enbart till innehållet i ett telemeddelande men inte till uppgifterna som rör just det telemeddelandet, exempelvis från vilken teleadress det inkommande samtalet rings.

4.6.2 Buggningsutredningen

Buggningsutredningen diskuterade frågan om vilka uppgifter hemlig teleavlyssning borde ge de brottsutredande myndigheterna och skrev följande (SOU 1998:46 s. 362 ff.).

> Slutligen skall utredningen beröra ytterligare en frågeställning som är av betydelse för hur tvångsmedlet hemlig teleavlyssning bör definieras. Det har i ett förhållandevis sent skede av utredningsarbetet framhållits att de brottsutredande myndigheterna vid hemlig teleavlyssning i princip alltid har behov av att få uppgift om identiteten på de teleadresser som kommer i kontakt med den avlyssnade teleadressen. Det har vidare sagts att sådana uppgifter redan i dag lämnas ut av teleoperatören utan att det föreligger ett särskilt beslut om hemlig teleövervakning. Vissa hävdar rent av, enligt principen att det större innefattar det mindre (major includit minor), att ett beslut om hemlig teleavlyssning redan enligt gällande rätt innefattar även teleövervakningsuppgifter. Det har dessutom påstått att den framtida tekniken kommer att innebära att det på sikt inte blir möjligt att separera teleövervakningsoch teleavlyssningsuppgifter, vilket skulle innebära att teleoperatören, vid verkställighet av ett beslut om hemlig teleavlyssning, med nödvändighet kommer att leverera även teleövervakningsuppgifter.
>
> Enligt utredningens uppfattning torde det inte råda något tvivel om att teleövervakningsuppgifter enligt gällande rätt kan lämnas ut lagligen endast under förutsättning att det finns ett särskilt beslut om hemlig teleövervakning. Här bortses från att sådana uppgifter i vissa fall enligt telelagen och sekretesslagen kan lämnas ut efter samtycke från den som berörs av åtgärden. Även om man kan tycka att det inte är helt orimligt att ett beslut om hemlig teleavlyssning borde innefatta även teleövervakningsuppgifter, finns det inget klart stöd, vare sig i lag eller förarbeten, för tanken att det större innefattar det mindre. Det uttalande som lämnades i prop. 1988/89:124 s. 48, när institutet hemlig teleövervak-

ning infördes i rättegångsbalken, nämligen: ”När tillstånd till telefonavlyssning meddelats torde dock med stöd av tillståndet uppgift också lämnas om de samtal som rings till eller från den avlyssnade apparaten.” syftar, menar utredningen, på det tidigare rättsläget, nämligen när tvångsmedlet hemlig teleövervakning fanns endast i 1952 års tvångsmedelslag, och kan inte tas till intäkt för en sådan tolkning.

Det ovan redovisade kan emellertid tala för att bestämmelsen om hemlig teleavlyssning bör utformas så att den omfattar även teleövervakningsuppgifter. Utredningen har övervägt en sådan lösning men avfärdat den, bl.a. på grund av att frågan har väckts så pass sent under utredningsarbetet att det inte funnits tid att undersöka vad den framtida tekniken kommer att innebära eller vad en sådan lösning skulle få för konsekvenser. Det finns alltså inte tillräckligt underlag för att föreslå en sådan lösning. Inte heller finns det i utredningens direktiv någon antydan om att man från regeringens sida kan tänka sig en ordning som innebär att hemlig teleavlyssning skall innefatta även hemlig teleövervakning. Frågan bör dock följas upp och – i ett annat sammanhang – bli föremål för fortsatta överväganden.

Däremot menar utredningen att det finns tillräckligt underlag för att låta hemlig teleavlyssning omfatta vissa av de uppgifter som enligt gällande rätt kan fås endast om det föreligger ett beslut om hemlig teleövervakning, närmare bestämt uppgifter om mellan vilka teleadresser meddelandet har utväxlats. En sådan lösning framstår också som godtagbar ur integritetssynpunkt. Enligt vad som sagts utredningen finns det ett stort behov av att samtidigt med innehållet i ett samtal få tillgång till sådana uppgifter, eftersom man i annat fall inte vet mellan vilka teleadresser samtalet utväxlas. Man kan naturligtvis hävda att inget hindrar att de brottsutredande myndigheterna i så fall alltid ansöker om såväl hemlig teleavlyssning som hemlig teleövervakning. Hemlig teleövervakning innefattar emellertid inte bara nu nämnda uppgifter utan även en rad andra uppgifter samt en möjlighet att hindra ett telemeddelande från att nå fram, vilket de brottsutredande myndigheterna kanske inte har något behov av i det enskilda fallet. Det är givetvis från integritetssynpunkt angeläget att inte fler uppgifter lämnas ut än som behövs. Det framstår vidare som en onödig åtgärd att i princip alltid behöva ansöka om såväl hemlig teleavlyssning som hemlig teleövervakning.

Hemlig teleavlyssning bör därför omfatta inte bara innehållet i ett telemeddelande utan även uppgifter om mellan vilka teleadresser det avlyssnade samtalet utväxlas.

4.6.3 Lagrådsremissen den 6 april 2000

I den lagrådsremiss som följde på Buggningsutredningens förslag konstaterade regeringen att det i samband med hemlig teleavlyssning ofta uppstår behov av att få veta vilka teleadresser som kommer i kontakt med den avlyssnade adressen. Regeringen instämde i Buggningsutredningens förslag om att hemlig teleavlyssning även skulle innebära att uppgifter om mellan vilka teleadresser meddelandet utväxlats får inhämtas. Regeringen menade dock att även uppgifter om samtalets längd borde kunna inhämtas vid hemlig teleavlyssning och motiverade sitt förslag på följande sätt (s. 73 f.).

Regeringen delar utredningens bedömning att det inte med stöd av nuvarande bestämmelser kan utläsas att även teleövervakningsuppgifter får lämnas ut efter ett beslut om hemlig teleavlyssning. Denna osäkerhet bör undanröjas. Man torde dock kunna utgå från att de omständigheter som ligger till grund för möjlighet till hemlig teleavlyssning också kan ge rätt till hemlig teleövervakning. Det framstår då som opraktiskt att åklagaren skall behöva, för säkerhets skull, ansöka om tillstånd till båda tvångsmedlen. Effektivitetsskäl talar därför för att införa en regel om att beslut om hemlig teleavlyssning också får innebära att uppgift får inhämtas om mellan vilka teleadresser de avlyssnade meddelandena utväxlas.

Rikspolisstyrelsen har särskilt tagit upp frågan om uppgift om samtalets längd. Uppgift om samtalets längd är främst av teknisk art. Hur lång tid ett samtal pågick kan dock ha stor betydelse i brottsutredningar. För att underlätta polisens arbete bör även uppgift om samtalets längd innefattas i ett beslut om hemlig teleavlyssning. Regeringen föreslår därför en sådan ändring av bestämmelserna om hemlig teleavlyssning.

Regeringens förslag innebär att om beslutet om teleavlyssning faller, t.ex. på grund av att det inte längre finns skäl för en sådan ingripande åtgärd, så faller därmed även beslutet till den del det avser de nu behandlade teleövervakningsuppgif-

terna. Finns det fortfarande skäl för hemlig teleövervakning, får åklagaren ansöka om tillstånd till det tvångsmedlet.

Lagrådet yttrade sig inte särskilt över frågan om teleövervakningsuppgifter bör få inhämtas vid hemlig teleavlyssning.

4.6.4 Våra överväganden

Förslag: Har tillstånd givits till avlyssning skall även övervakningsuppgifter (uppgifter om meddelanden och för lokalisering eller identifiering av tekniska hjälpmedel) få hämtas in med stöd av tillståndet och meddelanden hindras från att nå fram till eller lämna ett visst tekniskt hjälpmedel.

Hemlig teleavlyssning innebär som sagt att innehållet i ett telemeddelande blir tillgängligt medan hemlig teleövervakning ger myndigheterna uppgifter om telemeddelanden. Det rör sig exempelvis om uppgifter om uppringt respektive uppringande nummer, start- och sluttider, antalet ringsignaler, IMEI- och IMSI-numren och uppgifter för lokalisering. Vi föreslog i avsnitt 4.5.3 att även uppgifter för identifiering av tekniskt hjälpmedel skulle höra till den kategorin.

Det är naturligt att den information som hemlig teleövervakning därmed ger i de allra flesta fall är nödvändig att få tillgång till för de brottsutredande myndigheterna även vid hemlig teleavlyssning, där innehållet i ett telemeddelande blir tillängligt utan att myndigheten samtidigt får reda på exempelvis vilken teleadress som har varit i kontakt med den avlyssnade. Som Buggningsutredningen konstaterade finns det i princip alltid ett sådant operativt behov.

Ytterligare en förklaring till att ansökan görs om tillstånd till båda tvångsmedlen samtidigt är att den teknik som i dag finns tillgänglig inte gör det möjligt att separera avlyssningsdelen från vissa övervakningsuppgifter. Även detta berördes av Buggningsutredningen. Vilka teleövervakningsuppgifter som de brottsutredande myndigheterna automatiskt får vid hemlig teleavlyssning är hemligt. För att inte bryta mot lagstiftningen begär de brottsutredande myndigheterna tillstånd till båda tvångsmedlen.

Den ordning som tillämpas i dagsläget överensstämmer som framgått med den slutsats som såväl Buggningsutredningen som regeringen tidigare kom fram till, nämligen att teleövervakningsuppgifter inte kan hämtas in vid hemlig teleavlyssning. Det är rik-

tigt även enligt vår mening. Domstolen måste i stället ha gett tillstånd till hemlig teleövervakning.

Det finns med andra ord skäl som kan sägas vara såväl operativa som mer formella för att kombinera tvångsmedlen på det sätt som nu sker i praktiken. Detta ger anledning till att överväga hur ordningen bör vara i framtiden. Det gäller särskilt som det regelmässigt är så att de omständigheter som ligger till grund för hemlig teleavlyssning ger rätt till hemlig teleövervakning. Från den utgångspunkten framstår det, som uttalas av Buggningsutredningen och i lagrådsremissen, som onödigt och opraktiskt att ansökan görs och tillstånd ges till båda tvångsmedlen samtidigt.

Buggningsutredningens och lagrådsremissens förslag innebar att enbart vissa teleövervakningsuppgifter skulle göras tillgängliga för myndigheterna vid tillstånd till hemlig teleavlyssning. Det rörde vilken teleadress som varit i kontakt med den avlyssnade adressen respektive telemeddelandenas längd i tid. För att få övriga uppgifter skulle myndigheterna behöva få tillstånd även till hemlig teleövervakning. Buggningsutredningen motiverade det begränsade förslaget i första hand med att utredningen inte hade haft tid att undersöka vad den framtida tekniken kommer att innebära eller vilka konsekvenser en ordning skulle få som innefattar att bestämmelsen om hemlig teleavlyssning utformas så att tvångsmedlet även ger tillgång till övriga teleövervakningsuppgifter.

Den teknik som används i sammanhanget bygger på internationell standard. I ett internationellt perspektiv är det mer ovanligt med den uppdelning som förekommer i Sverige på flera tvångsmedel rörande dels innehållet i telemeddelanden, dels uppgifter om dessa. Därför ger de tekniska lösningarna i grunden även vissa teleövervakningsuppgifter vid tillstånd till hemlig teleavlyssning. Enligt uppgift skulle det ur teknisk synvinkel i och för sig vara möjligt att separera de två typerna av information. Detta skulle dock kräva att operatörerna lägger ner resurser på att specialanpassa sina system för det ändamålet. Hittills har det inte skett. Det saknas i dag skäl att tro att den internationella standarden kommer att förändras mot en större uppdelning av informationen.

Av vad som har sagts framgår att effektivitetsskäl av såväl operativ som mer formell eller administrativ karaktär talar för att tillstånd till avlyssning bör ge de brottsutredande myndigheterna tillgång även till övervakningsuppgifter, dvs. uppgifter om meddelanden och för lokalisering eller identifiering av tekniska hjälpmedel, liksom möjlighet att hindra meddelanden från att nå fram till eller lämna ett visst tekniskt hjälpmedel. Det kan enligt vår mening

starkt ifrågasättas om en ordning som innebär enbart en begränsad möjlighet i nu aktuellt hänseende skulle leda till några större fördelar från effektivitetssynpunkt.

Frågan blir då om en lösning som ger rätt att få ut samtliga typer av övervakningsuppgifter och möjlighet att hindra meddelanden från att nå fram till eller lämna ett tekniskt hjälpmedel framstår som godtagbar från integritetssynpunkt. Det är då att märka att de omständigheter som ger grund för möjlighet till avlyssning i princip också ger möjlighet att använda övervakning. Den ordning som tillämpas redan i dag innebär att tillstånd till hemlig teleavlyssning kombineras med tillstånd till hemlig teleövervakning. De teleövervakningsuppgifter som Buggningsutredningen och regeringen i lagrådsremissen föreslog inte skulle lämnas ut vid hemlig teleavlyssning, framstår principiellt inte som mer integritetskänsliga än de uppgifter förslaget faktiskt omfattade (uppgifter om teleadresser som varit i kontakt med den avlyssnade adressen respektive telemeddelandenas längd i tid). Det står också domstolen fritt att med hänsyn till proportionalitetsprincipen i sitt tillståndsbeslut föreskriva de begränsningar som kan krävas i nu aktuellt avseende. Dessutom åligger det de brottsutredande myndigheterna att vid såväl ansökan om tillstånd till tvångsmedlet som i samband med verkställigheten uppmärksamma den principen. Till det kommer att ett offentligt ombud deltar vid prövning av tillstånd till avlyssning men inte till övervakning (27 kap. 26 § RB).

Vi kan mot den bakgrunden inte se några avgörande skäl mot att föreslå att samtliga övervakningsuppgifter skall kunna lämnas ut vid tillstånd till avlyssning. Exakt vilka övervakningsuppgifter det rör sig om är mot bakgrund av den tekniska utvecklingen inte lämpligt att föreskriva i lagtext. Meddelanden bör även kunna hindras från att nå fram till eller lämna ett visst tekniskt hjälpmedel.

5 Polisens tillgång till uppgifter om abonnemang m.m.

5.1 Sammanfattning av bedömning och förslag

– Rätten enligt lagen om elektronisk kommunikation för de brottsutredande myndigheterna att få del av uppgifter om abonnemang från operatörer skall vara lika generell som den rätt som i dag finns för t.ex. SOS Alarm AB att få sådana uppgifter. Ordningen skall vara densamma för polis- och åklagarmyndighet i situationer utanför en förundersökning.
– Lagen om elektronisk kommunikation skall kompletteras med en bestämmelse som innebär att operatörer skall på begäran lämna ut uppgifter som abonnemang (vilket också följer av det nyss nämnda förslaget), andra uppgifter som angår särskilda elektroniska meddelanden och uppgifter för lokalisering av ett tekniskt hjälpmedel till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa.
– Någon särskild skyldighet för operatörer att registrera uppgifter om abonnemang för kontantkort och uppgifter som visar var och när kontantkortet köptes bör inte införas nu.

5.2 Inledning

Rikspolisstyrelsen har i två skrivelser, till Justitiedepartementet och till oss, tagit upp frågor om polisens tillgång till uppgifter om abonnemang (RÄS-005-4529/04, Ju2004/9044/PO och RÄS 000-5200/04). Frågorna rör dels hur polisen får en effektiv tillgång till uppgifterna, dels polisens behov av abonnemangsuppgifter för kontantkortsabonnemang, dvs. anonyma kontantkort. Rikspolisstyrel-

sen hemställer i skrivelserna att vi utreder frågorna och i förekommande fall föreslår ändringar i lagen om elektronisk kommunikation. Frågorna berör vårt uppdrag i stort och särskilt uppdraget i tilläggsdirektiven angående elektronisk kommunikation (Dir. 2000:90 och 2003:145, se *bilaga 1 och 2*). Justitiedepartementet har överlämnat den aktuella skrivelsen till oss.

Rikspolisstyrelsen har i ytterligare en skrivelse till Justitiedepartementet påtalat behov av en utvidgning av uppgiftsskyldigheten enligt 6 kap. 22 § LEK för operatörerna vid efterforskning av försvunna personer (Ju2003/3153 och RÄS-005-1286/03). Rikspolisstyrelsen menar att det finns ett sådant behov av att få tillgång till uppgifter som angår särskilda elektroniska meddelanden, främst lokaliseringsuppgifter rörande mobiltelefon, att ett tillägg bör göras i lagen om elektronisk kommunikation. Justitiedepartementet har överlämnat även den skrivelsen till oss.

5.3 Nuvarande bestämmelser

Som har framgått tidigare i betänkandet har den operatör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst tystnadsplikt för bl.a. uppgifter om abonnemang och andra uppgifter som angår särskilda elektroniska meddelanden som operatören har fått del av eller tillgång till (6 kap. 20 § LEK).

Med uppgifter om abonnemang avses främst namn, titel, adress och abonnentnummer. Uppgifter som angår särskilda elektroniska meddelanden kan vara uppgift om vilka som har deltagit i utväxlingen av ett elektroniskt meddelande samt när och under hur lång tid utväxlingen ägde rum. Även uppgifter om positionen hos en mobiltelefon hör till den sistnämnda kategorin.

I 6 kap. 22 § första stycket 1, 2, 6 och 7 LEK anges de fall när operatörerna är skyldiga, och därmed behöriga, att trots sin tystnadsplikt lämna *uppgifter om abonnemang* (”kataloguppgifter”) till polisen eller annan brottsutredande myndighet. Det rör situationer

- ✓ när delgivning enligt delgivningslagen (1970:428) är aktuell och myndigheten behöver uppgiften samt det kan antas att den som söks för delgivning håller sig undan eller det annars finns synnerliga skäl (punkten 1),

- ✓ när det gäller misstanke om brott för vilket fängelse är föreskrivet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter (punkten 2),
- ✓ när 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, dvs. överlämnande till föräldrar eller annan vårdnadshavare av en ung person som har omhändertagits (punkten 6), och
- ✓ när myndigheten finner att uppgiften behövs för att kunna fullgöra underrättelseskyldighet till vårdnadshavare enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare (punkten 7).

Operatörerna har dessutom en skyldighet enligt 6 kap. 22 § första stycket 8 att lämna bl.a. abonnemangsuppgifter till regional alarmeringscentral. Ett utlämnande från operatörerna av alla tillgängliga abonnemangsuppgifter till SOS Alarm AB (SOSAB) är således alltid tillåtet. Något ändamål för utlämnandet finns inte föreskrivet.

Abonnemangsuppgifterna enligt punkterna 6 och 7 ovan rör främst polisens s.k. hjälpande verksamheten (2 § 4 polislagen), alltså verksamhet eller åtgärder som i detta fall inte rör misstankar om brott utan som istället avser att ge allmänheten skydd, upplysningar och annan hjälp. I samband med att regler infördes i telelagen om operatörernas skyldighet att lämna ut abonnemangsuppgifter till polisen i samband med olyckor och dödsfall m.m. uttalade regeringen följande (prop. 1996/97:61 s. 81 f.).

> Den i Rikspolisstyrelsens framställning begärda utvidgningen av möjligheterna att ta del av hemliga teleabonnemang enligt 27 § telelagen */6 kap. 22 § LEK/* till att också omfatta uppgifter som behövs enligt 31 § tredje stycket lagen med särskilda bestämmelser om unga lagöverträdare och 12 § polislagen anser regeringen vara väsentlig för att polisen effektivt skall kunna utföra de uppgifter dessa lagrum kräver. Detsamma gäller vid underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall. – Regeringen föreslår att en bestämmelse med den innebörden införs i 27 § telelagen. Däremot framstår en utvidgning som omfattar polisens generella serviceskyldighet enligt 2 § 4 polislagen som alltför omfattande som grund för att bryta tystnadsplikten.

Operatören har också enligt nuvarande ordning en skyldighet att lämna ut *annan uppgift som angår ett särskilt elektroniskt meddelande* till bl.a. polisen. Det gäller i en förundersökning där misstanken rör brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år (6 kap. 22 § första stycket 3 LEK). Det saknas dock skyldighet för operatören att lämna ut sådana uppgifter till polisen utanför en förundersökningssituation. I avsnitt 4.2.5 föreslår vi att 6 kap. 22 § första stycket 3 LEK skall upphävas. De brottsutredande myndigheternas tillgång till uppgifterna skall uteslutande regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning.

5.4 En effektiv tillgång till uppgifter om abonnemang

5.4.1 Bakgrund

Som har framgått i avsnitt 2.1 är det Säkerhetspolisen som inom polisen har huvudansvaret för tekniska och administrativa frågor som rör hemlig teleavlyssning och hemlig teleövervakning. Det gäller t.ex. utveckling av teknik samt inköp, installation och teknisk drift av utrustning liksom slutande av avtal rörande verkställighet och kontakterna i övrigt med operatörerna (RPSFS 1999:9, FAP 171-1).

Genom Säkerhetspolisen driver Rikspolisstyrelsen ett projekt för att möjliggöra en effektiv tillgång för polisen till uppgifter om abonnemang genom ett samlat register över alla abonnenter. För Rikspolisstyrelsens del sker det främst i syfte att effektivisera verksamheten med hemlig teleavlyssning och hemlig teleövervakning och för att polismyndigheterna dygnet runt skall ha tillgång till abonnemangsuppgifter för att t.ex. snabbt kunna lokalisera larm. Målet med projektet är att på ett snabbare och mer lättillgängligt och från säkerhetssynpunkt bättre sätt kunna få information om vem som har ett visst telefonnummer och vilket telefonnummer en viss person har.

Rikspolisstyrelsen genomför just nu en upphandling av abonnemangsuppgifter från de aktörer som finns på marknaden. Tanken är att alla uppgifter skall överföras till Rikspolisstyrelsen genom ett s.k. bulkgränssnitt, dvs. all relevant data överförs samlat till en lokal databas belägen hos användaren. Den initiala överföringen skall sedan regelbundet kompletteras med uppdaterad information. Det

kan samtidigt nämnas att till skillnad från ett bulkgränssnitt är ett s.k. realtidsgränssnitt där applikationer hos användaren hämtar den specifika information som behövs i det enskilda fallet utan att komplett abonnentinformation finns lagrad hos användaren.

För öppna telefonnummer, där abonnenten har samtyckt till att operatören lämnar ut abonnemangsuppgifter, finns inget legalt hinder mot den tänkta ordningen.

Bestämmelserna om tystnadsplikt i lagen om elektronisk kommunikation får särskild betydelse vid hemliga uppgifter. Som har framgått tidigare innebär 6 kap. 20 § LEK att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till bl.a. uppgift om abonnemang, inte obehörigen får föra det vidare eller utnyttja det han har fått del av eller tillgång till. När det gäller hemliga uppgifter om abonnemang, där abonnenten inte har gett sitt samtycke till att uppgifterna lämnas ut, finns alltså inte något lagstöd för operatörerna att på det föreslagna sättet lämna informationen till polisen. Förutom vid hemlig teleavlyssning och hemlig teleövervakning får operatörerna, som framgått, enbart i vissa särskilda fall lämna uppgifter om hemliga abonnemangsuppgifter till polisen. SOSAB har däremot rätt att utan undantag få del av samtliga hemliga uppgifter.

För att personuppgifter om en abonnent som är fysisk person skall få behandlas i en allmänt tillgänglig abonnentförteckning fordras samtycke från denne (6 kap. 16 § LEK). Abonnentupplysning kan lämnas på flera olika sätt. Uppgifterna kan exempelvis ges ut i tryckt katalog eller på en CD-romskiva, en databas med abonnemangsuppgifter kan läggas ut på Internet eller så kan upplysning lämnas via t.ex. telefon efter enstaka förfrågningar (prop. 2001/02:98 s. 12).

Det är alltså ett behörigt utlämnande från operatören när abonnenten har samtyckt till utlämnande av abonnemangsuppgifterna. Operatörernas avtal med abonnenterna i detta avseende ser olika ut. I vissa fall följer av villkoren att uppgifterna får lämnas ut om kunden inte har begärt att uppgifterna skall hållas hemliga.

5.4.2 Marknaden för abonnemangsuppgifter

Av Rikspolisstyrelsens skrivelse framgår att marknaden för abonnemangsuppgifter är komplex med bl.a. fyra typer av aktörer, nämligen

1. rådataleverantör (operatör som levererar icke kvalitetssäkrade abonnemangsuppgifter),
2. aggregatör (aktör som sammanställer och kvalitetssäkrar abonnemangsuppgifter från rådataleverantörer),
3. detaljist (aktör som tillhandahåller abonnemangsuppgifter till användare och som ofta men inte alltid även har funktionen som aggregatör), och
4. användare (slutmottagare av abonnemangsuppgifter).

Rikspolisstyrelsen anger följande rörande marknaden för abonnemangsuppgifter.

> Marknaden för abonnentdata har också påverkats av att nya tekniker tillkommit, och denna utveckling fortsätter. Den största förändringen hittills har varit införandet av mobiltelefoni. Inom några år kommer därtill IP-telefoni att stå för en betydande del av all telefoni vilket kommer att innebära nya förändringar för framförallt abonnentupplysningsföretagen. Till detta kommer en kontinuerlig avregleringsprocess. Televerkets/Telias monopol på telefoni är sedan länge avskaffat. Nummerportabiliteten möjliggör för abonnenter att behålla sitt gamla telefonnummer även om de byter operatör. I maj 2004 hade enligt SNPAC totalt 603 289 mobilnummer flyttats vid byte av bolag. SNPAC (Swedish Number Portability Administrative Centre) är den organisation som tillhandahåller referensdata avseende portering av telefonnummer ingående i den svenska nummerplanen. Komplexiteten påverkas också av att nya operatörer tillkommer kontinuerligt. Enligt uppgift från Post- och telestyrelsen (PTS) finns fler än 340 operatörer anmälda. Samtidigt pågår en turbulent omdaning i den ovan beskriva aktörskedjan. Vissa aktörer som tidigare haft renodlade roller som aggregatörer rör sig i kedjan och har börjat konkurrera med detaljisterna. Företag som tidigare var samarbetspartners omvandlas genom denna process till konkurrenter och det gör att dataflödena förändras. Detta har medfört att vissa detaljister som inte vill vara beroende av tidigare samarbetspartner i högre grad upphandlar data direkt från rådataleverantörer, vilket gör att tidigare renodlade detaljister även blir aggregatörer.

5.4.3 Polisens inhämtning av abonnemangsuppgifter

Polisen saknar i dag generella tekniska system för inhämtning av abonnemangsuppgifter. Öppen information inhämtas normalt via t.ex. kataloger eller Internet och hemliga uppgifter via telefon eller fax från operatörerna. Dagens manuella system för identifiering av och kontakt med operatörer är enligt uppgift långsamt och arbetskrävande både för polisen och för operatörerna. Det är dessutom kostsamt och risken för fel och misstag vid hanteringen bedöms som stor.

Hanteringen vid inhämtning av uppgifter sker i dagsläget i flera steg. Eftersom förfarandet är olika beroende på vilken operatör abonnenten använder sig av, måste först den aktuella operatören identifieras. Först jämförs telefonnumret med de tilldelningar som framgår av den svenska nummerplanen. Därefter kontaktas den operatör abonnenten tillhör enligt planen. Om en abonnent har valt att portera sitt nummer till en ny operatör och den ursprungliga operatören 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. Det finns också möjlighet för handläggaren att kontakta SNPAC för att spåra den nuvarande operatören. Rutinerna vid utlämning av uppgifter varierar. Ofta lämnas uppgifterna ut mot ett diarienummer för den aktuella förundersökningen och/eller efter motringning. Rutinerna hos de mindre operatörerna är dock enligt uppgift ibland bristfälliga.

Rikspolisstyrelsen har angett att det med nuvarande hantering i vissa fall är svårt att få fram upplysningar om aktuella nummer, både hemliga och öppna, särskilt från mindre operatörer, 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 skall lokaliseras. Vad gäller hemlig teleavlyssning behöver t.ex. uppringda och uppringande telefonnummer kunna identifieras i realtid. Om detta inte är möjligt har Rikspolisstyrelsen bedömt att den brottsutredande verksamheten riskerar att missa möjliga tillfällen till ingripanden. Rikspolisstyrelsen har också angett att personer som är involverade i brottslig verksamhet tenderar att använda sig av hemliga nummer och anonyma kontantkort och fortsätter i skrivelsen med att ange följande.

> Förutom den otymplighet som det manuella systemet innebär finns också risker från säkerhetssynpunkt. För det fall att Polisen behöver uppgift om vilket nummer en viss person

har, t.ex. inför ett ärende om hemlig teleavlyssning, är det olämpligt att fler operatörer än den aktuella får kännedom om ärendet. Ju fler operatörer som behöver kontaktas för att få reda på uppgifter om t.ex. ett porterat abonnemang, desto större är risken att informationen om att Polisen är intresserad av just den eftersökta abonnenten läcker ut eller vidareförmedlas på ett icke önskvärt sätt. Informationen kan exempelvis nå personer som är under utredning, vilket kan vara förödande för Polisens utredningsverksamhet. Genom det ökande antalet operatörer kan det också vara svårt att upptäcka om en operatör har andra intressen än rent affärsmässiga.

Till detta kommer att risken för fel och misstag vid dagens hantering inte är försumbar. I alla de fall som rör brottsbekämpning är det av största vikt att risken elimineras för att fel person kopplas till ett specifikt nummer. Inte minst när det gäller hemlig teleavlyssning och hemlig teleövervakning är detta av grundläggande betydelse.

Vad gäller hemliga nummer är vedertaget bruk i t.ex. ärenden om hemlig teleavlyssning att operatörerna lämnar ut uppgifterna mot att de ges ett diarienummer för den aktuella förundersökningen. De större operatörerna har rutiner för att motringa om den som ringer inte är känd. Hos de mindre operatörerna varierar rutinerna och kan i vissa fall vara bristfälliga.

Sekretessaspekten kan ha betydelse även för den enskilde individ vars abonnentuppgifter Polisen efterfrågar eller kontrollerar. Om Polisen är tvungen att ringa runt till ett flertal operatörer, kan det vid bristfälliga sekretess- och säkerhetsrutiner hos dessa uppstå olägenhet för den enskilde.

Från säkerhets- och sekretessynpunkt är det således bättre att Polisen får tillgång till komplett abonnentinformation från en databas och att informationen blivit överförd till databasen med hjälp av aggregatörer som kvalitetssäkrat informationen. Om abonnentdatabasen finns tillgänglig lokalt hos Polisen, kan det inte heller via loggar hos operatörerna upptäckas vilka abonnenter som är utsatta för hemlig teleavlyssning eller teleövervakning.

Dagens manuella system för identifiering av och kontakt med operatörer är kostsamt genom att varje samtal till operatörerna betalas enligt taxa. Polisens kostnader för upplysningar om abonnemang kommer sannolikt att kunna minskas

> med ett antal miljoner kronor per år genom en lokal databas hos Polisen. Enligt beräkningar från det konsultföretag (NetLight Consulting AB) som RPS anlitat för detta projekt kan det röra sig om mellan fyra och fem miljoner kronor per år i reella besparingar. Dessutom skulle effektiviseringen innebära stora tidsbesparingar för Polisen, vilket i längden även ger kostnadsbesparingar.
>
> Sammanfattningsvis kan sägas att en fortsatt hantering med samma rutiner som nu inom ett par år kan väntas bli ohanterlig. Som nämnts ovan beror detta på det växande antalet operatörer parallellt med porteringen av telefonnummer, vilka omständigheter gör att Polisens kontroll av ett hemligt nummer kan kräva kontakt med ett flertal operatörer av vilka vissa endast är tillgängliga under vardagar på kontorstid. Till detta kommer de ovan nämnda riskerna för informationsläckor samt risker för fel och misstag i hanteringen och slutligen att systemet är kostnadskrävande.

Det skall i detta sammanhang nämnas att regeringen nyligen i en lagrådsremiss den 3 mars 2005 Kostnadsansvar för hemlig teleavlyssning m.m. har föreslagit att den som lämnar ut uppgifter enligt bl.a. 6 kap. 22 § första stycket 2 inte skall ha rätt till ersättning för det (jfr vårt förslag i SOU 2003:74).

I Rikspolisstyrelsens skrivelse skissas även på tänkbara lösningar på de angivna problemen på följande sätt.

> För att undvika en ohanterlig situation inom de närmsta åren krävs således en lagändring innebärande att Polisen får samma generella rätt att få del av telefonnummer som regionala alarmeringscentraler, t.ex. SOSAB. Vidare krävs en ändring som ger en aggregatör rätt att för Polisens räkning ta del av samtliga hemliga nummer. Även om vissa operatörer redan har lämnat ut uppgifter om hemliga abonnemang till aggregatörer, finns enligt styrelsens tolkning för närvarande inte något lagstöd för detta.
>
> När ett sådant stöd finns får avgöras hur den tekniska lösningen för överföring mellan den utvalda aggregatören och Polisen skall se ut. Redan nu kan sägas att den mest effektiva metoden, och även det bästa förfaringssättet från säkerhetssynpunkt, är att Polisen kan få en överföring från aggregatören av ett komplett sammanställt register över abonnenter

genom ett bulkgränssnitt med efterföljande kontinuerliga uppdateringar av registret.

En alternativ teknisk lösning är att öppna nummer överförs till Polisen via ett bulkgränssnitt och att hemliga telefonnummer överförs via ett realtidsgränssnitt från aggregatören vid varje förfrågan. Rikspolisstyrelsen anser emellertid att denna lösning inte är acceptabel från sekretess- och säkerhetssynpunkt eftersom en aggregatör vid detta förfaringssätt hela tiden kan se exakt vilka abonnemang som kontrolleras av Polisen.

En jämförelse kan göras med reglerna om lokaliseringsuppgifter, dvs. uppgifter som visar den geografiska positionen för terminalutrustningen för en användare. Enligt huvudregeln får lokaliseringsuppgifter, som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter, behandlas endast sedan de har avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen. Behandlingen får ske endast i den utsträckning och under den tid som krävs för tillhandahållandet av en tjänst där uppgifterna behövs (6 kap. 9 § LEK). Från huvudregeln får undantag göras för Polisen eller en regional alarmeringscentral genom att lokaliseringsuppgifter får tillhandahållas vid nödsamtal, oavsett samtycke eller t.o.m. trots vägran från abonnenten eller användaren (6 kap. 13 § LEK).

En förutsättning för att Polisen skall kunna ges tillgång till komplett abonnentinformation via bulkgränssnitt är att integritetshänsyn kan tillgodoses på ett betryggande sätt. Utgångspunkten är att hemliga abonnentuppgifter även fortsättningsvis skall få användas endast för de ändamål som i dag anges i 6 kap. 22 § punkterna 1, 2, 6 och 7 LEK. Dessa ändamål bör regleras i författning i samband med ändringen i LEK. Att reglerna efterföljs bör sedan säkerställas genom loggning och andra kontroller. Tänkbara interna kontrollsystem skulle kunna konstrueras så att varje person inom Polisen som behöver tillgång till ett hemligt nummer t.ex. måste ange ändamålet med förfrågan. Registernämnden skulle kunna ges ett särskilt ansvar att kontrollera att sökningar på hemliga nummer sker endast i de fall det finns stöd för att ta del av uppgiften. En sådan ordning skulle innebära ett bättre integritetsskydd än nuvarande system.

För abonnentregistret måste generella regler om sekretess, register och behandling av personuppgifter enligt sekre-

tesslagen (1980:100), polisdatalagen (1998:622) och personuppgiftslagen (1998:204, PUL) beaktas på samma sätt som för Polisens övriga register. Uppgifter om telefonabonnemang är sådana personuppgifter som omfattas av PUL. Det är av vikt att registret och åtkomsten till detta utformas så att inte otillbörligt intrång i den registrerades personliga integritet uppkommer.

5.4.4 Våra överväganden

Förslag: Rätten enligt lagen om elektronisk kommunikation för de brottsutredande myndigheterna att få del av uppgifter om abonnemang från operatörer skall vara lika generell som den rätt som i dag finns för t.ex. SOS Alarm AB att få sådana uppgifter. Ordningen skall vara densamma för polis- och åklagarmyndighet i situationer utanför en förundersökning.

Skyldigheten för operatörerna att lämna uppgifter till bl.a. polismyndighet i dess serviceverksamhet eller hjälpande verksamhet utvidgades genom en ändring i telelagen som trädde i kraft den 1 juli 1997. Då infördes det som i dag motsvarar 6 kap. 22 § första stycket 6 och 7 LEK, dvs. rätten att få ut abonnemangsuppgifter från operatörerna om detta behövs i samband med exempelvis underrättelse vid olyckor och dödsfall och underrättelse till vårdnadshavare i vissa fall.

I det lagstiftningsärendet hade Rikspolisstyrelsen i en skrivelse påtalat ett behov av att kunna få ut sådana uppgifter även i andra situationer där polisen enligt 2 § 4 polislagen fullgör sina skyldigheter att ge service till eller hjälpa allmänheten. Regeringen menade dock, utan att utveckla det närmare, att en utvidgning som motsvarar polisens generella serviceskyldighet var allt för omfattande som grund för att bryta operatörernas tystnadsplikt.

Rikspolisstyrelsen har återigen påtalat behovet av en utvidgning av regleringen i lagen om elektronisk kommunikation och förordar en ordning som motsvarar den som gäller för SOSAB:s del vad gäller abonnemangsuppgifterna. Enligt Rikspolisstyrelsen bör det alltså finnas en generell rätt för polisen att få del av sådana uppgifter.

Rikspolisstyrelsen vill med andra ord att polisen på ett enklare sätt skall få del av uppgifter som man i mycket stor utsträckning har rätt att få tillgång till redan i dag. Den formella skillnaden enligt

lagen om elektronisk kommunikation skulle bli dels att i förundersökningar skulle möjligheten att få abonnemangsuppgifter finnas även i bötesfall, dels att uppgifterna skulle bli generellt tillgängliga i den hjälpande verksamheten, vilket ofta avser åtgärder som vidtas i den enskildes eget intresse. Ett exempel på det sistnämnda utgör möjligheten att omedelbart kunna lokalisera larm. Här kan också paralleller dras med den ordning som redan gäller för SOSAB:s del.

Det har framkommit flera nackdelar för såväl polisen som operatörerna med den ordning som gäller i dag. Den är långsam, arbetskrävande, kostsam och leder ibland till att uppgifterna över huvud taget inte erhålls, i vart fall inte under den tid som är nödvändig för ett effektivt polisarbete. Dessutom finns säkerhetsrisker, sekretessbrister och stora risker för fel och misstag i hanteringen. Rikspolisstyrelsen har bedömt att den nuvarande ordningen kommer att bli ohanterlig inom ett par år.

Det står klart att det nuvarande systemet behöver förändras och att det finns stora fördelar med den ordning som Rikspolisstyrelsen förespråkar, dvs. att lagstiftningen ändras så att polisen får samma generella rätt som t.ex. SOSAB att ta del av abonnemangsuppgifter. Genom de datatekniska lösningar som då kan användas uppkommer klara effektivitetsvinster och därigenom minskade kostnader genom en ökad snabbhet, minskade arbetsinsatser och ett minskat bortfall av uppgifter. Dessutom ökar skyddet för sekretessbelagda uppgifter när sådana inte längre behöver delges operatörerna. Även säkerhetsriskerna minskar bl.a. genom en minskad risk för att polisen undanhålls uppgifter och för att operatören eller personal hos operatören påverkas av kriminella personer att genomföra åtgärder som försvårar polisens arbete.

Flera av de fördelar som nyss nämndes uppkommer även för operatörerna, främst genom en mer effektiv och billig ordning och genom att personalen riskerar att i mindre grad utsättas för påtryckningar från kriminella personer.

De fördelar som uppkommer för myndigheterna och operatörerna måste givetvis vägas mot intresset hos enskilda att uppgifter om hemliga abonnemang inte sprids i onödan. Det är viktigt att hålla i minnet att det här enbart rör sig om ”kataloguppgifter”, alltså uppgifter som namn, titel, adress och abonnentnummer, och inte om de mer integritetskänsliga uppgifterna om särskilda elektroniska meddelanden (motsvarande teleövervakningsuppgifter). Det är också viktigt att nämna att polisen många gånger har behov av uppgifterna vid ageranden som sker i den persons intresse som de hemliga uppgifterna avser. Den utvidgning som Rikspolisstyrelsen har

föreslagit i lagstiftningen är dessutom relativt begränsad och borde om den genomfördes kunna bli föremål för någon form av reglering och kontroll inom myndigheterna för att t.ex. begränsa den krets av personer som har tillgång till uppgifterna och undvika eventuella misstankar om otillbörlig användning.

Efter en avvägning mellan å ena sidan de många fördelar som finns att hämta av en utvidgad möjlighet för polisen att ta del av abonnemangsuppgifter och å andra sidan den i praktiken relativt begränsade risken för ökade intrång i enskildas integritet som skulle följa, finns det enligt vår mening inte något hinder mot att lagen om elektronisk kommunikation ändras på det sätt som Rikspolisstyrelsen har föreslagit. Ändringen kommer därmed att innebära att även andra myndigheter som utreder brott, dvs. åklagare, Tullverket, Kustbevakningen och Skatteverket, omfattas av regleringen när det finns misstankar om brott. För situationer som faller utanför en förundersökning kommer enbart polis- och åklagarmyndighet att omfattas av bestämmelsen (jfr vad som gäller i dag enligt 6 kap. 22 § första stycket 6 och 7 LEK).

I den aktuella bestämmelsen anges att operatören skall på begäran lämna uppgifterna till exempelvis polismyndighet. Rikspolisstyrelsen har i sin skrivelse dragit slutsatsen att det inte finns något lagstöd för ett utlämnande från operatören till en aggregatör. Rikspolisstyrelsen har därför föreslagit ett tillägg till bestämmelsen innebärande att en aktör som sammanställer och kvalitetssäkrar abonnentdata får rätt att för polisens räkning ta del av samtliga hemliga abonnemangsuppgifter.

Det tillägg som Rikspolisstyrelsen föreslår i 6 kap. 22 § LEK är enligt vår mening inte nödvändigt. Såväl operatören som polisen kan anlita en utomstående, alltså aggregatören, att för deras räkning biträda med tekniken och lämna respektive ta emot uppgifterna utan att det egentligen behöver påverka lagtextens utformning. Sekretessmässigt är det enklast att se det som att aggregatören handlar på operatörens uppdrag. För den motsatta ordningen, alltså att aggregatören anses ta emot uppgifterna för polisens räkning, är rättsläget vad gäller sekretessgränsen något oklar.

5.5 Utlämnande av vissa uppgifter från operatörer när personer har försvunnit

5.5.1 Bakgrund

Som framgick tidigare menar Rikspolisstyrelsen att det finns ett stort behov av att få tillgång till uppgifter som angår särskilda elektroniska meddelanden, främst lokaliseringsuppgifter rörande mobiltelefon, vid efterforskning av försvunna personer och att ett tillägg bör göras rörande detta i lagen om elektronisk kommunikation.

Den 1 januari 2004 trädde lagen (2003:778) om skydd mot olyckor i kraft och ersatte då räddningstjänstlagen (1986:1102). Lagen innehåller bestämmelser bl.a. om de åtgärder som stat och kommun skall vidta till skydd mot olyckor, om tjänsteplikt och om ingrepp i annans rätt. Det sistnämnda gäller t.ex. räddningstjänstpersonalens tillträde till fastighet, avspärrning eller utrymning av områden och användning av annans egendom. I 1 kap. 2 § lagen om skydd mot olyckor anges att med räddningstjänst avses de räddningsinsatser som staten eller kommunerna skall ansvara för vid olyckor och överhängande fara för olyckor för att förhindra och begränsa skador på människor, egendom eller miljön. Till räddningstjänst enligt lagen hör även vissa andra insatser som genomförs utan att det har inträffat någon olycka eller att det föreligger överhängande fara för sådan. Det gäller enligt 4 kap. 1-4 §§ lagen om skydd mot olyckor bl.a. efterforskning av försvunna personer. Även i sådana fall kan därmed bl.a. vissa av myndigheternas befogenheter vid räddningstjänst tillämpas. I 4 kap. 4 § lagen om skydd mot olyckor anges att, vid sidan om fjällräddnings-, flygräddnings- och sjöräddningstjänst, skall den eller de myndigheter som regeringen bestämmer efterforska personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa. I 4 kap. 11 § förordningen (2003:789) om skydd mot olyckor har regeringen bestämt att det är polismyndigheterna som ansvarar för efterforskning av försvunna personer i sådana fall.

5.5.2 Våra överväganden

Förslag: Lagen om elektronisk kommunikation skall kompletteras med en bestämmelse som innebär att operatörer skall på begäran lämna ut uppgifter som abonnemang (vilket också följer av förra avsnittet, 5.4.4), andra uppgifter som angår särskilda elektroniska meddelanden och uppgifter för lokalisering av ett tekniskt hjälpmedel till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa.

Det finns naturligtvis många anledningar till att människor kan sägas ”försvinna”. Orsaken är i de flesta fall inte att brott har begåtts och många gånger inte heller olyckor. Efterforskning av försvunna personer förekommer med andra ord i en mängd olika situationer och i många tusen fall årligen. I vissa fall fordras endast någon enkel åtgärd för att situationen skall klaras ut medan det i andra fall kan bli nödvändigt med omfattande ingripanden och insatser från myndigheter och enskilda, där bl.a. avsevärda personella resurser måste sättas in. I många fall, särskilt när barn, åldringar och personer med nedsatt mental förmåga har försvunnit, är det också nödvändigt med stor snabbhet i insatsen för att hindra eller begränsa skador på personerna.

Som har framgått ingår det i polisens uppgifter att efterforska försvunna personer. Stora resurskrävande insatser fordras i ett icke ringa antal fall årligen. I Rikspolisstyrelsens begäran om utvidgning av uppgiftsskyldigheten för operatörer ligger en bedömning av att om polisen får tillgång till särskilt lokaliseringsuppgifter hos mobiltelefoner i samband med efterforskning av försvunna personer skulle många gånger lidande hos den försvunne kunna förkortas genom att personen kan påträffas snabbare. Dessutom skulle stora resurser kunna sparas vid polisarbetet.

Vi har ingen annan uppfattning än den som Rikspolisstyrelsen ger uttryck för och instämmer i att sådana positiva följder helt säkert uppkommer genom en lagändring som ger polisen tillgång till uppgifterna vid försvinnanden. Vi menar alltså att en utvidgning av operatörernas uppgiftsskyldighet till att omfatta abonnemangsuppgifter (se även förra avsnittet, 5.4.4) och andra uppgifter som angår särskilda elektroniska meddelanden är väsentlig för att polisen på ett mer effektivt sätt än i dag skall kunna utföra sina uppgifter vid efterforskning. För tydlighetens skull skall nämnas att oavsett om

förslaget i förra avsnittet genomförs eller inte, bör alltså uppgiftsskyldigheten i detta fall utvidgas till att omfatta abonnemangsuppgifter.

I avsnitt 4.4 behandlade vi frågan om lokalisering av tekniska hjälpmedel och konstaterade då bl.a. att det inte kunde uteslutas att det finns en osäkerhet om uttrycket uppgift om angår ett särskilt elektroniskt meddelande i 6 kap. 20 § första stycket 3 LEK omfattar lokaliseringsuppgifter rörande en mobiltelefon som är påslagen utan att det samtidigt pågår ett samtal. Vi föreslog där att det uttryckligen skulle framgå av bestämmelsen om övervakning i rättegångsbalken att uppgifter får hämtas in för lokalisering av ett tekniskt hjälpmedel.

De situationer som avses i detta avsnitt är när polisen efterforskar personer som har försvunnit under sådana förhållanden att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa. Det är också det uttryck som används i 4 kap. lagen om skydd mot olyckor. Det är självklart att de lokaliseringsuppgifter som kommer att vara till nytta vid efterforskning av försvunna personer främst är sådana som inte har samband med ett samtal. Det bör därför klargöras i lagtexten att även sådana uppgifter omfattas av regleringen.

Det integritetsintrång som kan bli följden av förslaget är enligt vår bedömning mycket begränsat och nödvändigt. Dessutom sker polisens agerande i i stort sett samtliga fall helt i den enskildes intresse. Det är i aktuella fall inte fråga om att utreda misstankar om brott (se 6 kap. 22 § första stycket 2 och 3 LEK).

Det är självfallet så att vissa av de personer som försvinner gör det helt frivilligt. De vill alltså inte bli ”återfunna”, i vart fall inte under en viss period från tidpunkten för försvinnandet. Den bestämmelse vi föreslår är inte avsedd att tillämpas i de fallen, även om bedömningen av om det är fråga om ett sådant fall många gånger kan vara svår att göra. Finns det något som tyder på att försvinnandet är frivilligt bör det leda till bedömningen att det inte kan befaras att det föreligger fara för personens liv eller allvarlig risk för dennes hälsa. Vid exempelvis underårigas försvinnanden eller när personer som kan ha en nedsatt mental förmåga har försvunnit, kan man dock alltid utgå från att sådan fara eller risk föreligger även om försvinnandet kan framstå som ”frivilligt”(jfr 12 § polislagen).

5.6 Skyldighet att registrera abonnemangsuppgifter för kontantkort

5.6.1 Bakgrund

Teknikutvecklingen har medfört att användningsområdet för mobiltelefoner har vidgats från talkommunikation till komplexa tjänster för överföring av data, bilder etc. Vissa tjänster kan exempelvis ge tillgång till såväl e-post och outlook-kalender som ett företags intranät och databas. Tjänsten kan också nås med hjälp av ett datainstickskort i en PC och är ett exempel på att gränsen mellan mobiltelefoni och Internet suddas ut.

Det har under lång tid skett en stadig ökning av antalet mobiltelefonabonnemang i Sverige. Det totala antalet abonnemang per capita uppgick den 31 december 2003 till nära 981 abonnemang per 1000 invånare, vilket är en ökning med drygt nio procent jämfört med motsvarande tidpunkt ett år tidigare (PTS rapport Svensk telemarknad 2003 s. 33 ff.).

Det finns en tydlig tendens bland mobiltelefonkunder att använda kontantkort i stället för att teckna kontraktsabonnemang. Från att i stort sett inte ha förekommit år 1996 uppgick antalet aktiva kontantkort den 31 december 2003 till 5 003 000 stycken, eller närmare 58 procent av samtliga GSM-abonnemang (se den angivna rapporten från PTS).

I dagsläget är det vanligt att mobiltelefoner på olika sätt används vid brottslig verksamhet. Polisens möjligheter att få tillgång till uppgifter om abonnemang kan i sådana fall vara helt avgörande för om utredningen skall bli framgångsrik. Operatörer har ofta behov av att hålla register med uppgifter över sina abonnenter, kanske främst för att kunna sköta sin fakturering. Innehavarna av kontantkort med förutbetalda tjänster förblir dock i regel anonyma för operatören, vilket leder till att de brottsutredande myndigheterna inte har möjlighet att få ut nödvändiga abonnemangsuppgifter.

I Rikspolisstyrelsens skrivelse anges följande rörande registrering av innehav av kontantkort samt uppgifter om när och var kontantkortet köptes.

> Den anonymitet som kontantkort ger är i dag väl känd i kriminella kretsar och korten används i hög grad för att försvåra Polisens arbete. Den närmast explosionsartade ökningen av

mobiltelefonabonnemang och intresset för kontantkort har emellertid medfört att mobiltelefoner med kontantkort-abonnemang i dag är vanliga i alla typer av utredningar.

När det gäller den mer organiserade brottsligheten har utvecklingen gått så långt att det i exempelvis utredningar av narkotikabrott endast i undantagsfall förekommer mobiltelefoner med kontraktsabonnemang. Likaså är det i dag mycket vanligt att mobiltelefoner med kontantkortsabonnemang används i sådan brottslighet som ligger inom Säkerhetspolisens kompetensområde.

Polisens möjligheter att få tillgång till abonnemangsuppgifter är ofta avgörande för om en brottsutredning skall vara framgångsrik. Om exempelvis en person är skäligen misstänkt för ett allvarligt brott, kan brottsutredande myndigheter vilja använda hemlig teleavlyssning och hemlig teleövervakning i det fortsatta utredningsarbetet. En förutsättning för tvångsmedlet är emellertid att det går att identifiera en teleadress, exempelvis telefonnummer, som den misstänkte innehar eller annars kan komma att använda. När det saknas abonnentförteckningar måste polisen emellertid helt förlita sig på andra spaningsmetoder för att fastställa vilket mobiltelefonnummer det är fråga om. Viktig tid går härigenom förlorad. Det finns givetvis också en överhängande risk för att Polisen aldrig kan identifiera den aktuella mobiltelefonen. En annan situation då behovet av abonnemangsuppgifter är uppenbart är då Polisen fått uppgift om att en viss mobiltelefon använts i samband med ett brott, men Polisen ännu inte har någon misstänkt för brottet. Utan ett abonnentregister ger mobiltelefonens nummer föga ledning i polisens arbete. Uppgifter om när och var ett kontantkort köpts kan också vara viktig information i polisens arbete.

Polisens behov av att kunna identifiera kontantkortsabonnenter kan i dag knappast överskattas. Trenden med en ökad användning av kontantkort och teknikutveckling med nya tjänster som i allt högre grad suddar ut gränsen mellan tal- och datakommunikation kommer sannolikt härtill att medföra att behovet blir än mer påtagligt i framtiden.

De problem som kontantkortsabonnemang innebär för brottsutredande myndigheter har uppmärksammats i flera länder. I Norge föreskrivs exempelvis att telefonkatalogen även skall innehålla en översikt över kontantkortskunder (5-4 § Forskrift om elektronisk kommunikasjonsnett og kom-

munikasjonstjenste [ekomforskriften]). Även Schweiz (15 Art 5bis Bundesgesetz betreffend die Uberwachung des Post- und Fernmeldeverkehrs) och Tyskland (111 § Telekommunikationsgesetz vom 22. juni 2004) har en lagstiftning som innebär en skyldighet att registrera abonnenten bakom kontantkort.

Rikspolisstyrelsen är medveten om att frågan om registrering av abonnemangsuppgifter avseende kontantkort är komplex. En registreringsskyldighet medför med nödvändighet ökad administration och kostnader för de som tillhandahåller mobiltelefoni med kontantkortsabonnemang. Härtill kommer att ett system måste skapas för att hålla uppgifterna i registren aktuella. Även detta kommer att innebära kostnader. Det skulle också kunna ifrågasättas om det brottsutredande arbetet blir mer effektivt med en reglering, eftersom det skulle vara möjligt för en förutseende gärningsman att vara anonym genom att exempelvis använda en bulvan vid köpet av kontantkort. Man måste i sammanhanget dock komma ihåg att det stora flertalet innehavare av kontantkortsabonnemang sannolikt har valt detta alternativ främst för att det ger bra kontroll över samtalskostnaderna. Den stora förekomsten av kontantkortsabonnemang har också medfört att det i dag är vanligt att abonnemangen förekommer i utredningar av brottslighet som inte varit planerad.

Som har framgått på flera ställen i betänkandet har operatörerna i dag dels en tystnadsplikt för uppgift om abonnemang, dels en skyldighet att lämna sådana uppgifter till brottsutredande myndigheter om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter i det enskilda fallet (6 kap. 20 § första stycket 1 och 22 § första stycket 2 LEK).

Enligt 5 kap. 1 § första stycket 3 LEK får den som tillhandahåller samhällsomfattande tjänster och bedöms lämplig för det förpliktas att till överkomligt pris i en abonnentförteckning, som skall uppdateras årligen, göra uppgifter om samtliga telefonabonnemang tillgängliga i den utsträckning de inte omfattas av sekretess eller tystnadsplikt enligt lagen om elektronisk kommunikation. I propositionens författningskommentar till den bestämmelsen (prop. 2002/03:110 s. 383, jfr även s. 210 f.) anges att i en sådan abonnentförteckning inbegrips såväl fasta som mobila nummer. Enligt de uppgifter vi har fått har sådan skyldighet aldrig föreskrivits, varken

för fasta eller mobila nummer, eftersom konsumenternas behov har tillgodosetts av marknaden själv. Paragrafen utgår alltså från ett konsumentperspektiv, dvs. det är ur ett sådant perspektiv som skyldigheten får föreskrivas och inte främst av hänsyn till de brottsutredande myndigheternas behov.

5.6.2 Våra överväganden

Bedömning: Någon särskild skyldighet för operatörer att registrera uppgifter om abonnemang för kontantkort och uppgifter som visar var och när kontantkortet köptes bör inte införas nu.

När mobiltelefoner förekommer vid brottslig verksamhet är det i princip uteslutande anonyma kontantkort som utnyttjas för att undgå upptäckt och försvåra det brottsutredande arbetet. Vi har redogjort för problemet med sådana kort i avsnitt 4.5. Självfallet kan även sådana teleadresser omfattas av beslut om hemlig teleavlyssning och hemlig teleövervakning när såväl teleadressen som en skäligen misstänkt person är identifierad. De brottsutredande myndigheterna har dock stora problem såväl med att identifiera själva teleadressen som att knyta ett anonymt kontantkort till en viss person. Det står helt klart att tillgång till exempelvis uppgifter om abonnemang många gånger kan vara avgörande för om brottsutredningar skall bli framgångsrika.

Orsaken till att kontantkortskunder tillåts att vara anonyma för operatörerna är givetvis att operatörerna redan har fått betalt för sina tjänster genom kundernas köp av kontantkorten. Utvecklingen visar att allmänhetens intresse av att inneha kontantkort med förutbetalda tjänster är mycket stort. Som framgår fanns drygt fem miljoner aktiva kontantkort i Sverige i slutet av år 2003.

Vi har mycket stor förståelse för de brottsutredande myndigheternas påtagliga behov av att i olika sammanhang få tillgång till uppgifter om abonnemang rörande kontantkort. Till en viss del är detta möjligt redan i dag, nämligen när kunden frivilligt har valt att lämna sådana uppgifter till operatören. Vissa operatörer behandlar i sådana fall uppgifterna som öppna abonnemangsuppgifter medan andra betraktar uppgifterna som hemliga. Har kunden valt att lämna uppgifterna till operatören har myndigheterna under alla förhållanden rätt att för vissa ändamål få tillgång till uppgifterna enligt lagen om elektronisk kommunikation. Det stora problemet för

myndigheterna är när operatören saknar uppgifter om innehavaren av kontantkortet.

De brottsutredande myndigheternas behov av att få tillgång till uppgifterna måste vägas mot andra intressen. En skyldighet att registrera abonnenten bakom ett visst kontantkort innebär inte enbart ett åliggande för operatörerna, med kostnader som följd, utan även en skyldighet för den stora mängd personer som köper kontantkort att ge upp den anonymitet som hittills har funnits och i stället lämna uppgifter om sig själva till operatörerna för brottsutredande ändamål. Särskilt som det får förutsättas att anonymiteten i sig inte generellt är av avgörande betydelse för konsumenterna vid köp av kontantkort, är det sistnämnda enligt vår mening inte en så stor integritetsfråga att den ensam bör kunna hindra en reglering av det slag som Rikspolisstyrelsen föreslår.

Avgörande för oss är dock den tveksamhet som finns rörande hur effektiv den föreslagna ordningen skulle bli för den brottsutredande verksamheten. För att undvika att registreringen blir ”ett slag i luften” skulle en hel del kontrollmekanismer och annat behövas för att i största möjliga mån undvika t.ex. att köpare av kontantkort uppger felaktiga personuppgifter och att vissa köpare registrerar sig för större mängder kontantkort och sedan tillhandahåller dessa i kriminella kretsar. Mot bakgrund av att regleringen inte heller skulle bli enhetlig i ett större antal länder i vårt närområde, t.ex. EU-länderna, skulle anonyma kontantkort kunna köpas utomlands och utnyttjas i Sverige i brottsliga sammanhang.

Vi har med andra ord kommit fram till att det finns stora effektivitetsproblem med den ordning som Rikspolisstyrelsen har föreslagit om registrering av abonnemangsuppgifter till i dagsläget anonyma kontantkort. Särskilt mot den bakgrunden föreslår vi att någon sådan skyldighet inte skall införas nu. Frågan kommer säkert att få allt större betydelse framöver. Därför är det enligt vår mening till en början lämpligt att frågan drivs i internationella sammanhang eller utifrån de erfarenheter som finns i andra länder av nationell lagstiftning på området.

Vi tar upp problemet med anonyma kontantkort även i avsnitt 4.5, där vi bl.a. föreslår att de brottsutredande myndigheterna inom ramen för övervakning enligt 27 kap. 19 § RB skall få använda en metod för att identifiera de tekniska hjälpmedel som är aktuella vid användning av sådana kort. Vi ser att det finns ett påtagligt behov av den metoden i det brottsutredande arbetet. Metoden framstår dessutom som effektiv när det gäller att möta många av de problem som de anonyma kontantkorten skapar. Inom ramen för tvångs-

medlet övervakning kan metoden dessutom regleras så att den blir godtagbar från integritetssynpunkt.

6 Anpassningsskyldigheten

6.1 Sammanfattning av förslagen

– Anpassningsskyldigheten för operatörer skall finnas även fortsättningsvis och vara föreskriven i lagen om elektronisk kommunikation.
– I lagtexten skall anpassningsskyldigheten, liksom i dag, uttryckas så att den verksamhet som avses skall bedrivas så att beslut om avlyssning och övervakning kan verkställas och så att verkställandet inte röjs samt så att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden görs tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand.
– Anpassningsskyldigheten skall omfatta verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. RB eller tjänster inom ett sådant nät.
– Rikspolisstyrelsen skall i enskilda fall få medge undantag från anpassningsskyldigheten.
– Rikspolisstyrelsens beslut skall få överklagas hos allmän förvaltningsdomstol. Prövningstillstånd skall krävas vid överklagande till kammarrätten.
– Operatörerna skall även fortsättningsvis stå för de kostnader som krävs.
– Rikspolisstyrelsen skall få meddela de förelägganden som behövs för att anpassningsskyldigheten skall efterlevas. Föreläggandena skall kunna överklagas hos allmän förvaltningsdomstol. Prövningstillstånd skall krävas vid överklagande till kammarrätten.
– Rikspolisstyrelsen skall kunna förena föreläggandena med vite. Frågor om utdömande av vite skall prövas av allmän förvaltningsdomstol på ansökan av Rikspolisstyrelsen.

forts.

– Sekretesslagen skall kompletteras med en bestämmelse som anger att sekretess gäller för uppgift som hänför sig till Rikspolisstyrelsens prövning av frågor om undantag och förelägganden, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.
– Sekretess skall gälla i sådana ärenden hos Rikspolisstyrelsen även för uppgifter om den enskildes affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs.
– De operatörer vars verksamhet, till skillnad från i dag, kommer att omfattas av anpassningsskyldigheten skall få en viss tid för att vidta de åtgärder som krävs. Tiden från det att den ändrade lagstiftningen utfärdas till dess att den träder i kraft skall dock inte vara längre än ett år.

6.2 Inledning

En del av vårt uppdrag är enligt direktiven (Dir. 2003:145, se *bilaga 2*) att göra en översyn av vilka verksamheter som bör omfattas av anpassningsskyldighet och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Med anpassningsskyldighet avses att en operatör har skyldighet att bedriva verksamheten så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Dessutom skall innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden göras tillgängliga för de brottsutredande myndigheterna så att informationen enkelt kan tas om hand (6 kap. 19 § LEK).

Bestämmelserna om anpassningsskyldighet är i praktiken ofta en förutsättning för att beslut om tvångsmedlen över huvud taget skall kunna verkställas och att verkställandet kan ske i nära anslutning till domstolens beslut. Den snabba teknikutvecklingen gör att reglerna får än större betydelse, särskilt utifrån det perspektivet att bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken är teknikneutrala. Generellt gäller också att ett mer effektivt utnyttjande redan inom ramarna för de befintliga hemliga tvångsmedlen kan innebära betydande utredningsvinster och resursbesparingar för de brottsutredande myndigheterna.

I våra direktiv anger regeringen något om bakgrunden till det behov av översyn av anpassningsskyldigheten som föreligger. Lagen om elektronisk kommunikation bygger på de förslag som e-komutredningen lämnade i delbetänkandet Lag om elektronisk

kommunikation (SOU 2002:60). När utredningens förslag remitterades angavs det bl.a. följande i remisskrivelsen (dnr N2002/7230/ITFoU).

> De föreslagna bestämmelserna har ett delvis annat innehåll än de bestämmelser som gäller i dag. Vissa av de frågor som utredningen tar upp och vissa av de förslag som läggs fram har betydelse för de brottsbekämpande myndigheternas brottsutredande verksamhet. Det finns också ytterligare frågor av stor betydelse på området som inte behandlas i betänkandet. En viktig fråga ur brottsbekämpningssynpunkt är vilka verksamheter som bör omfattas av anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. En annan fråga är vilka trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndigheterna. Ytterligare en fråga är i vilken utsträckning och under vilka förutsättningar som trafikuppgifter bör bevaras hos operatörerna. Dessa frågor och andra frågor som har ett samband med dessa finns det ett klart behov av att utreda ytterligare. Detta kommer att ske i särskild ordning.

I propositionen till lagen om elektronisk kommunikation (prop. 2002/03:110 s. 269) bekräftade regeringen utredningsbehovet och angav att frågan om anpassningsskyldighetens omfattning i förhållande till det nya regelverket på området för elektronisk kommunikation är komplicerad och kräver en fördjupad analys som inte kunde göras inom ramen för det lagstiftningsärendet. Regeringen förklarade att frågan i stället skulle behandlas i ett annat sammanhang där även närliggande frågor skulle utredas.

Även i propositionen 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering gjorde regeringen bedömningen att vissa frågor kräver ytterligare utredning. I det lagstiftningsärendet föreslog regeringen vissa ändringar avseende bestämmelserna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Regeringen angav att när det bl.a. gällde frågan om att avskaffa möjligheten för brottsutredande myndigheter att inhämta uppgifter om telemeddelande direkt från teleoperatören, så skulle den övervägas ytterligare inom ramen för den kommande översynen av vissa frågor rörande teleoperatörers anpassningsskyldighet m.m. (s. 12).

6.3 Anpassningsskyldigheten enligt telelagen

Anpassningsskyldighet för operatörer infördes i telelagen genom propositionen 1995/96:180 Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning. Regeringen uttalade då bl.a. följande (prop. 1995/96:180 s. 17 ff.).

> Hemlig teleavlyssning och hemlig teleövervakning är betydelsefulla straffprocessuella tvångsmedel bl.a. i kampen mot narkotikan, den organiserade brottsligheten och allvarligare ekonomisk brottslighet samt vid brott mot rikets inre och yttre säkerhet. Tvångsmedlen är i dessa fall oumbärliga verktyg i den brottsutredande verksamheten. Det kan med fog hävdas att avancerade brottslingar som har tillgång till kommunikationsvägar som inte kan avlyssnas eller övervakas har goda möjligheter att bedriva sina kriminella aktiviteter utan att avslöjas. Det är därför enligt regeringens mening ytterst angeläget att möjligheterna till verkställighet av tvångsmedlen på teleområdet upprätthålls.
>
> ---
>
> En allmän förutsättning för att hemlig teleavlyssning och hemlig teleövervakning sålunda skall vara möjlig är att telekommunikationssystemet är anpassat för detta. Anpassningen kan avse såväl hård- som mjukvara. Det går inte att upprätthålla acceptabel kvalitet och effektivitet vid användningen av tvångsmedlen på teleområdet om sådana anpassningar inte har vidtagits i systemen. Bakgrunden till den inom EU antagna resolutionen om tvångsmedlen på teleområdet (9529/95 ENFOPOL 90, se avsnitt 6 och 8) är just risken för att de moderna telekommunikationssystemens utformning kan hindra hemlig teleavlyssning såvida de inte anpassas för det ändamålet.
>
> ---
>
> Förekomsten av enskilda från staten fristående teleoperatörer och den snabba tekniska utvecklingen innebär försämrade möjligheter för polisen att verkställa beslut om hemlig teleavlyssning och hemlig teleövervakning. Man kan inte utan vidare räkna med att alla nya teleoperatörer på marknaden kommer att medverka i den utsträckning som erfordras.
>
> ---
>
> Några remissinstanser har ifrågasatt om hemlig teleavlyssning och hemlig teleövervakning numera är så verkningsfulla

> straffprocessuella tvångsmedel att det finns skäl att, med beaktande bl.a. av de kostnader det medför, genomföra en reform av det slag som föreslås i promemorian. SAF hävdar att det redan av det förhållandet att telefonavlyssning endast förekommer i några hundratal fall per år kan dras slutsatsen att teleavlyssning inte har någon avgörande betydelse för brottsbekämpningen i landet. – Att antalet teleavlyssningar är begränsat kan enligt regeringens mening inte leda till slutsatsen att hemlig teleavlyssning inte är ett verkningsfullt straffprocessuellt tvångsmedel. Detta är i stället en naturlig följd av den restriktiva lagstiftningen på området, som har sin grund i en önskan att värna den enskildes integritet. Den användning av tvångsmedlen på teleområdet som varje år redovisas till riksdagen tyder tvärtom på en ganska hög grad av effektivitet (se regeringens skrivelse 1995/96:9).

Regeringen uttalade också att den faktiska anpassningen av systemen inte kan göras av de brottsutredande myndigheterna och fortsatte enligt följande (prop. 1995/96:180 s. 23).

> Det är knappast möjligt för polisen att på egen hand modifiera ett datorprogram i ett telekommunikationssystem, att tillföra systemet nya datorprogram eller att anpassa hårdvarorna. Förutom att det hos polisen skulle behöva finnas en omfattande teknisk expertis som hela tiden följde utvecklingen på teleteknikens område, skulle det vara nödvändigt för polisen att hålla sig med en stor mängd tekniska hjälpmedel. Härutöver skulle det krävas en rad olika provanläggningar. De tekniska hjälpmedlen skulle hela tiden behöva uppdateras. Vidare skulle polisen behöva se till att det fanns reservsystem för det fall t.ex. en växel slogs ut som en följd av någon polisens åtgärd. Även om polisen hade möjlighet att upphandla alla nödvändiga tekniska hjälpmedel och utbilda erforderlig personal skulle polisen ändå behöva stå i ständig kontakt med operatörerna. Det skulle nämligen vara nödvändigt för polisen att hela tiden få information om samtliga åtgärder som vidtas i telesystemen för att kunna genomföra erforderliga anpassningar. Risken för att polisen skulle kunna skada telekommunikationssystemet är också uppenbar om polisen själv skulle ansvara för anpassningarna av hård- och mjukvarorna.
>
> Det finns också en rad andra tungt vägande skäl mot att polisen svarar för den anpassning som krävs för att det skall

> vara möjligt att utföra hemlig teleavlyssning och hemlig teleövervakning. De åtgärder i maskin- och programvaror som behöver vidtas för att tvångsmedlen skall kunna verkställas bör ske på ett så tidigt stadium som möjligt. Det är alltså mindre lämpligt att anpassningarna görs i ett färdigt telekommunikationssystem. Det mest praktiska och överlägset mest ekonomiska tillvägagångssättet är att möjligheterna till telekontroll beaktas i utvecklings- och uppbyggnadsarbetet av telekommunikationssystemen. Detta innebär att den utrustning för telekommunikation, såväl hård- som mjukvara, som utvecklas och upphandlas av teleoperatörerna redan från början bör vara så konstruerad att den möjliggör hemlig teleavlyssning och hemlig teleövervakning.
>
> Vi vill framhålla att vi är ense med de remissinstanser som kritiserar det synsätt som redovisas i promemorian, nämligen att teleoperatörerna skall bära det huvudsakliga ansvaret för att beslut om hemlig teleavlyssning och hemlig teleövervakning kan genomföras. Vad vi åsyftar är ett faktiskt ansvar för teleoperatörerna när det gäller telesystemens utformning.

Av 7 och 17 §§ telelagen följde att den som hade beviljats tillstånd att inom ett allmänt tillgängligt telenät tillhandahålla telefonitjänst till fast nätanslutningspunkt, mobil teletjänst eller nätkapacitet, skulle bedriva verksamheten på sådant sätt att hemlig teleavlyssning och hemlig teleövervakning kunde verkställas och så att verkställandet inte röjdes. Innehållet i och uppgifter om de avlyssnade eller övervakade telemeddelandena skulle göras tillgängliga så att informationen enkelt kunde tas om hand. Tillstånd erfordrades om verksamheten hade en omfattning som med avseende på utbredningsområde, antalet användare eller annat jämförbart förhållande var betydande.

Det som nu har sagts innebär att skyldigheten enligt 17 § telelagen att anpassa verksamheten enbart gällde i förhållande till vissa teleoperatörer, eftersom bara vissa av teleoperatörerna var skyldiga att ha tillstånd enligt telelagen. När det gäller den avgränsningen uttalade regeringen följande i samband med att anpassningsskyldigheten infördes (prop. 1995/96:180 s. 24 f.).

> Som framhålls i promemorian skulle det naturligtvis vara önskvärt att samtliga teleoperatörer på marknaden anpassade sina system så att hemlig teleavlyssning och hemlig teleövervakning enkelt kunde genomföras i den utsträckning som re-

gleringen i rättegångsbalken medger. En sådan ordning är dock förenad med betydande svårigheter av olika slag och det finns marknadsmässiga aspekter som måste beaktas. Så skulle t.ex. en sådan generell skyldighet kunna drabba de mindre teleoperatörerna särskilt hårt, vilket skulle motverka konkurrensen på telemarknaden och hämma nyetableringar. En sådan utveckling är inte önskvärd. Det skulle vidare, delvis av samma skäl, föra för långt att belasta innehavare av privata nät, t.ex. interna företagsnät, med långtgående skyldigheter att svara för telesystemens uppbyggnad och utformning. – De brottsutredande myndigheternas behov av hemlig teleavlyssning och hemlig teleövervakning fokuserar i första hand på stora fasta telenät och på mobiltelefoni. Detta behov kan för närvarande i allt väsentligt tillgodoses genom att de stora teleoperatörerna förpliktas att anpassa sina system. Härigenom öppnas en möjlighet att verkställa tvångsmedlen även när teletjänsten tillhandahålls av en icke tillståndspliktig teleoperatör som hyr kapacitet i ett telenät av en tillståndspliktig operatör. Internationella erfarenheter visar också att de privata näten ännu inte har orsakat några större problem.

Varje gräns medför att det kan bli någon gråzon där det är osäkert om en viss teleoperatör faller strax innanför eller utanför gränsen. Det är därför angeläget att se till att gränsdragningen blir så förutsebar och klar som möjligt. Enligt regeringens mening bör skyldigheten att anpassa telesystemet anknytas till att en teleoperatör faktiskt beviljas tillstånd enligt 5 § telelagen. Det är alldeles klart vilka som fått tillstånd och det finns enligt telelagen möjlighet för en tveksam operatör att begära förhandsbesked från tillståndsmyndigheten om de är skyldiga att söka tillstånd för sin verksamhet (7 § telelagen). Skyldigheten att anpassa systemen bör omfatta alla tre kategorierna av tillståndshavare; för fasta teleförbindelser, för telefonitjänst och för mobil teletjänst. – Teleoperatörer som i och för sig inte är tillståndspliktiga kommer med denna reglering att bli skyldiga att anpassa telesystemen, om de begär och beviljas tillstånd enligt 5 § telelagen. Lagstiftningen innebär dock inte någon skyldighet för en mindre teleoperatör att söka tillstånd. Det finns för övrigt inte heller något hinder för mindre teleoperatörer att på frivillig väg anpassa sina telesystem. – Genom att man ålägger de teleoperatörer som beviljas tillstånd enligt 5 § telelagen att anpassa sina tele-

> system för hemlig teleavlyssning och hemlig teleövervakning kommer åklagare och polis att få effektiv tillgång till tvångsmedel på teleområdet i den utsträckning som behövs i dag. Skulle en avgränsning i enlighet med det nu sagda i en framtid visa sig vara alltför snäv kan frågan övervägas på nytt. Det finns därför, som Överåklagaren i Stockholm framhållit, skäl att noga följa utvecklingen i detta avseende.

I 15 § andra och tredje styckena telelagen föreskrevs att ett tillstånd enligt 7 § den lagen (tidigare 5 §) skulle förenas med villkor att på visst sätt fullgöra skyldigheten och att regeringen eller tillsynsmyndigheten meddelade närmare föreskrifter om det sätt på vilket tillståndsvillkoren skulle fullgöras.

I samband med att anpassningsskyldigheten infördes uttalade regeringen att skyldigheten inte kan vara begränsad till anpassningar i systemen varje gång ett beslut om tvångsmedel skall verkställas utan att det i stället bör vara fråga om en generell skyldighet som hänför sig till konstanta egenskaper i telesystemet. Regeringen menade att telesystemet vid varje givet tillfälle bör innehålla de egenskaper som behövs för att ett beslut om hemlig teleavlyssning eller hemlig teleövervakning genast skall kunna verkställas. Den närmare innebörden av teleoperatörernas skyldighet blir enligt regeringen i praktiken ett krav på att teleoperatörna skall använda sig av tekniska hjälpmedel som har vissa egenskaper och att operatörerna skall vidta de personella och organisatoriska dispositioner som krävs för att hantera hjälpmedlen (prop. 1995/96:180 s. 25).

Någon tid före det att anpassningsskyldigheten infördes i telelagen antog Ministerrådet i EU en resolution om hemlig teleavlyssning och hemlig teleövervakning (9529/95 ENFOPOL 90). Till resolutionen fogades en bilaga med en uppställning över polisens behov i olika hänseenden i anslutning till användningen av de berörda tvångsmedlen, med syftet att de angivna behoven skulle beaktas i det nationella lagstiftningsarbetet. Specifikationen anger bl.a. vilka uppgifter som polisen behöver få tillgång till när hemlig teleavlyssning och hemlig teleövervakning genomförs. Vidare anges på vilket sätt teleoperatören skall tillhandahålla uppgifterna samt vilka övriga åtaganden som operatören bör uppfylla vid verkställighet av tvångsmedlen. Enligt den angivna propositionen (1995/96:180 s. 14 och 26 f.) kan resolutionen utgöra utgångspunkten för de anpassningskrav som bör ställas på teleoperatörerna. De krav som ställs i resolutionen är enligt vad regeringen uttalade i propositionen mycket långtgående och regeringen gjorde bedöm-

ningen att andra aspekter, som teleoperatörernas möjligheter att med en rimlig arbetsinsats och till en rimlig kostnad uppfylla kraven, inte hade tillmätts samma vikt. Regeringen menade därför att de krav som ställdes i resolutionen inte utan vidare kunde läggas till grund för lagstiftning samtidigt som regeringen pekade på att det stod klart att teleoperatörerna måste uppfylla många av de krav som anges i resolutionen. Regeringen uttalade också följande (prop. 1995/96:180 s. 27 f.).

> Naturligtvis måste polisen kunna få tillgång till innehållet i ett telemeddelande som är föremål för hemlig teleavlyssning. Det är väsentligt att hela meddelandet utan inskränkning blir tillgängligt utan att för den sakens skull innehållet i ett annat telemeddelande tas upp. Den avlyssnade skall givetvis inte kunna upptäcka att han är föremål för ett beslut om hemlig teleavlyssning och inte heller någon annan abonnent skall kunna få kännedom om detta. Det bör särskilt framhållas att andra abonnenter över huvud taget inte skall behöva påverkas av den pågående verkställigheten som också bör ske på ett sådant sätt att förekomsten av hemlig teleavlyssning inte röjs. När en avlyssnad teleadress medflyttas till en annan abonnents telefon skall avlyssningen kunna begränsas till att omfatta endast den medflyttade teleadressen. Vidare är det av avgörande betydelse att telesystemen har kapacitet att genomföra flera avlyssningar samtidigt. Innehållet i telemeddelandet måste göras tillgängligt samtidigt som det förmedlas eller i vart fall i omedelbar anslutning till att det förmedlas. Det är också nödvändigt att polisen kan identifiera telemeddelandet. Likaså finns ett behov av att det avlyssnade telemeddelandet görs tillgängligt för polisen på ett sådant sätt och på en sådan plats att det enkelt kan tas om hand av polisen. Detta innebär att om teleoperatören, av effektivitetsskäl eller andra skäl, kodar eller komprimerar telemeddelandena, dessa måste levereras i klartext. Detsamma gäller för krypterade meddelanden. En förutsättning i det sistnämnda fallet är givetvis att det är teleoperatören som tillhandahåller krypteringssystemet och att teleoperatören har möjlighet att dekryptera meddelandet. Teleoperatörerna bör alltså inte kunna avkrävas telemeddelandena i klartext om abonnenten själv komprimerar eller krypterar sina meddelanden.
>
> ----

> Vad som tidigare sagts om innebörden av teleoperatörernas förpliktelser beträffande hemlig teleavlyssning gör sig i allt väsentligt gällande också för hemlig teleövervakning. Sålunda bör det finnas kapacitet som möjliggör flera övervakningar samtidigt och samtliga de uppgifter som omfattas av hemlig teleövervakning måste kunna hämtas in. Vidare bör övervakningen ske utan intrång för de abonnenter som inte omfattas av beslutet om övervakning och med beaktande av de olika behov av sekretess som ovan redovisats. Även för hemlig teleövervakning gäller att uppgifterna bör hållas tillgängliga inom viss tid, på visst sätt och på viss plats så att de enkelt kan tas om hand.

Som nämndes innehöll 15 § andra stycket telelagen en bestämmelse som innebar att tillståndsmyndigheten (PTS) skulle meddela individuella villkor för hur den berörde teleoperatören skulle uppfylla sin anpassningsskyldighet. När förslaget om anpassningsskyldighet utarbetades hade den synpunkten lämnats från några remissinstanser att det i stället skulle fastställas standardiserade normer för samtliga operatörer som omfattades av kravet på anpassning. Regeringen instämde dock inte i detta utan skrev följande (prop. 1995/96:180 s. 28).

> Detta låter sig emellertid knappast göras i praktiken. Det är självfallet så att en teleoperatör med ett mycket stort antal abonnenter kan behöva tillhandahålla ett system som möjliggör fler inkopplingar samtidigt än en teleoperatör som har ett förhållandevis litet antal abonnenter. De olika tekniska lösningar som används i moderna telesystem kan också föranleda att den avvägning mellan effektivitet och ekonomi som måste göras utfaller olika i de enskilda fallen om varje teleoperatör kan bedömas för sig. En mera fyrkantig reglering kan medföra behov av betydligt större ingrepp i vissa telesystem än andra och sålunda utgöra en tyngre börda för vissa teleoperatörer. Det skulle rent av kunna leda till att ett visst telesystem inte längre gick att använda på marknaden. Man skulle därigenom riskera att allvarligt snedvrida konkurrensen på telemarknaden. Vidare är en inte alltför handfast regel nödvändig om inte snart sagt varje teknisk landvinning på teleområdet skall leda till författningsändringar. Slutligen kan det finnas skäl att göra skillnad på krav som riktas mot en teleoperatör vid införande av ett nytt telesystem och krav på

> anpassningar av redan befintliga telesystem som lagstiftningen inledningsvis ger upphov till. Några mera preciserade anvisningar om vad som bör krävas av varje teleoperatör bör därför enligt regeringens mening inte anges direkt i lag eller annan författning.

Ett tillståndsvillkor kunde enligt regeringen avse exempelvis den kapacitet teleoperatören skulle ha för att kunna verkställa flera beslut samtidigt och på vilket närmare sätt innehållet i eller uppgifterna om det avlyssnade meddelandet skulle göras tillgängliga för polisen. Regeringen uttalade också att flera av de krav som framgår av den nämnda EU-resolutionen bör kunna anges som tillståndsvillkor, att tillståndsmyndigheten vid sin prövning bör beakta nyttan av en viss anpassning mot kostnaden och att särskild hänsyn bör tas till om det rör sig om ändringar i ett befintligt system eller krav som ställs vid byte av ny teknik. Regeringen pekade särskilt på att om det råder enighet mellan de inblandade parterna, alltså de brottsutredande myndigheterna, Rikspolisstyrelsen, Riksåklagaren (numera Åklagarmyndigheten) och teleoperatörerna, bör det normalt inte finnas anledning för PTS att göra någon mer ingående prövning utan myndigheten bör i de fallen kunna utfärda villkor i enlighet med parternas överenskommelse. I annat fall får PTS, enligt regeringen, efter att ha försökt jämka samman parterna, avgöra frågan genom att meddela tillståndsvillkor.

Innan generella föreskrifter skulle utfärdas av PTS fanns det enligt regeringen anledning för myndigheten att först höra parterna och fästa stor vikt vid deras gemensamma uppfattning (prop. 1995/96:180 s. 27 ff. och 37).

Det skall också nämnas att operatörerna samtidigt med anpassningsskyldigheten blev ålagda att svara för de kostnader som hänförde sig till anpassningarna och för drift och underhåll av systemen. I motiven till den ordningen anförde regeringen bl.a. följande (prop. 1995/96:180 s. 30 f.).

> Skyldigheten för teleoperatörerna att upprätthålla de tekniska och administrativa förutsättningarna för hemlig teleavlyssning och hemlig teleövervakning får naturligtvis ekonomiska konsekvenser. De största kostnaderna kommer att uppstå vid de tillfällen som nya tekniska lösningar introduceras i telesystemen. Det är nämligen de erforderliga grundinstallationerna i form av hård- och mjukvaror som är mest kostsamma. I praktiken innebär detta att kostnaderna kom-

mer att uppstå dels under ett initialt skede då berörda operatörer måste anpassa sina befintliga system, dels vid de senare tillfällen då operatörerna byter till ny teknik. Det kan antas att det är förenat med större kostnader att anpassa ett befintligt system än att bygga in vissa avlyssnings- och övervakningsfunktioner i ett helt nytt telesystem.

Hemlig teleavlyssning och hemlig teleövervakning medför även kostnader utöver vad som nu har anförts. Tekniska anpassningar i telesystemen för att kunna verkställa tvångsmedlen innebär att det uppstår drifts- och underhållskostnader, innefattande bl.a. kostnader för den arbetskraft som handhar och finns i beredskap för den praktiska hanteringen av verkställigheten.

Något underlag för en tillförlitlig beräkning av kostnaderna för anpassningar, drift och underhåll av telekommunikationssystemen finns inte och det är tveksamt om det över huvud taget är möjligt att i förväg få fram ett sådant underlag. Det finns heller inga möjligheter att nu förutse vilka ekonomiska konsekvenser som kommer att följa av den tekniska utvecklingen på teleområdet. Det finns emellertid anledning att anta att kostnaderna kommer att uppgå till avsevärda belopp. I promemorian redovisas att enligt företrädare för Telia en anpassning av bolagets samtliga nät sammanlagt kan beräknas uppgå till cirka 34 miljoner kronor. Av denna summa hänför sig 7 miljoner till NMT-nätet, 14 miljoner till GSM-nätet och 13 miljoner till det fasta telenätet. Det är här fråga om kostnader för anpassningar av befintliga redan uppbyggda nät. I remissvaren anger Europolitan att de belopp Telia angett för anpassningen av sitt GSM-nät synes inte vara helt orimliga medan Telia Mobitel bedömer att de angivna kostnaderna är för låga.

Kostnaderna torde variera väsentligt beroende på om det är fråga om en anpassning av ett befintligt telesystem eller om det gäller att försäkra sig om möjligheterna till hemlig teleavlyssning och hemlig teleövervakning vid uppbyggnaden av ett nytt telesystem. Det finns skäl att anta att kostnaden skulle bli väsentligt lägre i det senare fallet och kanske inte ens en gång gå att närmare särskilja från totalkostnaden.

I en skrivelse till regeringen under hösten 2002 om tillgång till telekommunikation för polisens brottsutredande verksamhet anger

Rikspolisstyrelsen bl.a. följande rörande anpassningsskyldigheten (dnr Ju2002/7018/PO och RÄS-002-3668/02).

> Rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning är teknikneutrala och omfattar exempelvis såväl vanlig fast telefoni som mobiltelefoni och telekommunikation via Internet. Dagens regler om anpassningsskyldighet är kopplade till tillståndspliktig verksamhet, vilket avsevärt begränsar reglernas tillämpning. Detta innebär problem för Polisens arbete, särskilt då de som tillhandahåller tjänster på Internet inte omfattas av anpassningsskyldigheten. Om denna inte knyts till tillståndspliktig verksamhet är det svårt att se varför inte skyldigheten skall korrespondera mot rättegångsbalkens teknikneutrala regler. Tvärtom talar de svårigheter som i dag kan uppstå vid verkställighet hos en inte anpassningsskyldig operatör för en sådan förändring. Framtida regler om anpassningsskyldigheten bör i princip omfatta all verksamhet som består av eller möjliggör att telemeddelanden förmedlas till eller ifrån en teleadress. Anpassningsskyldigheten bör i princip vara absolut och endast i undantagssituationer lämna utrymme för avsteg beträffande enskilda anpassningsåtgärder.

6.4 Tidigare handläggning av frågan om tillståndsvillkor

Bestämmelserna i telelagen om anpassningsskyldighet trädde i kraft den 1 juli 1996. Även de tillstånd som redan hade beviljats vid den tiden skulle enligt övergångsbestämmelser till lagändringen förenas med villkor. De teleoperatörerna fick dock en generell övergångstid för anpassningen på ett år från lagens ikraftträdande, alltså till den 1 juli 1997, dock alltid minst sex månaders övergångstid från det att PTS fastställt de närmare villkoren (se övergångsbestämmelserna till ändringen av dåvarande 13 §, sedermera 15 §, telelagen).

I skrivelsen till regeringen under hösten 2002 om tillgång till telekommunikation för polisens brottsutredande verksamhet anger Rikspolisstyrelsen följande rörande PTS tillståndsvillkor (dnr Ju2002/7018/PO och RÄS-002-3668/02).

> Då tillståndsvillkor för första gången skulle utformas påtog sig Telia AB att företräda övriga tillståndshavare i förhand-

lingarna med Polisen. Förhandlingarna var okomplicerade och inom några månader kom parterna fram till tillståndsvillkor grundade på ENFOPOL 90. PTS delade dock inte parternas bedömning och gjorde omfattande förändringar i de föreslagna villkoren. I det följande remissförfarandet var många tillståndshavare kritiska mot villkoren och hänvisade till de kostnader som en anpassning skulle innebära för dem. PTS:s handläggning av ärendet försenades och först i juli 1998 beslutade styrelsen i villkorsfrågan. Styrelsen fann i samtliga fall då någon eller några tillståndshavare haft invändningar, att kostnaderna för en anpassning av verksamheten var så stora i förhållande till den nytta som polisen hade av åtgärden, att tillståndsvillkor inte skulle utfärdas. PTS:s prövning resulterade i att likalydande tillståndsvillkor utfärdades för samtliga teleoperatörer som erhållit ett visst tillstånd. Generella villkor kom därför att fastställas för tillstånd att tillhandahålla telefonitjänst till fast nätanslutningspunkt och för tillstånd att tillhandahålla mobil teletjänst. För tillstånd att tillhandahålla nätkapacitet utfärdades över huvud taget inte några villkor om anpassning.

De tillståndsvillkor som PTS meddelat 1998 löpte ut den 31 december 2000. Polisen bedömde då att teknikutvecklingen medfört ett förändrat kostnadsläge och att det fanns förutsättningar att införa vissa av de tillståndsvillkor som PTS tidigare har vägrat att utfärda. En framställan om förlängning av gällande tillståndsvillkor samt en begäran om ”nya” kompletterande villkor gavs in till PTS under oktober 2000. PTS hann dock inte fatta beslut i frågan innan tillståndsvillkorens giltighet löpte ut, utan tidigare villkor förlängdes under viss tid. Efter ytterligare beslut om förlängning beslutade PTS den 28 mars 2002 om nya villkor för att tillhandahålla telefonitjänst till fast nätanslutningspunkt och mobil teletjänst. Liksom tidigare handlade PTS prövningen som om förutsättningarna att meddela tillståndsvillkor skulle vara desamma hos samtliga teleoperatörer som meddelats ett visst tillstånd. Förutom beträffande en tillståndshavare, som medgett att ett visst tillståndsvillkor utfärdades, fann styrelsen att det inte var möjligt att utfärda tillståndsvillkor för någon av de teleoperatörer som meddelats ett visst tillstånd även om bara några av dessa yttrat sig till PTS och anfört att anpassningskostnaderna var för höga. PTS har den 27 maj 2002 på samma

sätt beslutat om begränsade villkor för tillstånd att tillhandahålla nätkapacitet.

I den nämnda skrivelsen till regeringen angav Rikspolisstyrelsen även följande beträffande tillståndsvillkoren och handläggningen.

> Varje teleoperatörs telesystem innehåller unika tekniska detaljlösningar vilket omöjliggör generella beskrivningar av hur en fullt ut fungerande verkställighet skall genomföras. Sådana generella föreskrifter som PTS hittills meddelat i tillståndsvillkor kan därför aldrig ensamma ligga till grund för ett fungerande system för verkställighet.
>
> En fungerande anpassning kräver istället att Polisen och respektive teleoperatör träffar överenskommelse om de tekniska lösningar som skall användas. En förutsättning för dessa diskussioner har varit att PTS fattar beslut om tillståndsvillkor. PTS långa handläggningstider av villkorsärenden har därför utgjort ett direkt hinder för en snabb anpassning av teleoperatörernas verksamhet. När väl tillståndsvillkor utfärdats är Polisens erfarenhet att tekniken har hunnit förändras i sådan grad att det funnits skäl att till viss del ha nya utgångspunkter för förhandlingarna med teleoperatörerna om den teknik som skall användas inom ramen för tillståndsvillkoren. Polisen har hamnat i en situation med ständigt pågående förhandlingar med operatörerna.
>
> Lagstiftarens utgångspunkt torde ha varit att individuella tillståndsvillkor skall utfärdas (prop. 1995/96:180 s. 28). Eftersom teleoperatörernas system innehåller olika tekniska lösningar är det också givet att en viss anpassningsåtgärd hos en teleoperatör kan vara betydligt mer kostsam än hos en annan. PTS:s tillämpning av telelagen tar dock inte hänsyn till dessa skillnader. Tillståndsvillkor utfärdas inte för någon av de teleoperatörer som erhållit ett visst tillstånd, även om endast någon eller några operatörer anfört att deras anpassningskostnader är för stora, om inte villkoret uttryckligen medgivits. Presumtionen har härigenom närmast blivit att det inte skall ske någon anpassning av teleoperatörernas verksamhet.
>
> Det kan tyckas naturligt att PTS, utifrån dokument ENFOPOL 90 och det förtydligande av detta dokument som för närvarande är under bearbetning, har till uppgift att fastställa den tekniska utformning av gränssnittet vid hemlig te-

leavlyssning och hemlig teleövervakning. Det måste dock vara fråga om individuellt anpassade gränssnitt för varje operatör varför PTS skulle behöva en teknisk kompetens såväl beträffande de enskilda operatörernas nät som beträffande den avlyssningsutrustning som Polisen innehar. Härtill kommer att även Säkerhetspolisen använder avlyssningsutrustningen vilket ställer särskilda krav på säkerhet och sekretess för uppgifter om utrustningen.

Polisens erfarenhet av PTS handläggning av tillståndsärenden leder till slutsatsen att en modell där PTS fastställer den tekniska utformningen av gränssnitten skulle kräva betydande förändringar av PTS handläggningsformer. Det framstår också som om PTS skulle behöva såväl förstärka som utnyttja sin befintliga tekniska kompetens på annat sätt än som görs i dag. En modell där PTS fastställer den tekniska utformningen av gränssnitten framstår därför för närvarande som svår att genomföra.

Erfarenheterna av PTS tillståndsprövning leder till slutsatsen att det ligger närmare till hands att den enskilde teleoperatören och Polisen själva kommer överens om hur anpassningsskyldigheten skall fullgöras. Härigenom skulle en anpassning av den enskilde operatörens verksamhet sannolikt komma till stånd mycket snabbare än enligt det nuvarande systemet och större hänsyn kunna tas till förutsättningarna hos den enskilde teleoperatören. Om inte parterna kan enas om vilka konkreta åtgärder som skall vidtas, bör tillsynsmyndigheten i första hand ha en medlande funktion och, om parterna ändå inte kan träffa en överenskommelse, därefter avgöra frågan. För en sådan lösning talar också de svårigheter som de teleoperatörer som över huvud taget yttrat sig till PTS hittills har haft att närmare precisera hur stora kostnader en anpassning enligt tillståndsvillkoren skulle medföra. Tillsynsmyndigheten skulle sannolikt ha ett mycket bättre underlag för prövningen av en viss anpassningsåtgärd hos en enskild teleoperatör.

Vi har med anledning av Rikspolisstyrelsens skrivelse inhämtat uppgifter från PTS om handläggningen och då fått följande beskrivning.

Den 10 november 1996 bjöd PTS in Riksåklagaren och Rikspolisstyrelsen till samråd angående föreskrifter om tillstånds-

villkor (ärende 96-16693). Den 12 november 1996 lämnade Rikspolisstyrelsen ett förslag till villkor. Förslaget remitterades till operatörerna. Den 10 december 1996 hölls ett sammanträde med myndigheter och operatörer. Då antecknades bl.a. att Rikspolisstyrelsen uttryckte tveksamhet i frågan om olika eller likalydande krav skulle ställas på operatörerna. Efter ytterligare skriftväxling inkom Rikspolisstyrelsen den 25 april 1997 med vad som får antas vara det i styrelsens skrivelse till regeringen omtalade förslaget. Detta överensstämde i allt väsentligt med det omnämnda ENOPOL 90. Av följebrev framgår att förslaget utarbetats av Rikspolisstyrelsen, Riksåklagaren och Telia. Det framgår också att Telia inte företrädde övriga operatörer och inte heller helt delade förslagets mening. Förslaget remitterades av PTS.

Av skriftväxlingen i ärendet framgår att Telia invände den 15 maj 1997 till PTS mot ett av de av Rikspolisstyrelsen föreslagna villkoren såsom synnerligen svårt eller rent av omöjligt att utföra. Telia uppgav då också att det aktuella villkoret borde utformas olika för olika operatörer eftersom dessa hade olika tekniska förutsättningar. Efter ytterligare kommunikation mellan Rikspolisstyrelsen, Telia och PTS, remitterades ett reviderat förslag till Rikspolisstyrelsen och Riksåklagaren den 5 juli samt till operatörerna den 16 juli 1997. Sedan operatörerna inkommit med synpunkter upprättade PTS ett nytt förslag som översändes till Rikspolisstyrelsen den 27 november samma år. Den 10 december 1997 inkom synpunkter från Rikspolisstyrelsen på detta förslag. Den 21 januari 1998 tillskrev PTS operatörerna med begäran om uppgifter på kostnader för genomförande av förslaget. Under tiden fram till den 3 april 1998 inkom sådana uppgifter.

Den 6 juli 1998 meddelade PTS tre beslut. Där anfördes allmänt att vid överenskommelse mellan parterna skulle någon närmare prövning av villkoren inte göras, att anpassningskostnaderna måste stå i rimlig proportion till nyttan med anpassningen, att kraven skulle ställas lägre på operatörernas befintliga nät än på nyetableringar och att operatörerna inte borde åläggas så tunga bördor att en viss tjänst skulle bli olönsam (prop. 1995/96:180 s. 34). I besluten förordnades bl.a. om följande.

För operatörer av fasta telenät: Ett antal villkor meddelades, varom det rådde enighet. Beträffande två av de villkor Rikspolisstyrelsen begärt – möjlighet till parallell avlyssning och

möjlighet att särskilja utgående och ingående trafik – gjordes bedömningen att kostnaderna för att uppfylla villkoren inte uppvägde nyttan därav.

För operatörer av mobila telenät: Ett antal villkor meddelades, varom det rådde enighet. I frågor om nätanslutningspunkter och vilka tekniska gränssnitt som skulle användas föreskrevs att parterna skulle särskilt komma överens om detta. I fråga om NMT-nätet antecknades att näten enligt överenskommelse mellan Rikspolisstyrelsen och Telia endast skulle omfattas av tillståndsvillkoren i de delar som var tillämpliga beträffande befintlig funktionalitet. Beträffande möjlighet till parallell avlyssning gjordes samma bedömning som i fråga om de fasta näten. Vad gäller Mobitex-näten, ERMES- och Minicall-näten, flygtelefonitjänsten och tjänsten Maritim Radio konstaterade PTS att nyttan med att införa anpassningsskyldighet i dessa nät inte stod i rimlig proportion till kostnaderna för detta. Inga villkor om anpassning utfärdades därför för dessa nät.

För operatörer som tillhandahåller nätkapacitet: PTS konstaterade att avlyssning var komplicerad och kostnadskrävande eftersom enskilda meddelanden var svåra att utskilja och att avlyssning kunde ske hos operatörernas kunder, dvs. de operatörer som tillhandahöll kopplade teletjänster. PTS godtog dessa uppgifter från operatörerna. Några villkor utfärdades därför inte för de operatörer som tillhandahöll enbart nätkapacitet.

PTS beslut överklagades inte. Inte heller har något ärende aktualiserats där Rikspolisstyrelsen klagat över efterlevnaden av besluten. PTS har heller inte ex officio tagit upp någon tillsyn i detta hänseende. Därför har heller inte något ärende om föreläggande eller annan åtgärd mot någon operatör varit aktuellt. Tillståndsvillkoren löpte till utgången av år 1999.

Rikspolisstyrelsen och Riksåklagaren uttryckte inför utgången av år 1999 (ärende nr 99-17098) åsikten att gällande villkor borde förlängas till utgången av år 2000. PTS beslöt om detta. Av samma skäl förlängdes villkoren därefter till den 31 mars 2002. Villkoren har senare förlängts till dess lagen om elektronisk kommunikation trädde i kraft den 25 juli 2003. Villkor beslutades också för nya tillhandahållare av nätkapacitet.

PTS har därefter i samråd med Rikspolisstyrelsen, Riksåklagaren och operatörer bedrivit ett arbete med att bedöma

lämpligheten av att ge ut föreskrifter (ärende nr 03-7089). I ärendet har förekommit omfattande diskussioner i materiella och formella frågor. Den 23 februari 2004 meddelades parterna att PTS då inte bedömde behov finnas av föreskrifter på området.

Det har framkommit att bl.a. det förhållandet att beslut kunnat fattas först efter långdragna förhandlingar mellan parterna har bidragit till att göra processen långsam. Faktorer som exempelvis handläggningsformer och bristen på instrument för den prövande myndigheten att pressa upp hastigheten hos parterna, samtidigt som i vart fall operatörerna inte har någon fördel av ett snabbt avgörande, har verkat i samma riktning. Av de handlingar vi har tagit del av framgår t.ex. att enbart en tredjedel av de tillståndspliktiga operatörer som berördes av Rikspolisstyrelsens förslag till tillägg i befintliga tillståndsvillkor svarade på PTS remiss under våren 2001. Frågan om hur anpassningsskyldigheten skall bestämmas måste bli föremål för nya överväganden. Vi återkommer till det i avsnitt 6.6.

6.5 Anpassningsskyldigheten enligt lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation ersatte telelagen från och med den 25 juli 2003. Den ställer upp liknande krav på anpassning som telelagen tidigare gjorde (17 § telelagen). Bestämmelsen finns i 6 kap. 19 § LEK och har följande lydelse.

> En verksamhet skall bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av
>
> 1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller
>
> 2. tjänster inom ett allmänt kommunikationsnät vilka består av
>
> a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med

> en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller
>
> b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.
>
> Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand.
>
> Med telemeddelande avses ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.
>
> Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om frågor som avses i första och andra styckena samt får i enskilda fall medge undantag från kravet i första stycket.

Bestämmelserna om anpassningsskyldighet grundas på det tidigare nämnda auktorisationsdirektivet (se avsnitt 2.6). Av artikel 6.1 i direktivet och del A punkten 11 i bilagan till direktivet framgår att villkor som möjliggör avlyssning för behöriga nationella myndigheter får uppställas för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Sådana villkor skall vara objektivt motiverade med avseende på det nät eller den tjänst som berörs, samt öppet redovisade, icke-diskriminerande och proportionella (prop. 2002/03:110 s. 268, 437 och 442).

Telelagens bestämmelser i nu aktuellt avseende byggde på en *tillståndsplikt*. Lagen om elektronisk kommunikation utgår i stället från en *anmälningsplikt*. För att, som det anges i den citerade bestämmelsen, tillhandahålla ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst fordras i allmänhet endast en anmälan (2 kap. 1 § LEK). När det gäller anpassningsskyldigheten hänvisade regeringen i prop. 2002/03:110 till bl.a. det betänkande som låg till grund för förslaget (SOU 2002:60) och angav följande (s. 269).

> I betänkandet uttalas att reglerna i telelagen angående hemlig teleavlyssning och hemlig teleövervakning föreslås överförda till den nya lagen. Någon saklig ändring i förhållande till vad som gäller enligt nuvarande bestämmelser synes således inte vara avsedd. Enligt regeringens bedömning innebär emellertid utredningens förslag att tillhandahållande av vissa nät och tjänster som i dag omfattas av anpassningsskyldigheten skul-

le komma att falla utanför denna. Det gäller dels tillhandahållande av sådan nätkapacitet som inte avser ett allmänt telefonnät men väl ett allmänt kommunikationsnät som inte enbart är avsett för utsändningar till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen (YGL), dels vissa elektroniska kommunikationstjänster till mobil nätanslutningspunkt. Exempelvis skulle den anpassningsskyldighet som enligt telelagen gäller för tillståndet att bedriva tredje generationens mobiltelefoni (UMTS) komma att avsevärt begränsas. Vidare bör det med hänsyn till den något ändrade terminologin i den nya lagen klargöras att beträffande telefonitjänst till fast nätanslutningspunkt innefattar detta förutom överföring av lokala, nationella och internationella samtal även telefax samt datakommunikation med viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet. Sådan datakommunikation benämns enligt telelagen datakommunikation via låghastighetsmodem. Utredningens förslag innebär dock samtidigt en utvidgning av tillämpningsområdet genom att verksamheten inte behöver ha viss omfattning för att omfattas.

Frågan om anpassningsskyldighetens omfattning i förhållande till det nya regelverket på området för elektronisk kommunikation är komplicerad och kräver en fördjupad analys som inte kan göras inom ramen för detta lagstiftningsärende. Frågan kommer i stället att behandlas i ett annat sammanhang där även andra närliggande frågor kommer att utredas. I avvaktan på sådan ytterligare utredning av anpassningsskyldigheten bör skyldighetens omfattning enligt den nya lagen ansluta så nära som möjligt till den omfattning som gäller enligt nu gällande regler i telelagen. Avsikten är alltså inte att låta skyldigheten omfatta fler och ej heller färre verksamheter än vad som omfattas enligt nuvarande regler.

Samtidigt uttalade sig regeringen om begreppet telemeddelande och förklarade varför detta begrepp har behållits i 6 kap. 19 § LEK. Regeringen angav följande (prop. 2002/03:110 s. 269).

I bl.a. 4 kap. brottsbalken och 27 kap. rättegångsbalken används begreppet telemeddelande. I telelagen finns en definition av detta begrepp. Med telemeddelande avses därvid ljud, text, bild, data eller information i övrigt som förmedlas med

> hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare. Begreppet används inte i EG:s regelverk för elektronisk kommunikation och skulle därför inte behövas i övrigt i lagen om elektronisk kommunikation. Som framgår av avsnitt 19.2 föreslås ett särskilt begrepp, elektroniskt meddelande, med avseende på bestämmelserna om integritetsskydd. I avvaktan på sådan ytterligare utredning som nämnts ovan anser regeringen att det, för att inte skapa rättsosäkerhet i fråga om tillämpningen av de författningar som innehåller begreppet telemeddelande, är lämpligt att såsom en övergångslösning använda detta begrepp även i den nya lagen såvitt avser anpassningsskyldigheten. Begreppet bör också definieras i bestämmelsen i enlighet med vad som anges i telelagen.

Regeringen avslutade resonemangen om anpassningsskyldigheten med att bl.a. nämna s.k. IP-telefoni på följande sätt (prop. 2002/03:110 s. 270).

> Som framgår av avsnitt 13 omfattar tillhandahållandet av allmänt kommunikationsnät vad som enligt telelagen definieras såsom att inom ett allmänt tillgängligt telenät tillhandahålla nätkapacitet. Genom den nu föreslagna utformningen av anpassningsskyldigheten torde således ett rättsläge som i allt väsentligt motsvarar dagens uppnås.
>
> Utredningen har som nämnts inte föreslagit någon motsvarighet till gällande begränsning av anpassningsskyldigheten till verksamheter med viss omfattning. Regeringen eller, efter regeringens bemyndigande, den myndighet som regeringen bestämmer skall dock få möjlighet att i enskilda fall medge undantag från kravet på anpassningsskyldighet för en verksamhet. En rimlig avvägning, i stort motsvarande den som nu gäller, bör kunna uppnås med en sådan reglering. Skulle skyldigheten t.ex. bli alltför betungande för en mindre operatör kan undantag således medges.
>
> Beträffande telefoni till fast nätanslutningspunkt som förmedlas med hjälp av Internetprotokoll (IP-telefoni) bör även den som tillhandahåller en sådan tjänst kunna omfattas av skyldigheterna under förutsättning att kriterierna för en allmänt tillgänglig telefonitjänst är uppfyllda. Hitintills har förhållandena varit sådana att IP-telefoni, i vart fall med undantag av viss s.k. gateway-telefoni, dvs. fall där en operatör med

> hjälp av en gränsnätstation (eng. gateway) sköter om övergången från ett kopplat telefonnät till ett paketförmedlat datanät och omvänt, inte faller under definitionen av telefonitjänst.

PTS har i rapporten Internet och lagen om elektronisk kommunikation (PTS-ER-2003:36 s. 44 ff.) utvecklat frågan om IP-telefoni skall anses omfattas av begreppet telefonitjänst enligt 1 kap. 7 § LEK. I paragrafen definieras telefonitjänst som en elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan, inklusive nödsamtal. Om IP-telefoni faller under begreppet telefonitjänst innebär det också att anpassningsskyldighet föreligger enligt 6 kap. 19 § första stycket 2 LEK. PTS angav bl.a. följande i rapporten.

> Den grundläggande skillnaden mellan ett telefonnät (PSTN) och Internet är att PSTN är ett kretskopplat nät optimerat för att uppfylla kraven för telefonsamtal medan Internet är ett paketförmedlat nät optimerat för att överföra data utan realtidskrav.
> ---
> PSTN transporterar redan idag signalerna mellan samtalsparterna i digital form. För IP-telefoni sker omvandlingen av de analoga signalerna till digital form redan i hemmet. Ett inkommande samtal från en användare med ett vanligt E.164-nummer konverteras i en sluss (s.k. gateway) från ett digitalt format till ett annat. Rösten komprimeras sedan för att inkapslas i IP-paket över IP-nätet. De olika kompressionsteknikerna medför ofta ett mindre bandbreddsutnyttjande än i PSTN. Detta leder till att den fysiska kabeln kan utnyttjas bättre vilket bl.a. är en av drivkrafterna för att börja använda IP-teknik i stamnäten för att förmedla vanlig kretskopplad telefoni.
>
> Det föreligger en viss förvirring kring de allmänna begreppen inom IP-telefoni. Internettelefoni och Röst över IP (VoIP, Voice over IP) används för att beskriva kommunikationstransporten. Enligt International Telecommunication Union (ITU) äger IP-telefoni rum över IP-baserade nätverk i allmänhet, medan Internettelefoni, en undergrupp till IP-telefoni, är telefoni mellan enheter helt eller delvis över Internet. Voice over IP, ytterligare en undergrupp till IP-

telefoni, används ofta för att beteckna kommunikation över slutna, privata IP-baserade nätverk.

Det har förelegat en viss ovisshet om huruvida vissa former av IP-telefoni omfattades av telelagens begrepp telefonitjänst eller inte. I och med lagen om elektronisk kommunikation har definitionen av telefonitjänst omformulerats varför erfarenheter och slutsatser från telelagens definition inte självklart längre kan appliceras.

IP-telefoni anses enligt lagen om elektronisk kommunikation utgöra telefonitjänst under förutsättning att överföringen är av sådan kvalité att den av användarna uppfattas som realtid och tjänsten tillåter uppringning och mottagning av samtal till nummer som omfattas av en nummerplan samt nödtelefonnummer.

Kan IP-telefoni då anses utgöra en telefonitjänst? Till en början kan konstateras att allt för stora fördröjningar i talöverföringen inte får förekomma, eftersom tjänsten då inte skulle uppfattas som realtid vilket krävs för att det skall anses utgöra ett samtal. För det andra krävs att nummer ur en nationell eller internationell nummerplan för telefoni måste kunna ringas upp eller tas emot vilket innebär att användare som nyttjar programvara för att kontakta varandra via IP-telefoni direkt mot en IP-adress därmed inte skulle anses utgöra telefonitjänst. Däremot torde IP-telefoni som sker genom s.k. gateway, dvs. fall där operatören tillhandahåller övergången mellan ett kretskopplat telefonnät till ett paketförmedlat datanät, omfattas eftersom möjligheten finns att nå och bli nådd genom nummer ur en nummerplan för telefoni. Det återstår dock ett krav enligt definitionen för att det skall vara tal om en telefonitjänst enligt lagens mening, nämligen att nödtelefonnummer kan nås.

Av förarbetena framgår det uttryckligt att ”för att tjänsten skall omfattas av begreppet krävs att det går att ringa nödsamtal”. Formuleringen torde inte kunna tolkas på annat sätt än om att nödsamtal inte går att ringa så utgör tjänsten inte heller en telefonitjänst. --- I praktiken innebär formuleringen (i lagen om elektronisk kommunikation) att operatörerna ges möjlighet att själva välja om de vill kunna förmedla nödsam-

tal och därmed omfattas av lagens definition av telefonitjänst eller inte.

Det är svårt att generellt säga om IP-telefoni omfattas av begreppet eller inte eftersom IP-telefoni är mer ett samlingsnamn inom vilket en rad olika tekniker kan innefattas. Det får dock nu anses klarare än under telelagen att IP-telefoni som uppfyller vissa kriterier är att anse som telefonitjänst och att operatören som tillhandahåller den då också kan omfattas av de skyldigheter som följer av en sådan tjänst.

Det kan tänkas uppstå relativt svåra gränsdragningar vid avgörandet om vem som faktiskt anses tillhandahålla telefonitjänsten när denna sker över IP-telefoni. Det kan tänkas att Internetoperatörer tillhandahåller själva anslutningen till Internet men att de inte vare sig kan eller vill kontrollera om trafiken som sker över nätet utgör taltelefoni eller annan kommunikation. Den Internetoperatör som tillhandahåller anslutningen behöver inte ha något samarbete eller kontakt med den aktör som tillhandahåller en ”gateway” eller annan möjlighet till övergång mellan ett paketförmedlat datanät och ett kretskopplat telefonnät. Det torde i sådana fall inte anses vara självklart vem som kan anses tillhandahålla telefonitjänsten och därmed vem som skall bli ansvarig för de skyldigheter som lagen medför. Det får ankomma på den framtida rättstillämpningen att närmare avgöra dessa avgränsningar.

Som nyss nämndes innebär lagen om elektronisk kommunikation att den tidigare tillståndsplikten för viss verksamhet har ersatts av en anmälningsplikt. Detta har haft till följd att de tillståndsvillkor om anpassningsskyldighet som var kopplade till de gamla tillstånden upphörde att gälla i samband med ikraftträdandet av lagen om elektronisk kommunikation. Den slutsatsen kan dras eftersom det saknas övergångsbestämmelser om fortsatt giltighet av de tillståndsvillkoren i lagen (2003:390) om införande av lagen om elektronisk kommunikation.

Det nu sagda måste därmed innebära att anpassningsskyldigheten gäller, så att säga, fullt ut, dvs. operatörerna har en skyldighet att se till att aktuella verksamheter bedrivs så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, allt enligt vad som föreskrivs i 6 kap. 19 § första stycket LEK.

Den enskilde operatören har dock, enligt 6 kap. 19 § fjärde stycket LEK, en möjlighet att begära undantag från kravet på hur verksamheten skall bedrivas i det nämnda avseendet. Undantagsbestämmelsen, som alltså medger beslut anpassade efter omständigheterna i det enskilda fallet, kom till mot bakgrund av att den anpassningsskyldighet som anges i lagen om elektronisk kommunikation inte är begränsad till verksamheter av viss storlek. Skulle skyldigheten bli allt för betungande för en mindre operatör, kan undantag medges efter en prövning i det enskilda fallet (prop. 2002/03:110 s. 270).

Enligt 6 kap. 19 § fjärde stycket LEK meddelar regeringen eller den myndighet som regeringen bestämmer föreskrifter rörande anpassningsskyldigheten. I 36 § förordningen (2003:396) om elektronisk kommunikation har regeringen bestämt att PTS, efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen, dels får utfärda verkställighetsföreskrifter, dels får medge undantag i enskilda fall från kravet på hur verksamheten skall bedrivas enligt 6 kap. 19 § första stycket LEK. Verkställighetsföreskrifterna i sig kan inte innehålla generella undantag från anpassningsskyldigheten.

PTS har i rapporten Internet och lagen om elektronisk kommunikation skrivit om anpassningsskyldigheten för bl.a. de s.k. Internetoperatörerna. Det sistnämnda begreppet används i många olika sammanhang med en viss begreppsförvirring när det gäller termerna Internet Service Provider (ISP) och Internetoperatör. Med ISP avses vanligen de företag som erbjuder Internetaccsess till slutkunder – hushåll eller företag. Med Internetoperatör avses ibland hela gruppen ISP:er och ibland bara de som själva äger det nät som Internetanslutningen nyttjar. PTS menar att med Internetoperatör bör avses detsamma som operatör enligt lagen om elektronisk kommunikation (den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation, 1 kap. 7 § LEK) men också tillhandahållare av en allmän elektronisk kommunikationstjänst. På det sättet skulle definitionen av Internetoperatör innefatta de “klassiska” ISP:erna (som innehar ett eget kommunikationsnät eller råder/förfogar över eller hyr access till ett elektroniskt kommunikationsnät) och sådana ISP:er som inte själva råder över det nät kommunikationen sker över (PTS-ER-2003:36 s. 13 f.). PTS uttalade sig om anpassningsskyldigheten enligt lagen om elektronisk kommunikation i förhållande till skyldigheten enligt den upphävda telelagen på följande sätt (s. 43 f.).

Konsekvenserna för vissa Internetoperatörer torde kunna bli omfattande. Även om syftet med bestämmelsen är att upprätthålla rättsläget från telelagen kommer den nya bestämmelsen att omfatta en bredare grupp av aktörer. Telelagens bestämmelser omfattade nämligen de aktörer som innehade tillstånd. Att erhålla ett tillstånd krävde att aktören bedrev en viss form av verksamhet och att verksamheten hade en viss omfattning. Även om de verksamheter som angivits i lagen om elektronisk kommunikation i stort kan anses motsvaras av telelagens bestämmelser om tillstånd återstår fortfarande problemet med verksamhetens omfattning. I lagen om elektronisk kommunikation ges inget krav på att verksamheten skall ha en viss omfattning utan anmälningsplikten är betydligt bredare än telelagens tillståndsplikt. Det innebär att en större grupp av Internetoperatörer, låt vara inom samma typ av verksamheter som under telelagen, kommer att omfattas av bestämmelsen. Det bör vidare understrykas att begreppet teletjänst givits en ny definition i lagen om elektronisk kommunikation, vilken sannolikt kan komma att innebära en förändring av de typer av aktörer som kan anses omfattas av begreppet. Bland annat kan Internetoperatörer som tillhandahåller IP-telefoni anses tillhandahålla en telefonitjänst vilket under tidigare lagstiftning inte var självklart. Även om anpassningsskyldigheten i avvaktan på ytterligare utredning inte skall vara annorlunda än enligt telelagen torde därför konsekvenserna kunna bli betydande för de Internetoperatörer som tidigare inte ansågs vara tillståndsskyldiga.

Tillsynsmyndigheten ges möjlighet att i enskilda fall meddela undantag från bestämmelsen. Sådana undantag torde i främsta fall bli aktuella då skyldigheten skulle bli alltför ekonomiskt betungande för en mindre Internetoperatör. Mot beaktande av att bestämmelsen enligt direktivet skall vara icke diskriminerande torde det dock finnas svårigheter för tillsynsmyndigheten att meddela generella föreskrifter om undantag från skyldigheten i de eventuella fall där skyldigheten kan anses allt för betungande för en hel typ av tjänst. Detta skulle kunna innebära att incitamentet minskar för Internetoperatörer att tillhandahålla tjänster som kan betecknas som telefonitjänster, eftersom de i sådana fall undviker bestämmelsen (under förutsättning att de inte tillhandahåller ett allmänt kommunikationsnät). En sådan utveckling vore olycklig då den torde motverka konvergensen mellan tradi-

tionell taltelefoni och annan elektronisk kommunikation. --- Konsekvenserna, särskilt för mindre tillhandahållare av allmänna kommunikationsnät, torde kunna bli både tekniskt och ekonomiskt betungande.

6.6 Våra överväganden

6.6.1 Var bör bestämmelsen vara placerad?

Förslag: Anpassningsskyldighet för operatörer skall finnas även fortsättningsvis och vara föreskriven i lagen om elektronisk kommunikation.

Vårt uppdrag är i huvudsak att göra en översyn av vilka verksamheter som bör omfattas av anpassningsskyldigheten och hur den skall vara reglerad i olika avseenden. Bestämmelserna om anpassningsskyldighet är i praktiken ofta en förutsättning för att beslut om tvångsmedlen över huvud taget skall kunna verkställas och att verkställandet kan ske i nära anslutning till domstolens beslut.

När skyldigheten infördes uttalade regeringen att hemlig teleavlyssning och hemlig teleövervakning är betydelsefulla och oumbärliga hjälpmedel i kampen mot särskilt den grova brottsligheten och att det av effektivitetsskäl är ytterst angeläget att möjligheterna till verkställighet av tvångsmedlen på området upprätthålls (prop. 1995/96:180 s. 17 f.). Den slutsatsen är än mer giltig i dag, framför allt mot bakgrund av teknikutvecklingen under senare tid. En annan sak är att nya tvångsmedel av den anledningen kan behöva tillskapas för att myndigheterna skall kunna bekämpa brottsligheten på ett sätt som hittills inte har varit möjligt (se avsnitt 9 angående hemlig dataavläsning).

Som också nämndes i samband med att anpassningsskyldigheten infördes är det av många skäl inte ett rimligt alternativ att polisen och andra brottsutredande myndigheter på egen hand svarar för den anpassning som krävs för att det skall vara möjligt att genomföra hemlig teleavlyssning och hemlig teleövervakning (prop. 1995/96:180 s. 23). Att anpassningsåtgärder har skett från operatörernas sida är som sagt en allmän förutsättning för att tvångsmedlen skall kunna verkställas. Det bör särskilt framhållas att frågan har stor betydelse för allmän ordning och allmän säkerhet, där-

ibland rikets säkerhet och skyddet mot terrorism. Det är orimligt att förutsätta att alla de operatörer som kan vara aktuella vid verkställigheten frivilligt skulle medverka i den utsträckning som erfordras. Det råder ingen tvekan om att en författningsreglerad anpassningsskyldighet är en avgörande förutsättning för en effektiv verkställighet och måste finnas även fortsättningsvis. Något annat följer heller inte av våra direktiv.

I dag finns anpassningsskyldigheten föreskriven i lagen om elektronisk kommunikation. När skyldigheten infördes i telelagen uttalade regeringen (prop. 1995/95:180 s. 29) att den föreslagna ordningen lämpligen borde regleras i telelagen och att en hänvisning skulle göras i rättegångsbalken till telelagens bestämmelser. Hänvisningen finns i 27 kap. 25 § andra stycket RB, där det numera sägs att i lagen om elektronisk kommunikation finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning som gäller för den som driver verksamhet som avses i 6 kap. 19 § den lagen.

I 27 kap. 25 § första stycket RB finns bestämmelsen som innebär att de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen får användas av de brottsutredande myndigheterna vid verkställigheten av tvångsmedlen. Vi behandlar den bestämmelsen i avsnitt 8 och konstaterar där att regeln redan i dag innebär bl.a. att de tekniska hjälpmedlen får anslutas, underhållas och återtas, vilket tidigare också framgick av paragrafens ordalydelse, samt att det av detta följer att operatörerna har en skyldighet att biträda polisen vid verkställigheten. Vi föreslår i samma avsnitt en förändring av paragrafen så att skyldigheten för operatörerna att medverka vid verkställigheten utvidgas. Det måste påpekas att skyldigheten att medverka inte är densamma som anpassningsskyldigheten. Det utvecklas närmare i avsnitt 8.3.

Anpassningsskyldigheten är av central betydelse för effektiviteten vid verkställigheten av beslut om hemlig teleavlyssning och hemlig teleövervakning och har som syfte att möjliggöra användningen av tvångsmedlen och därmed skapa förutsättningar för effektiva utredningar när det gäller grövre brott. Bestämmelserna i lagen om elektronisk kommunikation, där anpassningsskyldigheten finns föreskriven, är av näringsrättslig art och syftar till att enskilda och myndigheter skall få tillgång till säkra och effektiva elektroniska kommunikationer på en väl fungerande marknad (se t.ex. prop. 2002/03:110 s. 114). Rikspolisstyrelsen har till oss uttryckt den uppfattningen att vid tolkningen och tillämpningen av bestämmelsen om anpassningsskyldighet har det lagts allt för stor vikt vid det

näringsrättsliga synsättet och att bestämmelsens stora betydelse från brottsutredningssynpunkt har kommit i skymundan.

Vi har mot den bakgrunden diskuterat om anpassningsskyldigheten bör vara föreskriven i lagen om elektronisk kommunikation. Bl.a. som en följd av vårt förslag nedan till utformning av anpassningsskyldigheten som en mer generell skyldighet än i dagsläget med möjlighet för Rikspolisstyrelsen att föreskriva om undantag, har vi kommit fram till att det för närvarande inte finns tillräckliga skäl att flytta bestämmelsen. Det bakomliggande syftet med anpassningsskyldigheten är och förblir att underlätta tvångsmedlen. Vi vill dock understryka att om det visar sig att bestämmelserna om anpassningsskyldigheten får en allt för snäv tillämpning ur ett brottsutredande perspektiv, måste det övervägas att föreskriva om skyldigheten någon annanstans, kanske i rättegångsbalken. Där finns redan i dag exempelvis bestämmelserna om operatörernas skyldigheter att på visst sätt medverka vid verkställigheten.

6.6.2 Vad innefattas i anpassningsskyldigheten?

Förslag: I lagtexten skall anpassningsskyldigheten, liksom i dag, uttryckas så att den verksamhet som avses skall bedrivas så att beslut om avlyssning och övervakning kan verkställas och så att verkställandet inte röjs samt så att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden görs tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand.

I samband med att anpassningsskyldigheten infördes gjordes, som framgick tidigare, några uttalanden om vad som innefattas i den skyldigheten (prop. 1995/96:180 s. 25 ff.). Det kan inte vara fråga om anpassningar av systemen varje gång ett beslut om tvångsmedel skall verkställas. Det är i stället fråga om en generell skyldighet som hänför sig till konstanta egenskaper i systemen, oberoende av om det pågår någon hemlig teleavlyssning eller hemlig teleövervakning. Systemen skall vid varje givet tillfälle innehålla de egenskaper som behövs för att tvångsmedelsbesluten skall kunna verkställas. Den närmare innebörden av skyldigheten blir i praktiken ett krav på att operatörerna skall hålla beredskap och kunna verkställa tvångsmedelsbesluten genom att använda sig av tekniska hjälpmedel som har vissa egenskaper. Operatörerna skall därför använda sig av viss maskinell utrustning, hårdvaror och av de datorprogram och mjukvaror som erfordras för att tillgodose de krav som riktas mot dem.

Operatörerna skall också vidta de personella och organisatoriska dispositioner som krävs för att hantera hjälpmedlen.

I den resolution om hemlig teleavlyssning och hemlig teleövervakning som nämndes tidigare (9529/95 ENFOPOL 90) och som fortfarande är gällande finns en bilaga med polisiära behov, vilka skulle vara en utgångspunkt i det nationella lagstiftningsarbetet rörande anpassningen. Regeringen uttalade att behoven var så långtgående att de inte utan vidare kunde läggas till grund för lagstiftning, även om det stod klart att operatörerna måste uppfylla många av kraven (prop. 1995/95:180 s. 26 f.). Som också nämndes tidigare avfärdade regeringen ett förslag om att det skulle fastställas standardiserade normer för samtliga operatörer som var anpassningsskyldiga. Skälen var främst den stora variation som finns hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar samt den fortlöpande tekniska utvecklingen.

Regeringen gjorde även uttalanden om vad som skulle innefattas i anpassningsskyldigheten. Mot bakgrund av teknikutvecklingen och med tanke på att varje operatörs system är unikt är det inte möjligt att i detalj beskriva vad anpassningsskyldigheten för dagen innebär. Däremot kan exempelvis följande nämnas om innebörden vid hemlig teleavlyssning, vilket i tillämpliga delar även gäller vid hemlig teleövervakning.

- ✓ Anpassning skall ske så att konstanta egenskaper finns i systemen för att upprätthålla beredskap inför verkställighet av beslut om tvångsmedlen. Anpassningsskyldigheten omfattar införandet av teknik som gör det möjligt att överföra telemeddelanden fram till och med den s.k. överlämningspunkten där informationen överlämnas till polisen. Ett exempel på en konstant egenskap är att det med nuvarande teknik i GSM-system förs in en mjukvara i systemens växlar som för över de telemeddelanden som omfattas av verkställighetsbeslut till polisen.
- ✓ Anpassningsskyldigheten omfattar åtgärder som gör de möjligt för polisen att ta del av såväl innehåll i meddelanden (ljud, bilder, text, data etc.) som trafikuppgifter och lokaliseringsuppgifter.
- ✓ Telemeddelanden skall kunna identifieras och polisen få tillgång till innehållet utan inskränkning och utan att andra telemeddelanden avlyssnas.
- ✓ Verkställigheten skall inte riskera att röjas, dvs. tvångsmedlen skall kunna verkställas på sådant sätt att åtgärderna inte

obehörigen riskerar att röjas inom den egna verksamheten eller för den som är föremål för åtgärden eller för tredje man. Operatören skall iaktta de säkerhetskrav som följer av lag eller annan författning, framförallt säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) och aktuella föreskrifter. Kraven enligt sistnämnda regelverk kan avse informationssäkerhet, tillträdesbegränsning och säkerhetsprövning.

- ✓ Abonnenternas kommunikation skall inte märkbart påverkas av en pågående verkställighet.
- ✓ Vid medflyttning och liknande skall avlyssningen alltjämt kunna begränsas till den teleadress som beslutet avser.
- ✓ Kapacitet skall finnas för att genomföra flera avlyssningar samtidigt.
- ✓ Polisen skall kunna få tillgång till telemeddelanden i realtid eller i vart fall i omedelbar anslutning till att de förmedlas.
- ✓ Telemeddelanden skall göras tillgängliga för polisen på ett sådant sätt och på en sådan plats att informationen enligt polisens bedömning enkelt kan tas om hand. Att operatören använder teknik för att effektivisera överföring i sitt eget nät, s.k. kodnings- eller komprimeringsteknik, innebär ingen begränsning i skyldigheten att oavsett teknikval leverera information till polisen på ett sådant sätt och i ett sådant standardiserat format att informationen enkelt kan tas om hand. Skyldigheten innebär bl.a. att sambandet mellan telemeddelanden och informationen inte får förvrängas eller att informationen på annat sätt får ett felaktigt innehåll.
- ✓ Telemeddelanden skall levereras till polisen i klartext om operatören tillhandahåller krypteringssystem eller liknande.
- ✓ Samtliga de uppgifter som omfattas av hemlig teleövervakning skall kunna hämtas in.
- ✓ Varje operatör har trots samtrafik ett eget ansvar för anpassningen och skall se till att den tekniska standarden, servicen och tillgängligheten vad gäller anpassningen i övrigt motsvarar vad som gäller i operatörens övriga verksamhet.

De uttryck som används i dag i lagen om elektronisk kommunikation för att uttrycka anpassningsskyldighetens innebörd är att verksamheten skall bedrivas dels så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, dels så att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden görs tillgängliga för polisen så att

informationen enkelt kan tas om hand. Enligt vår mening beskriver det uttryckssättet väl de krav som bör ställas på operatörerna i detta avseende. Det finns bl.a. mot bakgrund av teknikutvecklingen ingen anledning att i lagtexten beskriva skyldigheten på en högre detaljnivå än så.

Regeringen har nyligen lämnat propositionen 2004/05:144 Internationell rättslig hjälp i brottmål: Tillträde till 2000 års EU-konvention m.m. till riksdagen. Regeringen föreslår där bl.a. två nya former av rättslig hjälp, nämligen tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning samt tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning. Förslagen skall ses mot bakgrund av utvecklingen av ny teknik, t.ex. möjligheterna att avlyssna och övervaka en person som finns i en annan stat. Dessutom gör tekniken det möjligt att omedelbart överföra telemeddelanden utan att den stat som tekniskt bistår med avlyssningen behöver ta upp avlyssningen. Det sker i stället i den stat som begärt hjälp (s. 2).

Användningen av t.ex. satellitsystem för telemeddelanden gör det möjligt att fånga upp och vidareförmedla meddelanden som sänds eller tas emot inom mycket vidsträckta geografiska områden. Åtkomsten sker via en markstation, en s.k. nätport. Detta kan innebära att en stat vars territorium befinner sig inom satellitens täckningsområde, men som inte har någon nätport, tekniskt sett inte kan avlyssna vissa telemeddelanden som sänds eller mottas på dess territorium. I dessa fall får den stat som vill avlyssna telemeddelandena ansöka om rättslig hjälp från den stat där nätporten är belägen. En annan, mer permanent lösning är att den kommunikation som sker via nätporten görs tillgänglig för andra stater genom användning av en slags fjärrkontroll (s. 101).

I propositionen berör regeringen anpassningsskyldigheten och nämner bl.a. att om en installation för fjärråtkomst till en utländsk nätport skall anses utgöra en del av en operatörs verksamhet som omfattas av anpassningsskyldigheten får avgöras om det blir aktuellt att installera en fjärrkontroll i Sverige (s. 103). När det gäller frågan om andra stater skall ha direkt åtkomst via en fjärrkontroll till en svensk nätport anger regeringen att det torde kräva en utvidgad anpassningsskyldighet enligt lagen om elektronisk kommunikation (s. 105). De nu aktuella frågorna har väckts i slutskedet av vårt arbete och det har inte funnits tid att utreda behovet av förändringar i lagstiftningen.

6.6.3 Vilka verksamheter skall omfattas av anpassningsskyldigheten?

Förslag: Anpassningsskyldigheten skall omfatta verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. RB eller tjänster inom ett sådant nät.

Utgångspunkter

Enligt telelagen omfattade skyldigheten att anpassa verksamheten de operatörer som hade fått tillstånd att inom ett allmänt tillgängligt telenät tillhandahålla telefonitjänst till fast nätanslutningspunkt, mobil teletjänst eller nätkapacitet, om verksamheten ansågs vara betydande. För en sådan operatör omfattade skyldigheten enbart den tillståndsgivna verksamheten och inte annan verksamhet som den operatören eventuellt bedrev (prop. 1995/96:180 s. 26).

Lagen om elektronisk kommunikation utgår från en anmälningsplikt och inte en tillståndsplikt för operatörerna avseende viss verksamhet. I samband med att telelagen upphörde att gälla förändrades även utformningen av den aktuella bestämmelsen om vilka verksamheter som omfattas av anpassningsskyldigheten. Anpassningsskyldigheten omfattar enligt 6 kap. 19 § första stycket LEK de verksamheter som avser tillhandahållande av

- ✓ ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller
- ✓ tjänster inom ett allmänt kommunikationsnät vilka består av
  - en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller
  - en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

I lagen om elektronisk kommunikation finns alltså angivet vilka verksamheter som omfattas av anpassningsskyldigheten. En del av de begrepp som används i bestämmelsen definieras i andra bestämmelser i lagen. Regeringen uttalade i propositionen (prop. 2002/03:110 s. 269) att någon saklig ändring av vilka verksamheter som omfattades av anpassningsskyldigheten inte var avsedd i samband med att lagen om elektronisk kommunikation infördes men hänvisade också till det vidare utredningsarbetet.

Bestämmelserna i rättegångsbalken om hemlig teleavlyssning och hemlig teleövervakning är teknikneutrala och således inte begränsade till en viss typ av teknik för att befordra meddelanden. Enligt reglerna får telemeddelanden avlyssnas eller övervakas om de befordras eller har befordrats till eller från ett telefonnummer, kod eller annan teleadress (27 kap. 18 och 19 §§ RB). Om det är fråga om fast telefoni, mobiltelefoni eller Internet har alltså ingen betydelse för frågan om meddelandet är sådant att det faller under tvångsmedelsregleringen. Vi nämnde i avsnitt 3.2 att två grundläggande utgångspunkter när nya bestämmelser utformas bör vara att skilda lösningar för olika typer av elektronisk kommunikation skall undvikas och att regleringen i största möjliga utsträckning skall göras oberoende av den snabba tekniska utvecklingen och kunna stå sig över tiden. Det gäller givetvis även utanför rättegångsbalkens område.

Den anpassningsskyldighet som operatörerna åläggs i 6 kap. 19 § LEK är begränsad så till vida att den inte omfattar samtliga de verksamheter där sådana meddelanden som omfattas av tvångsmedlen befordras eller, om man så vill, samtliga de tekniker som är aktuella. Trots att den legala möjligheten finns att avlyssna eller övervaka ett visst meddelande enligt rättegångsbalken, medför avsaknaden av anpassningsskyldighet för vissa verksamheter stora effektivitetsförluster vid utredning av grova brott, eftersom tvångsmedelsbesluten med stor sannolikhet inte kan verkställas över huvud taget. Till det kommer att anpassningsskyldigheten leder till en snabb verkställighet, vilket ofta kan vara av stor betydelse i det brottsutredande arbetet.

Säkerhetspolisen har berättat om de operativa begränsningar som den nuvarande bestämmelsen för med sig. Av sekretesskäl väljer vi att avstå från att redogöra för dessa. Vi kan ändå konstatera att inte minst teknikutvecklingen medför att anpassningsskyldigheten behöver vidgas om inte den brottsutredande verksamheten skall hamna hjälplöst efter den grövre brottsligheten.

I samband med att anpassningsskyldigheten infördes uttalade regeringen att varje gräns medför att det kan bli någon gråzon där det är osäkert om en viss operatör faller strax innanför eller utanför gränsen och att det därför är angeläget att se till att gränsdragningen blir så förutsebar och klar som möjligt. Detta är en viktig utgångspunkt även vid våra överväganden. Den nuvarande regleringen av vilka verksamheter som omfattas av anpassningsskyldigheten ger i flera fall inte sådana klara besked.

Tydlighet i regleringen

Såväl Rikspolisstyrelsen som operatörerna har efterlyst en tydlighet och förutsebarhet när det gäller anpassningsskyldighetens omfattning. Gränserna för anpassningsskyldigheten har uppenbarligen många gånger har varit föremål för skilda uppfattningar och diskussioner mellan bl.a. Rikspolisstyrelsen och operatörerna. Oklarheter när det gäller gränserna för anpassningsskyldigheten, tillsammans med frågan om kostnadsansvaret för anpassningsåtgärderna (se nedan), förefaller vara de främsta orsakerna till att anpassningsarbetet hos operatörerna i många fall är lågt prioriterat. Rikspolisstyrelsens uppfattning har också varit och är fortfarande att den nuvarande regleringen är otillräcklig ur ett brottsutredande perspektiv, vilket även vi har konstaterat. T.ex. har Rikspolisstyrelsen bedömt att det är otillräckligt att anpassningskravet omfattar datakommunikation med viss angiven lägsta datahastighet vid överföring i de fasta telenäten, vilket är en begränsning som inte finns för de mobila näten. Det kan nämnas att regeringen förutskickade redan i samband med att anpassningsskyldigheten infördes att den avvägning som då gjordes kunde komma att bli allt för snäv i en framtid (prop. 1995:96:180 s. 25).

Ett skäl till oklarheten är att teknikutvecklingen, tillsammans med en bristfällig logik i terminologin gör det svårt att varaktigt klargöra vilka verksamheter som omfattas av den nuvarande anpassningsskyldigheten. En svårighet uppkommer exempelvis genom att tjänster som tidigare tillhandahållits endast i de kopplade telefoninäten nu tillhandahålls även genom Internet, varigenom definitioner som exempelvis telefonitjänst har blivit oklar. Detsamma gäller gränsdragningen mellan att tillhandahålla allmänna kommunikationsnät och att tillhandahålla elektroniska kommunikationstjänster. Även innebörden av begrepp som elektronisk kommunikationstjänst torde i gränsfall kräva klargörande genom

rättstillämpningen eller av lagstiftaren. Genom detta kan effektiviteten av ett tvångsmedel komma att undergrävas till följd av tveksamheter vad gäller anpassningskravet. Detsamma gäller för övrigt på verkställighetsstadiet. Samma tjänst kan omfattas av anpassningskravet – och möjligheten att verkställa tvångsmedlet – eller inte, beroende på vilken teknik som valts för att tillhandahålla tjänsten. Exempel på detta är uppkoppling till Internet. Detta är självfallet otillfredsställande såväl för brottsutredningarnas effektivitet som från rättssäkerhetssynpunkt.

Även från operatörernas sida har det framförts att anpassningsskyldighetens omfattning måste tydliggöras i författning och att skyldigheten i enskilda fall inte bör bero på t.ex. resultatet av en förhandling mellan operatören och en myndighet.

Vi instämmer helt i de uppfattningar som finns både hos Rikspolisstyrelsen och hos operatörer om att anpassningsskyldighetens omfattning måste regleras tydligare än i den gällande lagstiftningen. För att åstadkomma detta bör skyldigheten så långt det är möjligt regleras i författning och inte vara en förhandlingsfråga mellan en operatör och en myndighet. Vi vill därför inte förorda en ordning som Rikspolisstyrelsen föreslagit och som innebär att polisen och den enskilde operatören skulle vid förhandlingar komma överens om hur anpassningsskyldigheten skall fullgöras och att PTS vid oenighet skulle få medla och eventuellt avgöra frågan.

För att i största möjliga mån undvika den osäkerhet som hittills har funnits i frågor rörande anpassningsskyldigheten och de problem och effektivitetsförluster som detta har medfört, är det enligt vår uppfattning och särskilt mot bakgrund av den snabba tekniska utvecklingen helt nödvändigt att reglera skyldigheten på ett så teknikneutralt sätt som möjligt, dvs. utan att t.ex. viss typ av överföringsteknik anges i författningstexten.

Vårt förslag blir därför att anpassningsskyldigheten skall träffa verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. RB eller elektroniska kommunikationstjänster inom ett sådant nät. Verksamheten skall bedrivas så att beslut om avlyssning och övervakning kan verkställas och så att verkställandet inte röjs. Dessutom skall innehållet i och uppgifter om avlyssnade eller övervakade meddelanden göras tillgängliga för polisen på sådant sätt att informationen enkelt kan tas om hand. Vi föreslog i avsnitt 3.4 att det i 27 kap. 18 § fjärde stycket RB skulle föras in en definition av vad elektroniskt kommunikationsnät avser i 27 kap. RB. Med det begreppet avses detsamma som i lagen om elektronisk kommunikation med undan-

tag för nät som enbart är avsett för utsändning av program i ljudradio eller television.

Den utvidgning av anpassningsskyldigheten som i praktiken följer av förslaget och som främst motiveras av det stora allmänna intresset av att effektivt kunna verkställa tvångsmedlen vid misstankar om grova brott, är att kravet också kommer att omfatta verksamhet som avser tillhandahållande av Internettjänster. Dessutom kommer anpassningsskyldigheten i de fasta telenäten inte att bli begränsad till en viss lägsta datahastighet för funktionell tillgång till Internet.

Anpassningsskyldigheten skall alltså gälla både för den som tillhandahåller nät och för den som tillhandahåller tjänst. Detta kan i praktiken innebära en parallell skyldighet, vilket dock inte med automatik innebär att det måste vidtas ”dubbla” anpassningsåtgärder. Primärt ansvarig för anpassningen bör vara den som tillhandahåller tjänsten. Den som tillhandahåller nätet bör vara ansvarig för att möjliggöra tjänstetillhandahållarens anpassningsåtgärder. De bör också vara skyldiga att tillsammans vidta åtgärder för anpassningen om detta är möjligt. Genom detta ges förutsättningar att välja den lösning som tillgodoser brottsutredande myndigheters behov till lägsta kostnad för de anpassningsskyldiga. Det kan t.ex. komma att medföra att den som tillhandahåller tjänster genom annans nät köper sin del av anpassningsåtgärderna från den nätinnehavare han har valt.

Regeringen uttalade i samband med att anpassningsskyldigheten infördes (prop. 1995/96:180 s. 24) att det naturligtvis skulle vara önskvärt om samtliga operatörer anpassade sina system så att hemlig teleavlyssning och hemlig teleövervakning enkelt kunde genomföras i den utsträckning som regleringen i rättegångsbalken medger men framhöll också att en sådan ordning är förenad med betydande svårigheter, bl.a. av marknadsmässigt slag. Regeringen nämnde att en generell skyldighet kunde drabba de mindre operatörerna hårt, motverka konkurrensen och hämma nyetableringar och att det skulle föra för långt att belasta innehavare av privata nät, t.ex. interna företagsnät, med långtgående skyldigheter att svara för telesystemens uppbyggnad och utformning.

Det är självfallet så att många operatörer inte skall behöva vidta några anpassningsåtgärder över huvud taget eftersom de är så ointressanta ur ett polisoperativt perspektiv att det inte vore rimligt att med hänsyn framför allt till kostnaderna kräva sådana åtgärder av operatören. I andra fall är det kanske bara vissa begränsade anpassningar som bör genomföras.

I 27 kap. 20 § andra stycket RB finns den begränsning som innebär att avlyssning eller övervakning inte får avse telemeddelanden som 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. Från tillämpningsområdet för tvångsmedelsbesluten och därmed också från anpassningskravet undantas bl.a. system för snabbtelefoner, porttelefoner, PC-nät och liknande utrustning inom eller intill en bostad, hörslingor för hörselskadade eller interna system för personsökning i form av fasta installationer. Även interna telekommunikationer på mindre arbetsplatser via t.ex. PC-nät utgör telenät av mindre betydelse. Motsatsen gäller vanligtvis beträffande sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät eller större företagsnät. Detsamma gäller fristående datorer som är försedda med modem och datorer i t.ex. små interna nätverk som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem. Om kommunikationen endast sker internt inom ett slutet nät bör det krävas att nätet är av större omfattning för att en tvångsåtgärd skall få äga rum. Frågan om ett telenät skall anses vara av mindre betydelse prövas utifrån en samlad bedömning av de olika omständigheter som rör ett telenäts betydelse från allmän kommunikationssynpunkt. Då kan bl.a. antalet anslutningar, geografisk spridning och hur utrustningen fungerar och används ha betydelse (prop. 1994/95:227 s. 27 och 31 och Fitger, Rättegångsbalken 2 s. 27:41). I domstolens tillstånd till hemlig teleavlyssning och hemlig teleövervakning skall det enligt 27 kap. 21 § tredje stycket RB särskilt anges om tvångsmedlen får verkställas utanför ett allmänt tillgängligt telenät.

Det är en självklarhet att det inte skall finnas ett anpassningskrav för sådana verksamheter där meddelandena över huvud taget inte får bli föremål för beslut om hemlig teleavlyssning och hemlig teleövervakning. Av hänsyn till mindre operatörer finns det också skäl att begränsa omfattningen av anpassningsskyldigheten ytterligare. Vi har därför valt att i lagtexten föreskriva att den verksamhet som omfattas av skyldigheten skall avse ett *allmänt* tillhandahållande av näten respektive tjänsterna.

Genom att anpassningsskyldigheten skall omfatta ett allmänt tillhandahållande utesluts bl.a. sådana nät eller tjänster som inte står till förfogande för användning av allmänheten och som samtidigt inte heller effektivt konkurrerar med sådan verksamhet. Sålun-

da kommer företag, bostadsrättsföreningar eller andra sammanslutningar som internt tillhandahåller vissa tjänster generellt sett inte att vara anpassningsskyldiga, även om beslut om tvångsmedel kan omfatta meddelanden som befordras i deras nät. I den mån dessa erbjuder sina tjänster till en vid krets, t.ex. i en stadsdel eller ett motsvarande större geografiskt område, och därigenom kan sägas effektivt konkurrera med operatörer på marknaden, kommer de dock att omfattas av anpassningsskyldigheten. Det skall dock tilläggas att vi nedan föreslår att undantag från anpassningsskyldigheten kan meddelas för den enskilde.

Det skall nämnas att Rikspolisstyrelsen när det gäller anpassningsåtgärder kräver enligt uppgift enbart att operatörerna följer standardlösningar i den mån sådana finns för anpassning i sina system. De standarder som för närvarande finns på området, t.ex. ETSI, omfattar emellertid inte exempelvis nationella krav på säkerhetsskydd eller tekniklösningar som är anpassade till andra nationella krav. Standarderna lämnar även i övrigt öppet hur vissa nationella parametrar skall beaktas, t.ex. vad som krävs för att tillgodose brottsutredande myndigheters behov av tvångsmedlen.

Det måste, när den författningsreglerade anpassningsskyldigheten till stor del blir ”absolut”, finnas en möjlighet till avvägning mellan nytta eller effektivitet och ekonomi efter mer individuella bedömningar och utan att några preciserade anvisningar ges i författningsform. Frågan blir då om sådana undantag skall ges i form av generella föreskrifter eller som undantagsbeslut i enskilda fall.

6.6.4 Skall undantagen meddelas genom generella föreskrifter eller genom beslut i enskilda fall?

Förslag: Rikspolisstyrelsen skall i enskilda fall få medge undantag från anpassningsskyldigheten.

Rikspolisstyrelsens beslut skall få överklagas hos allmän förvaltningsdomstol. Prövningstillstånd skall krävas vid överklagande till kammarrätten.

Undantagens karaktär

Som framkom tidigare avfärdade regeringen i samband med att anpassningsskyldigheten infördes den synpunkten att det skulle fastställas standardiserade normer som skulle gälla för samtliga opera-

törer. Skälen var främst den stora variation som finns hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar samt den fortlöpande tekniska utvecklingen. I stället skulle PTS meddela tillståndsvillkor för varje operatör och därigenom avgöra vilka åtgärder som skulle vidtas i det enskilda fallet för att uppfylla kraven på anpassning. Regeringen uttalade också att det inte fanns något hinder för PTS att närmare precisera krav i generella föreskrifter inom ramen för den normala föreskriftsrätten rörande tillståndsvillkor (prop. 1995/95:180 s. 28 f.).

Av redogörelser från Rikspolisstyrelsen och PTS framgår i avsnitt 6.4 något om hur den nuvarande lagstiftningen har tillämpats. Handläggningen av ärendena har tagit avsevärd tid i anspråk. Exempelvis utfärdade PTS likalydande, generella tillståndsvillkor i vissa delar först ett par år efter det att bestämmelserna om anpassningsskyldighet hade trätt i kraft. Dessutom fanns en sex månader lång övergångstid. Av de handlingar vi har tagit del av framgår att Rikspolisstyrelsen vid endast ett tillfälle överklagat PTS beslut och att överklagandet sedermera återkallades. PTS avgöranden har därigenom fått styra utformningen av anpassningsskyldigheten. Avvägningen mellan telepolitiska och kriminalpolitiska mål har inneburit att PTS har tagit relativt stor hänsyn till operatörernas kostnader, främst – i brist på annat – på grundval av operatörernas egna uppgifter och bedömningar. Detta har Rikspolisstyrelsen framhållit som otillfredsställande, särskilt som enbart en tredjedel av de tillståndspliktiga operatörer som berördes av Rikspolisstyrelsens begäran om tillägg till tillståndsvillkoren svarade på PTS remiss under våren 2001. Enligt Rikspolisstyrelsens bedömning har resultatet i något fall blivit att operatörer inte varit skyldiga att tillhandahålla brottsutredande myndigheter standardfunktioner, trots att operatörerna redan haft funktionerna i sina verksamheter. De likalydande villkoren har inte varit tillräckliga för att åstadkomma effektiva verkställigheter av enskilda tvångsmedelsbeslut. Förutom att villkoren inte utformats med beaktande av den individuella tekniska beskaffenheten hos respektive operatör, har anledningen främst varit att villkor om anpassning under lång tid helt kom att saknas för de som tillhandahöll nätkapacitet.

Rikspolisstyrelsen uttalade i den tidigare nämnda skrivelsen till regeringen att varje operatörs system innehåller unika detaljlösningar vilket omöjliggör generella beskrivningar av hur en fullt ut fungerande verkställighet skall genomföras och att de generella föreskrifter som PTS då hade meddelat aldrig ensamma skulle kunna ligga till grund för en fungerande verkställighet. Därmed kan Riks-

polisstyrelsen sägas ha anslutit sig till den slutsats som regeringen tidigare kom fram till i lagstiftningsärendet, nämligen att individuellt avpassade tillståndsvillkor skulle utfärdas. Enligt uppgift som numera har lämnats till oss skulle detta också har varit PTS uppfattning.

Numera gäller inte de tillståndsvillkor som tidigare beslutades med stöd av telelagen. I stället gäller anpassningsskyldigheten fullt ut för de operatörer som bedriver sådan verksamhet som omfattas av bestämmelsen i lagen om elektronisk kommunikation. Skulle skyldigheten bli allt för betungande framför allt när det gäller ekonomiska aspekter, kan den enskilde operatören enligt 6 kap. 19 § fjärde stycket LEK och 36 § förordningen om elektronisk kommunikation begära undantag från kravet på hur verksamheten skall bedrivas enligt 6 kap. 19 § första stycket LEK. Det har såvitt bekant aldrig skett. Enligt samma bestämmelse har PTS också möjlighet att meddela verkställighetsföreskrifter. Några sådana föreskrifter har inte utfärdats.

Vi föreslog nyss att anpassningsskyldigheten skall omfatta samtliga de verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. RB eller tjänster inom ett sådant nät. Med en sådan reglering behöver det finnas möjlighet till undantag från skyldigheten. Frågan blir alltså vilken karaktär sådana undantag skall ha.

Den tekniska utvecklingen går fort. De tekniska förhållandena hos varje operatör är i många avseenden unika. I dag kan det sägas finnas en än högre grad av variation hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar jämfört med för tio år sedan då anpassningsskyldigheten infördes i telelagen. Detta ställer krav på differentierade lösningar vad gäller anpassningen i detalj. Den bedömning som regeringen gjorde tidigare har blivit bekräftad i den praktiska tillämpningen, nämligen att anpassningsskyldigheten i sig och särskilt undantag från denna inte lämpar sig att närmare beskriva i generella föreskrifter eller villkor av generell karaktär. Det kan leda till en osäkerhet såväl hos operatörerna som hos de brottsutredande myndigheterna om anpassningsskyldighetens innebörd och omfattning och därmed också till bristande effektivitet. Det skall också sägas att den grova brottsligheten enligt Rikspolisstyrelsen är uppmärksam på gränserna för de brottsutredande myndigheternas operativa möjligheter, dvs. generella föreskrifter om undantag från anpassningsskyldigheten, men även offentliga undantagsbeslut i enskilda fall, ger de kriminella personerna en bra uppfattning om vilka operatörer och vilka kom-

munikationsformer som är lämpliga att använda för deras verksamhet. Till detta kommer särskilt att operatörerna har påtalat för oss vikten av en tydlig, förutsebar reglering av anpassningsskyldigheten.

Vi föreslår mot den bakgrunden att undantagen från skyldigheten att bedriva verksamheten så att tvångsmedelsbesluten kan verkställas och så att verkställandet inte röjs skall kunna meddelas enbart i enskilda fall och alltså inte i form av generella föreskrifter. Undantag bör kunna ges generellt från anpassningsskyldigheten eller med avseende på vissa anpassningsåtgärder.

Vilken myndighet skall meddela undantagen?

Frågan blir då vilken myndighet som skall meddela beslut om undantag för en enskild operatör. Det finns för närvarande två myndigheter som har delar av den sakkunskap som behövs och sådana arbetsuppgifter som kan motivera att de tilldelas den uppgiften. Den ena är PTS och den andra är Rikspolisstyrelsen. Bestämmelsen om anpassningsskyldighet knyter starkt an till frågan om verkställighet av tvångsmedel. Bestämmelsen har en sådan väsentlig betydelse för möjligheterna att verkställa de aktuella tvångsmedelsbesluten och därigenom samhällets förmåga att utreda allvarlig brottslighet, att de telepolitiska målen inte kan sättas före de kriminalpolitiska vid en tillämpning. Utgångspunkten måste i stället vara att samtliga de meddelanden som omfattas av tvångsmedlen också i praktiken skall vara möjliga att avlyssna respektive övervaka eftersom systemen är anpassade fullt ut.

Vad som också talar för att välja Rikspolisstyrelsen är att styrelsen enligt egen utsago genom sina kontakter med bl.a. operatörerna har en ingående kunskap om tekniska verkställighetsfrågor samt om hur systemen generellt ser ut hos de enskilda operatörerna. En sådan detaljkunskap saknas hos PTS.

Det finns också ytterligare starka skäl för att välja Rikspolisstyrelsen som den myndighet som skall göra prövningen av undantag. Rikspolisstyrelsen konstaterade i sin tidigare nämnda skrivelse att PTS handläggningsformer skulle behöva förändras betydligt för att få arbetet effektivt. Vi instämmer i att PTS handläggning av villkorsärendena inte har fungerat tillfredsställande och varit, som det framstår, lågt prioriterat med bl.a. mycket långa handläggningstider som följd. Tidsutdräkten har varit till allvarligt men för de brottsutredande myndigheterna. Samtidigt kan det konstateras att en pri-

oritering hos PTS av frågor av brottsbekämpande karaktär kan verka främmande jämfört med myndighetens roll i övrigt.

Sammantaget gör vi därför bedömningen att det är mest lämpligt att Rikspolisstyrelsen meddelar undantag från anpassningsskyldigheten i de enskilda fallen. Uppgiften blir ett naturligt inslag i den övriga verksamheten. Eventuella ”målkonflikter” i verksamheten som bottnar i det förhållandet att effektiv verkställighet av tvångsmedel kan ge budgetmässiga fördelar för de brottsutredande myndigheterna, kan undvikas genom intern arbetsfördelning inom styrelsen. Vi föreställer oss att det på det sättet kommer att fattas snabba beslut där stor hänsyn tas till förutsättningarna hos den enskilde operatören. Det är i det sammanhanget viktigt att framhålla att Rikspolisstyrelsens beslut blir av den karaktären att de kan överklagas hos allmän förvaltningsdomstol. Prövningstillstånd skall krävas vid överklagande till kammarrätten (jfr exempelvis 8 kap. 19 § LEK).

Vilken avvägning bör ske?

I samband med att anpassningsskyldigheten infördes uttalade regeringen i propositionen (prop. 1995/96:180 s. 37) bl.a. att tillståndsmyndigheten vid prövningen av frågan om villkor skulle väga nyttan av en viss anpassning mot kostnaden för denna och att myndigheten skulle ta särskild hänsyn till om det rör sig om ändringar i ett befintligt system eller krav som ställs vid byte till ny teknik. Avvägningar i dessa avseenden, mellan nyttan eller effektiviteten och kostnader blir de mest centrala även vid bedömningar om den enskilde operatören skall meddelas undantag från anpassningsskyldigheten i något avseende enligt vårt förslag.

I fråga om bedömningar av nyttan eller effektiviteten är det viktigt att beakta det samhällsintresse som ligger i att kunna upprätthålla en beredskap för att ha möjlighet att snabbt verkställa beslut om tvångsmedlen. Nyttan eller effektiviteten av en anpassning kan svårligen mätas i beräknade antal verkställigheter hos en enskild operatör. I vissa fall kan en enskild lyckad verkställighet innebära en oerhört stor samhällelig nytta i olika avseenden. Som vi tidigare angett har bestämmelserna om anpassningsskyldighet en sådan väsentlig betydelse för möjligheterna att verkställa de aktuella tvångsmedelsbesluten, och därigenom samhällets förmåga att utreda allvarlig brottslighet, att de telepolitiska målen inte kan sättas före de kriminalpolitiska vid en tillämpning. Utgångspunkten för

en prövning och en avvägning mot kostnadsaspekten måste istället vara att samtliga de meddelanden som omfattas av tvångsmedlen också i praktiken skall vara möjliga att avlyssna respektive övervaka eftersom systemen är anpassade fullt ut.

Ett beslut om undantag skall kunna villkoras så att det endast gäller under vissa förutsättningar. Förändrade förutsättningar vad gäller t.ex. teknik och verksamhetens omfattning, art eller kundkrets kan genom sådana villkor medföra att undantaget inte längre gäller. Den tidsperiod under vilket ett undantag skall gälla måste givetvis också avpassas utifrån omständigheterna i det enskilda fallet, såsom nyttan av åtgärden, kostnaderna och teknikutvecklingen.

Med hänsyn till vårt förslag om hur anpassningsskyldigheten skall vara utformad och mot bakgrund av att det är fråga om undantagsbeslut efter ansökan i enskilda fall, får det åligga den enskilde operatören att i ansökan och det eventuella överklagandet visa och i övrigt utveckla vilka kostnader som operatören menar blir för höga för att anpassningsskyldigheten skall kunna fullgöras.

6.6.5 Kostnadsansvaret för åtgärderna

Förslag: Operatörerna skall även fortsättningsvis stå för de kostnader som krävs.

Kostnadsansvaret i nuläget

I den principiella frågan vem som skall stå för kostnaderna för åtgärderna resonerade regeringen på följande sätt i samband med att anpassningsskyldigheten infördes (prop. 1995/96:180 s. 31 ff.).

> Kostnaderna kan bäras av polisen eller av teleoperatörerna. En tredje möjlighet är att, utan att belasta polisens anslag, betala kostnaderna via statsbudgeten. Det finns också den möjligheten att fördela kostnaderna mellan teleoperatörerna och polisen/staten. Ytterligare en möjlighet är att de teleoperatörer som redan har erhållit tillstånd att driva televerksamhet kompenseras för de kostnader som de initialt kommer att drabbas av till följd av den nya regleringen medan de vid byte till ny teknik liksom också nya operatörer får stå kostnaderna fullt ut.
>
> ----

En allmän utgångspunkt när det gäller kostnader för den brottsutredande verksamheten är att polisen skall svara för dessa. Detta argument har också framförts av de remissinstanser som är kritiska mot promemorians förslag. Den brottsutredande verksamheten är enligt dessa remissinstanser en statlig angelägenhet som bör bekostas av samhällsmedborgarna som kollektiv och inte av teleabonnenterna. Frågan är då om detta argument bör hindra andra lösningar.

Det finns en rad verksamhetsområden där samhället som förutsättning för att få idka näring kräver att vissa samhälleliga intressen beaktas. I promemorian lämnas flera exempel på detta. Det tydligaste exemplet är kanske arbetsgivares skyldighet att uppbära, redovisa och inbetala preliminär skatt för anställda. Som ett annat exempel kan nämnas miljöfarlig verksamhet där företagen måste investera stora summor för att minimera de skador som kan följa med verksamheten. Denna jämförelse har kritiserats under remissbehandlingen. Enligt regeringens mening finns det emellertid ingen avgörande principiell skillnad mellan dessa förpliktelser och en förpliktelse att på egen bekostnad anpassa telesystemen så att möjligheterna till hemlig teleavlyssning och hemlig teleövervakning bibehålls. Inte heller kan hemlig teleavlyssning och hemlig teleövervakning sägas inta någon särställning i nu berört avseende endast på den grunden att det rör sig om brottsutredande verksamhet. Det finns redan i dag lagstadgade skyldigheter för företag att vidta vissa åtgärder för att underlätta den brottsutredande verksamheten. Bankernas uppgiftsskyldighet enligt lagen (1993:768) om åtgärder mot penningtvätt är ett exempel på detta. Om man ålägger teleoperatörerna skyldighet att på egen bekostnad anpassa sina system innebär det inte att man därigenom ålägger dem ett ansvar för brottsutredande verksamhet i egentlig mening. Teleoperatörernas skyldighet att anpassa sina system så att möjligheterna till verkställighet av beslut om hemlig teleavlyssning och hemlig teleövervakning bibehålls är nämligen helt fristående från pågående förundersökningar och aktualiseras utan hänsyn till hur och när polisen sedan kan komma att verkställa ett beslut om hemlig teleavlyssning eller hemlig teleövervakning. Från principiell synpunkt skiljer sig denna situation enligt regeringens mening inte från bestämmelserna om bankernas skyldighet att lämna uppgifter enligt lagen om åtgärder mot penningtvätt.

Regeringen fortsatte resonemanget med att ange vissa skäl för att låta operatörerna stå kostnaderna för åtgärderna enligt följande.

> Det finns andra skäl som skulle kunna åberopas för att teleoperatörerna inte bör svara för de nu aktuella kostnaderna. En finansiering över statsbudgeten kan sägas stå i överensstämmelse med vad som anges i förarbetena till telelagen om bestridande av vissa kostnader, särskilt de kostnader som uppkommer för totalförsvarets behov av telekommunikationer och handikappades behov av särskilda teletjänster (prop. 1992/93:200 s. 115 ff. och s. 288 ff.).
>
> De tillståndspliktiga teleoperatörerna kan emellertid inom andra områden genom villkor åläggas att driva televerksamheten med beaktande av vissa centrala samhälleliga intressen som medför kostnader för operatörerna utan att de får ekonomisk kompensation från staten för detta. Ett exempel på en sådan funktion är skyldigheten att tillhandahålla teletjänster i glesbygd. Tillståndshavare, som genom ett villkor blir ålagd att ansluta även inte lönsamma kunder, skall som regel göra detta utan särskild ersättning från staten (a. prop. s. 113). Såsom påpekats under remissbehandlingen bör det framhållas att det hittills endast är Telia som har ålagts en sådan skyldighet och att Telia kan kompensera sig för detta via samtrafikavgifter. Denna ordning med avgiftsfinansiering i stället för finansiering via statsbudgeten är enligt regeringen ett exempel som skulle kunna tjäna som förebild för en reglering på tvångsmedelsområdet. Lika viktigt som goda kommunikationer i glesbygd är det att bibehålla möjligheten att bekämpa den allvarligare brottsligheten.

Regeringen diskuterade också kostnadseffektiviteten i de olika lösningarna enligt följande.

> En betydelsefull omständighet att beakta vid valet mellan olika lösningar är kostnadseffektiviteten. Den som drabbas av kostnaderna har naturligtvis ett starkt incitament att söka hålla kostnaderna nere. I promemorian görs den bedömningen att teleoperatörerna här har ett försteg framför polisen. RRV delar i sitt remissvar den bedömningen och anför att det finns skäl att tro att ett eget finansieringsansvar hos operatörerna skulle leda till mer kostnadseffektiva lösningar. Till

skillnad från polisen kan teleoperatörerna påverka priserna vid upphandlingen av de hård- och mjukvaror som krävs. Teleoperatörerna har en förhandlingsposition som bör kunna leda till att största kostnadseffektivitet uppnås i detta hänseende. Teknik som möjliggör hemlig teleavlyssning och hemlig teleövervakning kommer nämligen att omfattas av förhandlingar om helt nya telesystem och om ny teknik i befintliga system som en mycket liten del i ett större paket. Teleoperatörerna kan också i stor utsträckning välja mellan olika tillverkare. Ifrågavarande kostnader kan hållas nere om de aktuella funktionerna beaktas på ett så tidigt stadium som möjligt. En internationellt godtagen standard på området, som EU-samarbetet kan leda till, skulle också bidra till lägre merkostnader. Polisen däremot är utlämnad till den teleoperatör vars system skall göras avlyssningsbart, vilket innebär att någon upphandlingssituation i egentlig mening inte uppstår. Vidare skulle polisen i dessa fall ha stora svårigheter att bedöma rimligheten i de ekonomiska krav som teleoperatörerna skulle rikta mot dem. Den kompetens som erfordras för en sådan bedömning skulle inte utan betydande svårigheter kunna inhämtas och upprätthållas hos polisen. Det saknas också i denna situation ett eget ekonomiskt incitament för operatörerna att förhandla fram ett så fördelaktigt pris som möjligt. Dessutom skulle polisen komma in i bilden, om man ser till kostnadseffektiviteten, på ett alldeles för sent stadium. Det är heller inte önskvärt att polisen skulle behöva förhandla med operatörerna varje gång ny teknik tas i anspråk. Det som för polisen skulle kunna bli ansenliga kostnader bör alltså kunna begränsas av operatörerna, särskilt om det ligger i operatörernas intresse att hålla nere kostnaderna.

Det nu sagda har under remissbehandlingen kritiserats av flera teleoperatörer. Det anförs från flera håll att promemorians förslag riskerar att öka kostnaderna och att det finns risk för att polisen överkonsumerar en till synes gratis nyttighet. Om polisen har ett kostnadsansvar skulle detta avhålla polisen från att begära alltför vidlyftiga tekniska lösningar till stora kostnader. Ett kostnadsansvar för polisen skulle i enlighet med detta resonemang medföra att endast de anpassningar av telesystemen vidtogs som de brottsutredande myndigheterna fann mest angelägna. De brottsutredande myndigheterna skulle helt enkelt på vanligt sätt prioritera

olika verksamheter och lägga sina pengar där de bedömdes göra bäst nytta.

Regeringen kan inte ansluta sig till detta resonemang. Den ordning som vi redovisat i det föregående innebär inte att polisen fritt får bestämma vilka anpassningar som skall göras i telesystemen. Enligt vårt förslag skall de grundläggande kraven på teleoperatörerna framgå av lag och den närmare innebörden av teleoperatörernas skyldigheter formuleras genom tillståndsvillkor och föreskrifter, som bestäms av Post- och telestyrelsen efter samråd med teleoperatören, Riksåklagaren och Rikspolisstyrelsen. Med en sådan reglering kan de telepolitiska målen balanseras mot de kriminalpolitiska och därigenom elimineras också risken för att polisen skulle kunna utverka t.ex. orealistiskt dyra anpassningar av vissa telesystem.

Regeringen avslutade sitt resonemang med följande överväganden.

En reglering som innebär att teleoperatörerna skall bära kostnaderna för anpassningarna av telesystemen måste vägas mot de konsekvenser som en sådan reglering innebär. Det är av stor betydelse att de telepolitiska målen, såsom de kommit till uttryck i bl.a. telelagen, kan uppnås och vidmakthållas. Detta framhålls också med skärpa från flera remissinstanser. Det är därför mycket viktigt att de tillståndspliktiga operatörerna ges möjlighet att verka på telemarknaden på rimliga villkor för att på så sätt tillgodose samhällets behov av goda och billiga telekommunikationer. Mot denna bakgrund är det olyckligt om teleoperatörerna skulle bli ekonomiskt ansvariga för alltför stora samhälleliga åtaganden. Samtidigt är televerksamheten så speciell att det är oundvikligt att ett relativt stort samhällsansvar måste följa med verksamheten. Självklart kan det innebära en stor ekonomisk belastning för en operatör att stå kostnaderna för anpassningen av det egna telesystemet. Det torde emellertid inte vara fråga om summor som inte kan bäras av en teleoperatör. Detta gäller särskilt som de teleoperatörer vars verksamhet inte är av betydande omfattning är undantagna från skyldigheten att anpassa systemen. De telepolitiska målen bör enligt regeringens mening kunna uppnås och vidmakthållas även med en sådan reglering.

Till bilden hör att det i en framtid kan komma att finnas ett stort antal teleoperatörer som erbjuder teletjänster och att ett kostnadsansvar för polisen skulle bli mycket betungande. Det är inte realistiskt att förvänta sig att polisen kan tillföras motsvarande ekonomiska resurser, särskilt mot bakgrund av det ytterst ansträngda statsfinansiella läget. Det är av samma skäl inte ett alternativ att sköta finansieringen över statsbudgeten. Till en del gäller detta även ett system där kostnaderna delas upp mellan operatörerna och de brottsutredande myndigheterna. Förutom den administration som erfordras för ett sådant system blir det dessutom alltid i sista hand fråga om skönsmässiga bedömningar.

Alternativet till ett kostnadsansvar för teleoperatörerna är i praktiken att tvångsmedlen på teleområdet får ges upp. Även om ett kostnadsansvar för de tillståndspliktiga teleoperatörerna i någon mån skulle verka hämmande för televerksamheten som helhet är det enligt regeringens mening inte rimligt att oinskränkt vidmakthålla de telepolitiska målen på bekostnad av statens möjligheter att bekämpa grova brott och upprätthålla rikets inre och yttre säkerhet.

I de fall samtrafik förekommer kan nätoperatören kompensera sig via samtrafikavgifterna. I övrigt innebär en ordning där teleoperatörerna står för alla kostnader för anpassningar, drift och underhåll av telesystemen i slutändan att abonnenterna får betala. Detta är inte orimligt med tanke på att det är abonnenterna som drar nytta av att telesystemen hela tiden moderniseras och förbättras, vilket ju i sin tur är orsaken till att polisens möjligheter att bedriva hemlig teleavlyssning och hemlig teleövervakning har försämrats. En sådan ordning kan därför förefalla mer rättvis än att låta skattebetalarna betala, oavsett i vilken utsträckning de använder sig av moderna telekommunikationer.

Det finns också utrymme för teleoperatörerna och polisen att dela på kostnaderna i vissa fall. Skulle det t.ex. visa sig att ett system i och för sig är avlyssningsbart men att, om teleoperatören installerade ny teknik, detta skulle innebära lägre kostnader för polisen vid varje enskild verkställighet bör det finnas utrymme för förhandlingar mellan teleoperatören och polisen. Detsamma bör kunna gälla om det finns möjlighet för teleoperatörerna att välja olika lösningar när ett system skall anpassas och en av lösningarna innebär högre kostnader för teleoperatören men lägre kostnader för varje

enskild verkställighet. Även i sådana fall bör förhandlingar om hur kostnaderna skall bäras vara till gagn både för teleoperatörerna och polisen. Det finns enligt regeringens mening inte anledning att, som Telia föreslagit i sitt remissvar, lagreglera denna möjlighet. En sådan bestämmelse skulle nämligen endast kunna slå fast att polisen och teleoperatörerna har frihet att förhandla i nu berört hänseende.

Några remissinstanser har uttalat farhågor för att anpassningskostnaderna kan leda till en snedvridning av konkurrensen. Europolitan hävdar att det föreligger en mycket stor risk för att kostnaderna kommer att bli olika för de olika operatörerna, vilket medför att konkurrensförutsättningarna blir olika. Telenordia anför att investeringarna förefaller vara av den karaktären att kostnaderna är relativt oberoende av antalet abonnenter. Följden härav är enligt deras mening att förslaget riskerar att snedvrida konkurrensen genom att kostnaderna per abonnent blir större för små operatörer. Konkurrensverket å sin sida har principiellt inget att erinra mot förslaget att teleoperatörerna skall svara för anpassningskostnaderna. Enligt verket är det emellertid från konkurrenssynpunkt väsentligt att - när statsmakterna ändrar spelreglerna för en marknad - de operatörer som redan erhållit tillstånd att verka på telemarknaden ges rimlig tid att anpassa sina system.

I fråga om sådana operatörer som ännu inte har fått tillstånd att bedriva televerksamhet anser regeringen i belysning av de överväganden vi redovisat i det föregående att det närmast är en självklarhet att den kostnad som uppkommer för att anpassa systemen för hemlig teleavlyssning och hemlig teleövervakning skall bäras av operatörerna.

Situationen är en annan för de operatörer som redan har tillstånd att bedriva televerksamhet och som påbörjade sin verksamhet under de förutsättningar som då gällde; ett kostnadsansvar för anpassning av de befintliga systemen kan sägas rubba dessa förutsättningar. Mot detta kan sägas att en förpliktelse för operatörer med tillstånd att bekosta anpassningar i befintliga system drabbar dem alla, även om kostnaderna av naturliga skäl inte blir lika tunga att bära för alla operatörer. Regeringen har anledning att utgå från att de aktuella operatörerna kan bära dessa kostnader om de ges en rimlig övergångstid och rimliga villkor för anpassningen.

Skall nuvarande ordning förändras?

Den nuvarande ordningen innebär alltså att operatörerna står för de kostnader för anpassning, drift och underhåll av systemen som krävs för att beslut om hemlig teleavlyssning och hemlig teleövervakning skall kunna verkställas. När skyldigheten infördes konstaterade regeringen att detta i sig inte innebär att operatörerna får ett ansvar för brottsutredande verksamhet och att det principiellt inte finns någon skillnad mellan den skyldigheten och andra förpliktelser eller samhälleliga intressen som åläggs respektive måste beaktas av enskilda för att få idka näring (prop. 1995/96:180 s. 32). Den slutsatsen har giltighet även i dag. Regeringen har dessutom nyligen i lagrådsremissen den 3 mars 2005 Kostnadsansvar för hemlig teleavlyssning m.m. uttalat att det inte finns någon principiell skillnad i det avseendet mellan anpassningsskyldigheten och det förhållandet att operatörerna inte får ersättning för verkställigheten av beslut om hemlig teleavlyssning, hemlig teleövervakning samt för utlämnande enligt lagen om elektronisk kommunikation.

Även om regeringens resonemang utgår från förhållandena enligt telelagen, instämmer vi även utifrån nuvarande förhållanden generellt i bedömningarna rörande kostnadseffektiviteten och i slutsatsen att det som för det allmänna skulle kunna bli ansenliga kostnader kan begränsas av operatörerna, särskilt som det ligger i operatörernas intresse att hålla kostnaderna nere. Operatörerna har nämnt för oss att även teknikutvecklingen, det allt mer omfattande internationella standardiseringsarbetet och det förhållandet att många av operatörerna har verksamhet i flera länder innebär att kostnaderna för anpassningsåtgärderna kan minska. Vi vill dock peka på att anpassningen av en verksamhet knappast kan anses fullgjord genom åtgärder som innebär att den punkt där verkställigheten sker, exempelvis en viss router, läggs i ett annat land än Sverige. Förutom de uppenbara svårigheter detta medför ur säkerhetsskyddslagens perspektiv skulle brottsutredande myndigheter sannolikt vara hänvisade till att ansöka om rättslig hjälp från det andra landets myndigheter varje gång ett tvångsmedelsbeslut skulle verkställas. Sådana ärenden förekommer utomlands redan i dag.

Liksom i det tidigare lagstiftningsärendet har operatörerna även till oss framfört den synpunkten att ett kostnadsansvar för operatörerna riskerar att öka kostnaderna eftersom det finns risk för att polisen överkonsumerar ”nyttigheten” genom att inte avhålla sig från att begära allt för vidlyftiga tekniska lösningar. Regeringen avfärdade tidigare det argumentet med att säga att den utformning

av anpassningsskyldigheten som föreslogs i propositionen utgjorde en sådan balans mellan telepolitiska och kriminalpolitiska mål att risken för att polisen skulle utverka orealistiskt dyra anpassningar eliminerades. Vi kan i den delen konstatera att det helt saknas konkreta uppgifter som skulle tyda på att det faktiskt har ställts sådana krav på anpassning från polisens sida. Ett tungt vägande skäl till att sådana fördyringar med största sannolikhet inte har uppkommit är att operatörerna kunnat upphandla utrustning som i stort följer internationell standard för sådana åtgärder. Det finns enligt uppgift en växande internationell marknad för dylik utrustning vilket gynnar priskonkurrens och utveckling av ny materiel. Vi ser bl.a. av det skälet i princip ingen risk för att operatörerna tappar förhandlingspositioner av betydelse mot leverantörer när dessa är medvetna om att operatörerna har vissa skyldigheter.

När anpassningsskyldigheten infördes uttalade regeringen att det inte fanns något underlag för en tillförlitlig beräkning av operatörernas kostnader i olika avseenden och att det var tveksamt om det skulle vara möjligt att få fram ett sådant underlag. Dessutom menade regeringen att det inte fanns några möjligheter att förutse vilka ekonomiska konsekvenser som skulle följa med den tekniska utvecklingen på området men att det fanns anledning att anta att kostnaderna skulle uppgå till avsevärda belopp.

Givetvis är kostnaderna för anpassning olika stora för operatörerna och i de olika verksamheterna hos respektive operatör. Vi har uppfattat att kostnadsansvaret tillsammans med oklarheter om hur långt anpassningsskyldigheten sträcker sig i vissa avseenden är de främsta orsakerna till att anpassningsarbetet hos operatörerna i många fall är lågt prioriterat. Vi har i sammanhanget till och med hört uttalas från en av de största operatörerna, att det som skall göras gratis läggs det inga resurser på. Med hänsyn till att det är fråga om en lagreglerad skyldighet får denna inställning betraktas som anmärkningsvärd.

Genom det förslag som vi presenterar skapas en så tydlig reglering som möjligt av anpassningsskyldighetens gränser. Säkert skulle det motstånd som kan tänkas finnas hos operatörerna minska om det då samtidigt bestämdes att staten skulle stå för anpassningskostnaderna helt eller delvis. Som framgick konstaterade regeringen tidigare att en operatörs verksamhet är så speciell att det är oundvikligt att ett relativt stort samhällsansvar följer med verksamheten men också att anpassningsåtgärderna inte torde kräva sådana summor att de inte kan bäras av operatörerna och i slutändan av abonnenterna.

Även om förutsättningarna har förändrats något sedan tillståndsplikten avskaffades, ansluter vi oss även i övrigt till de överväganden som regeringen redovisade och kan då bl.a. konstatera att, på liknande sätt som i det tidigare lagstiftningsärendet, har inte heller vi fått några summor presenterade av de operatörer vi har haft kontakt med om hur mycket anpassningskostnaderna faktiskt uppgår till i dagsläget. Det kan då vara på sin plats att framhålla att anpassningskostnaderna kan vara svåra att skilja från andra kostnader för operatörerna.

Av flera skäl kan det vara svårt att närmare beräkna kostnaderna för anpassningen. När det finns tekniska standarder för verkställighet baseras brottsutredande myndigheters krav på dessa standarder. Funktionaliteten för verkställighet blir då ofta en integrerad del i den standardfunktionalitet som leverantören tillhandahåller. Priset för verkställighetsfunktionen är en del av totalpriset och det är inte självklart att priset går att skilja från totalpriset. Det går inte heller alltid att med säkerhet säga hur den anpassningsskyldiges kostnad påverkas om leverantören tvingas ta bort den funktionalitet som gäller verkställigheten. En anpassning genomförs vanligen genom att den anpassningsskyldige implementerar funktionaliteten. Uppgraderingar av funktionaliteten för verkställighet brukar därefter följa ”releaserna” för den övriga funktionaliteten. Den anpassningsskyldiges personalkostnad för implementering och uppgradering av verkställighetsfunktionen är ofta svår att uppskatta. När det däremot gäller krav som inte baseras på tekniska standarder är kostnaderna lättare att identifiera.

I frånvaro av uppgifter från operatörerna om hur stora belopp det är fråga om, är kostnaderna näst intill omöjliga för oss att uppskatta. I likhet med vad som nämndes i den tidigare propositionen (prop. 1995/95:180 s. 31) har det även till oss framförts att ett rimligt belopp för anpassning hos de största operatörerna skulle kunna uppgå till ett engångsbelopp om något tiotal miljoner kronor med en tillkommande årlig driftkostnad på någon miljon kronor. De investeringar som krävs är dock i allt väsenligt redan gjorda, med undantag för den anpassningsskyldighet för vissa operatörer som tillkommer med vårt förslag. Det kan också sägas att kostnaderna för anpassningsåtgärderna i förhållande till den totala ”kommunikationsvolymen” måste numera vara klart lägre jämfört med när operatörernas kostnadsansvar infördes.

Mot bakgrund av detta verkar det inte sannolikt att kostnaderna skulle överstiga vad berörda operatörer rimligen kan bära, särskilt som det sker en ”pulvrisering” så att kostnaderna tas igen genom

intäkter från abonnenterna. Den avgiftshöjning som på detta sätt kan komma att drabba respektive abonnent kan antas bli marginell och är försvarlig med hänsyn till den nytta som den genom våra förslag förbättrade möjligheten till brottsbekämpning för med sig.

Sammantaget har vi inte kommit fram till någon annan lösning i kostnadsfrågan vad gäller anpassningsskyldigheten än den nu gällande. Regeringen har nu senast i den nämnda lagrådsremissen rörande visst kostnadsansvar uttalat att elektronisk kommunikation har utvecklats till en så betydelsefull del i samhället att ett stort samhällsansvar måste följa med verksamheten. Genom förslaget om att operatörerna även skall få stå för bl.a. verkställighetskostnader vid hemlig teleavlyssning har regeringen markerat principen om operatörernas ansvar och i slutänden abonnenternas ansvar för kostnader på området. Vad som har förekommit under de år anpassningsskyldigheten har funnits ger alltså inte anledning för oss att föreslå en annan ordning. Även i fortsättningen skall operatörerna stå för de kostnader som uppkommer. Som framgår av det tidigare sagda har kostnadsfrågan givetvis betydelse vid bedömningen av om en enskild operatör skall medges undantag i något avseende.

6.6.6 Vad bör ske om anpassningsskyldigheten inte efterlevs?

Förslag: Rikspolisstyrelsen skall få meddela de förelägganden som behövs för att anpassningsskyldigheten skall efterlevas. Förelägganden skall kunna överklagas hos allmän förvaltningsdomstol. Prövningstillstånd skall krävas vid överklagande till kammarrätten.

Rikspolisstyrelsen skall kunna förena förelägganden med vite. Frågor om utdömande av vite skall prövas av allmän förvaltningsdomstol på ansökan av Rikspolisstyrelsen.

Regleringen i telelagen och lagen om elektronisk kommunikation

Anpassningsskyldigheten fanns tidigare föreskriven i 17 § telelagen. Enligt 15 § andra stycket den lagen skulle ett tillstånd att driva televerksamhet förenas med villkor om skyldighet för tillståndshavaren att på visst sätt fullgöra anpassningsskyldigheten. Ett tillstånd skulle enligt 12 § den lagen återkallas om verksamheten bedrevs i strid med bl.a. tillståndsvillkor om avvikelsen inte kunde anses vara av

mindre betydelse. Tillsynsmyndigheten (PTS) fick för övrigt också meddela de förelägganden och förbud som behövdes för efterlevnaden av bl.a. tillståndsvillkor. Förelägganden och förbud fick förenas med vite (60 och 63 §§ telelagen).

Det har sagts tidigare att lagen om elektronisk kommunikation i nu aktuellt avseende inte bygger på en tillståndsplikt utan i stället på en anmälningsplikt avseende verksamheterna. Liksom telelagen innehåller lagen om elektronisk kommunikation regler om tillsyn och om tillsynsmyndighetens befogenheter i den verksamheten. Enligt 7 kap. 1 § LEK skall tillsynsmyndigheten (PTS) ha tillsyn över efterlevnaden av lagen. En möjlighet som PTS har är enligt 7 kap. 3 § LEK att förelägga den som driver verksamhet att lämna myndigheten de upplysningar och handlingar som behövs för kontroll av efterlevnaden av de allmänna skyldigheter som finns för operatören. Ett sådant föreläggande får förenas med vite.

Skulle PTS finna skäl att misstänka att den som bedriver verksamhet enligt lagen om elektronisk kommunikation inte efterlever lagen, skall myndigheten enligt 7 kap. 4 § LEK underrätta operatören om det och samtidigt ge denne möjlighet att yttra sig. Skulle det förfarandet inte leda till rättelse, får PTS enligt 7 kap. 5 § LEK också meddela de förelägganden och förbud som krävs för att rättelse skall ske. Sådana förelägganden eller förbud får förenas med vite. Följs inte föreläggandet, får PTS bl.a. besluta att den som har åsidosatt en skyldighet helt eller delvis skall upphöra med verksamheten.

Bestämmelser om viten

När en förvaltningsmyndighet riktar ett åläggande eller förbud mot viss person, kan myndigheten ofta samtidigt hota med att personen kan komma att få betala ett visst penningbelopp (vite) om myndighetens beslut inte följs (se om viten Strömberg, Allmän förvaltningsrätt, 22 uppl., s. 136 ff.).

Vitets storlek bestäms redan i beslutet. Detta hot betecknas ofta vitesföreläggande, vilket är en term som också används för att beteckna myndighetens beslut i dess helhet.

I stort sett gäller samma regler för materiellt vite, som används när en myndighet avgör ett ärende (t.ex. för att framtvinga rivning av en byggnad eller reparation av en bostadslägenhet) som för förfarandevite, som används under handläggningen av ett ärende (t.ex.

för att framtvinga personlig inställelse eller ingivande av vissa handlingar).

En myndighet anses i princip inte ha rätt att förelägga vite utan uttryckligt författningsstöd (prop. 1984/85:96 s. 19). De viktigaste allmänna bestämmelserna om vite finns i lagen (1985:206) om viten (viteslagen), som gäller viten som enligt lag eller annan författning får föreläggas av myndigheter. Lagen skall inte tillämpas i den mån annat följer av vad som är särskilt föreskrivet (1 § viteslagen). Myndigheternas rätt att förelägga vite finns föreskriven i en mängd bestämmelser, som kan avvika från viteslagens föreskrifter. Allmänna bestämmelser om viten finns också i brottsbalken (25 kap. och 35 kap.) och i bötesverkställighetslagen (1979:189).

Ett vitesföreläggande skall vara riktat till en eller flera namngivna fysiska eller juridiska personer (adressater). Adressat kan bara den vara som kan antas ha faktisk och rättslig möjlighet att efterkomma föreläggandet. Vid ingripanden mot juridiska personer kan myndigheten välja mellan att rikta föreläggandet mot den juridiska personen som sådan eller mot en eller flera företrädare, t.ex. styrelseledamöter i ett aktiebolag. En kombination av båda metoderna är också möjlig (2 § viteslagen).

Om föreläggandet innebär en skyldighet för adressaten att vidta en viss åtgärd, skall det av föreläggandet framgå vid vilken tidpunkt eller inom vilken tidsfrist åtgärden skall vidtas. Tiden kan komma att förskjutas genom ett överklagande. Även om överklagandet lämnas utan bifall, är det vanligt att det då meddelas en ändrad tidsbestämmelse, vilket innebär att klaganden i vart fall vinner lite tid. När vite har förelagts får nytt vite mot adressaten i samma sak inte föreläggas förrän det tidigare föreläggandet har vunnit laga kraft. Ett vitesföreläggande skall delges adressaten (2 § viteslagen). Där blir delgivningslagen (1970:428) tillämplig.

När vite föreläggs skall det fastställas till det belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som har förenats med vite. Vitet skall fastställas till ett bestämt belopp, om det inte är fråga om ett s.k. löpande vite, alltså att vitet bestäms till ett visst belopp för varje tidsperiod av viss längd under vilken föreläggandet inte har följts eller för varje gång adressaten underlåter att fullgöra en återkommande förpliktelse. Om vite föreläggs flera personer gemensamt skall ett särskilt belopp fastställas för var och en av dem (3 och 4 §§ viteslagen).

Om ett vitesföreläggande inte har fullgjorts i tid, kallas det att vitet har försuttits. Då uppkommer frågan om vitets utdömande. För att ett försuttet vite skall kunna dömas ut måste föreläggandet bl.a. ha vunnit laga kraft. Som huvudregel gäller att frågor om utdömande av viten prövas av länsrätt på ansökan av den myndighet som har utfärdat föreläggandet. Målet om vitets utdömande kommer då att utformas som ett tvåpartsförfarande. Prövningstillstånd krävs vid överklagande till kammarrätten. Frågor om utdömande av viten som har förelagts en part eller någon annan till fullgörande av en skyldighet i en rättegång eller i annat motsvarande förfarande prövas dock utan särskild ansökan av den myndighet som har utfärdat föreläggandet. I vissa särskilda fall prövar tingsrätt frågor om utdömande av vite (6 och 7 §§ viteslagen).

I ett mål om vites utdömande har länsrätten att pröva om vitesföreläggandet är lagligen grundat men däremot inte om det har varit behövligt eller lämpligt. Rätten har vidare att konstatera om föreläggandet har åtlytts eller inte, och i det senare fallet om den enskilde kan åberopa något giltigt skäl för sin underlåtenhet. Om rätten finner att vitet är försuttet, skall den i princip döma ut just det belopp som har fastställts i föreläggandet. Någon ”straffmätning” i vanlig mening skall alltså inte ske. Finns det särskilda skäl, t.ex. så att den enskilde har fullgjort föreläggandet efter tidsfristens utgång, får vitet dock jämkas. Om flera viten döms ut samtidigt läggs de ihop utan någon maximigräns. Vitet skall inte dömas ut om ändamålet med vitet har förfallit. Vite bortfaller, om talan om att det skall dömas ut inte har delgetts adressaten inom två år från det att förutsättningarna för att väcka sådan talan uppkom (9 § viteslagen).

Enligt bötesverkställighetslagen gäller lagens bestämmelser om böter också vite. Det innebär bl.a. att vite kan förvandlas till fängelse (1 och 15 §§ den lagen). Även i brottsbalken finns bestämmelser som gäller viten. Där föreskrivs bl.a. att utdömda viten tillfaller staten (25 kap. 7 och 9 §§ BrB). I 35 kap. BrB finns regler om bortfallande av påföljd. I kapitlet finns en bestämmelse som gäller viten (7 §).

Vitesföreläggande vid bristande åtgärder

Som framgår har det sedan anpassningsskyldigheten infördes bl.a. funnits möjlighet för PTS att meddela de förelägganden som har behövts för att skyldigheten skall efterlevas. Även om arbetet med

anpassningsåtgärder har varit lågt prioriterat hos många operatörer, har den frågan, såvitt bekant, aldrig ens aktualiserats.

För efterlevnaden av anpassningsskyldigheten är det nödvändigt att det även i fortsättningen finns ett påtryckningsmedel på operatörerna att vidta de åtgärder som krävs. Vi kom tidigare fram till att Rikspolisstyrelsen i enskilda fall skulle få meddela vissa undantag från anpassningsskyldigheten. Rikspolisstyrelsen skall också få meddela de förelägganden som behövs för efterlevnaden av skyldigheten att bedriva verksamheten så att tvångsmedelsbesluten kan verkställas och så att verkställandet inte röjs samt för att göra informationen tillgänglig så att den enkelt kan tas om hand. Vi utgår från att den möjligheten sällan kommer att aktualiseras och ser i dagsläget inget behov av att göra bestämmelsen vidare än så. Föreläggandet, som måste kunna förenas med vite, skall kunna överklagas hos allmän förvaltningsdomstol, där prövningstillstånd skall krävas vid överklagande till kammarrätten.

Det är nödvändigt att räkna med att det uppstår ett behov av att i några fall döma ut vitet. Som huvudregel gäller enligt 6 § viteslagen att frågor om utdömande av vite prövas av länsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet. Den ordningen skall gälla även för de förelägganden som Rikspolisstyrelsen meddelar enligt vårt förslag.

6.6.7 Sekretessfrågor

Förslag: Sekretesslagen skall kompletteras med en bestämmelse som anger att sekretess gäller för uppgift som hänför sig till Rikspolisstyrelsens prövning av frågor om undantag och förelägganden, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

Sekretess skall gälla i sådana ärenden hos Rikspolisstyrelsen även för uppgifter om den enskildes affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs.

Det är ett faktum att särskilt den grova brottsligheten vidtar en mängd åtgärder för att skydda den olagliga verksamheten. Bl.a. innebär det att man noggrant följer de brottsutredande myndigheternas förmåga att genomföra olika brottsbekämpande åtgärder. Får de kriminella personerna tillgång till uppgifter om begränsningar i avlyssnings- och övervakningsmöjligheterna hos de enskilda opera-

törerna, kan det få allvarliga konsekvenser för myndigheternas arbete, eftersom det kan resultera i att personer väljer operatörer och kommunikationsformer där tvångsmedel inte kan verkställas.

Vid Rikspolisstyrelsens prövning av frågor om undantag och förelägganden kan det förekomma uppgifter som avslöjar begränsningar i möjligheten för de brottsutredande myndigheterna att verkställa tvångsmedelsbesluten. Det är därför nödvändigt att det finns en möjlighet att hålla de uppgifterna hemliga.

I 5 kap. 1 § sekretesslagen finns bestämmelser till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Enligt första stycket fjärde punkten i den paragrafen gäller sekretess för uppgift som hänför sig till åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet för att förebygga, uppdaga, utreda eller beivra brott. Sekretessen gäller om följden av att uppgifterna lämnas ut kan antas bli att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Om uppgifterna hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott gäller sekretess enligt 5 kap. 1 § andra stycket sekretesslagen, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas (se även sekretessen till skydd för rikets säkerhet i 2 kap. 2 § sekretesslagen).

För att det inte skall råda någon tvekan i fråga om sekretess för de uppgifter som förekommer i ärendena hos Rikspolisstyrelsen om undantag och förelägganden, föreslår vi att 5 kap. 1 § första stycket sekretesslagen skall kompletteras med en ny punkt som anger att sekretess skall gälla för uppgift som hänför sig till prövningen av sådana frågor, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

Bestämmelsen i 5 kap 1 § sekretesslagen gäller också vid förvaltningsdomstolarnas handläggning. Enligt 12 kap. 4 § första stycket sekretesslagen gäller som huvudregel att sekretess för uppgifter i ett ärende hos domstol upphör att gälla om uppgifterna tas in i domstolens beslut. Domstolen har dock möjlighet enligt andra stycket i den nämnda bestämmelsen att förordna att sekretessen skall bestå i olika delar (se SvJT 1992 s. 542 och SOU 1998:46 s. 93).

I samband med att en operatör ansöker hos Rikspolisstyrelsen om undantag från anpassningsskyldigheten ligger det i sakens natur

att operatören måste lämna uppgifter om sina tekniska system och liknande. Sådana uppgifter kan vara mycket avslöjande i förhållande till framför allt konkurrenter på marknaden. Sådana uppgifter kan även förekomma i ärenden om förelägganden. Sekretess måste därför också gälla för uppgift om den enskildes affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs.

Enligt 8 kap. 6 § sekretesslagen gäller sådan sekretess i den utsträckning regeringen föreskriver det vid bl.a. statlig myndighets tillståndsgivning och tillsyn, vilket får anses träffa det nu aktuella fallet. Enligt 2 § sekretessförordningen (1980:657) finns en bilaga till den förordningen med uppräknade verksamheter i vilka sekretess gäller. Den bilagan skall kompletteras med de nu aktuella ärendena. Sekretessen skall även kunna omfatta Rikspolisstyrelsens beslut i sådant ärende.

Vad däremot gäller förvaltningsdomstolarnas handläggning finns i dag enligt 12 kap. 2 § sekretesslagen den begränsningen att sekretess enligt 8 kap. 6 § sekretesslagen inte gäller hos domstolen i liknande fall. Det saknas tillräckliga skäl att göra undantag från den principiella ordningen enligt sekretesslagen vad gäller sekretessen för uppgifter om enskildas affärs- eller driftförhållanden vid handläggning hos förvaltningsdomstolarna. Samma ordning torde gälla även i dag vid överklagande till förvaltningsdomstol t.ex. av beslut fattade av PTS enligt 6 kap. 19 § fjärde stycket LEK (se 8 kap. 19 § LEK, jfr även 9 kap. 8 § sekretesslagen och bilagan till sekretessförordningen, nr 109).

6.6.8 Tid för att genomföra förslagen

Förslag: De operatörer vars verksamhet, till skillnad från i dag, kommer att omfattas av anpassningsskyldigheten skall få en viss tid för att vidta de åtgärder som krävs. Tiden från det att den ändrade lagstiftningen utfärdas till dess att den träder i kraft skall dock inte vara längre än ett år.

När anpassningsskyldighet infördes i telelagen föreskrevs en generell övergångstid om ett år från lagens ikraftträdande för de operatörer som tidigare hade beviljats tillstånd. För de operatörer som beviljades tillstånd efter lagens ikraftträdande gällde anpassningsskyldigheten omedelbart.

Vårt förslag innebär att vissa operatörer, vars verksamhet inte tidigare har omfattats av anpassningsskyldigheten, kommer att behöva anpassa sina system så att tvångsmedelsbesluten kan verkställas. Det är rimligt att operatörerna får en viss tid på sig för anpassningsåtgärder från det att bestämmelserna utfärdas till dess att de träder i kraft. Det finns inte anledning att bestämma den tiden till längre än ett år. Det får anses vara en tillräcklig tid för operatörerna att förbereda och vidta erforderliga åtgärder alternativt att förbereda en ansökan till Rikspolisstyrelsen om undantag från skyldigheten i något avseende.

7 Bevarandeskyldigheten

7.1 Sammanfattande bedömning

– Många europeiska länder har en nationell lagstiftning som innebär en skyldighet för operatörer att bevara trafikuppgifter under viss tid för brottsbekämpande ändamål. Inom EU pågår för närvarande ett arbete i frågan om bevarandeskyldighet. Detta gör att det inte är meningsfullt att vi lämnar något förslag på nationell lagstiftning i den delen. Däremot finns anledning att beskriva det behov som de brottsutredande myndigheterna har av att få tillgång till trafikuppgifter i förundersökningar och av de ”operativa” problem som de nuvarande reglerna på området skapar.
– Vid utredningar av grövre brott används trafikuppgifter på något sätt i nästan samtliga fall. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt.
– Det är av synnerlig vikt för det brottsutredande arbetet att trafikuppgifter finns tillgängliga under längre tid tillbaka än tolv månader.
– Frånvaron av en bevarandeskyldighet för operatörerna medför många gånger stora problem för de brottsutredande myndigheterna med att få tillgång till de uppgifter som behövs. Det förhållandet leder i sin tur till allvarliga problem med effektiviteten i förundersökningsarbetet. Särskilt som det rör sig om utredningar av grövre brottslighet kan konsekvenserna från brottsbekämpningssynpunkt i längden bli oacceptabla.

7.2 Inriktningen på vårt arbete

Bedömning: Många europeiska länder har en nationell lagstiftning som innebär en skyldighet för operatörer att bevara trafikuppgifter under viss tid för brottsbekämpande ändamål. Inom EU pågår för närvarande ett arbete i frågan om bevarandeskyldighet. Detta gör att det inte är meningsfullt att vi lämnar något förslag på nationell lagstiftning i den delen. Däremot finns anledning att beskriva det behov som de brottsutredande myndigheterna har av att få tillgång till trafikuppgifter i förundersökningar och av de ”operativa” problem som de nuvarande reglerna på området skapar.

Frågan om bevarande av trafikuppgifter nämns särskilt i våra direktiv (Dir. 2003:145, se *bilaga 2*). Vi skall överväga om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna. Regeringen anger också några utgångspunkter för våra överväganden, nämligen att inte fler uppgifter bevaras för brottsbekämpande ändamål eller under längre tid än vad som är nödvändigt och att personuppgifter som bevaras inte skall användas för något annat ändamål än brottsbekämpning.

Sedan regeringen beslutade om våra tilläggsdirektiv i november 2003 drabbades Europa av det största terroristattentatet sedan andra världskriget. Attentaten i Madrid den 11 mars 2004 tog omkring 200 personers liv och skadade över 1 500. Det är den främsta bakgrunden till att ett rambeslut håller på att arbetas fram inom EU. Det är ett svar på den uppmaning som EU:s stats- och regeringschefer gav vid toppmötet i Bryssel i mars 2004 i deklarationen om kampen mot terrorism. I deklarationen uppmanas rådet att med prioritet undersöka möjligheten till åtgärder för att fastställa regler för bevarande av trafikuppgifter hos operatörer som tillhandahåller tele- eller Internettjänster. Förslaget till rambeslut är lagt av Frankrike, Irland, Storbritannien och Sverige gemensamt och håller för närvarande på att förhandlas. Målet är att rambeslutet skall antas i juni 2005. Syftet med förslaget är att trafikuppgifter skall bevaras av operatörer under viss tid så att uppgifterna finns tillgängliga för de brottsbekämpande myndigheterna i det internationella straffrättsliga samarbetet.

I dagsläget finns alltså inget färdigt förslag till rambeslut. Nyligen har dessutom EG-kommissionen meddelat att man anser att saken till viss del är en s.k. förstapelarfråga där kommissionen och inte medlemsstaterna har initiativrätt. Kommissionen har uttalat att arbetet med frågorna är angeläget och att avsikten är att arbeta fram

ett förslag till direktiv som tar upp i princip samma frågor. Kommissionen har också försäkrat medlemsstaterna att den har samma målsättning med arbetet, nämligen att skapa förutsättningar för en effektiv bekämpning av terrorism och organiserad brottslighet. Det nuvarande ordförandeskapet har aviserat att förhandlingarna om rambeslutet fortsätter tills vidare och att ett nytt ställningstagande får göras om och när kommissionen presenterar ett förslag.

Många europeiska länder har en nationell lagstiftning som innebär en skyldighet för operatörer att bevara trafikuppgifter under viss tid för brottsbekämpande ändamål. Vi kan konstatera att förutsättningarna för oss att arbeta fram ett ändamålsenligt förslag i frågan om bevarandeskyldighet har förändrats kraftigt sedan regeringen beslutade om våra direktiv. Vi har bedömt att det med hänsyn till de oklarheter som finns i dagsläget i fråga om resultatet av det arbete som nu bedrivs inom EU inte är meningsfullt att vi lämnar något förslag på nationell lagstiftning rörande bevarandeskyldigheten. Vid överväganden i frågan om och i så fall hur en eventuell bestämmelse som ålägger operatörerna en bevarandeskyldighet rörande trafikuppgifter skall utformas, är det självfallet så att faktorer som de brottsutredande myndigheternas behov av uppgifterna, problemen med den nuvarande ordningen samt integritets- och kostnadsaspekter får stor betydelse. Med hänsyn till frågans aktualitet och stora betydelse har vi dock funnit det angeläget att beskriva det behov som de brottsutredande myndigheterna har av att få tillgång till trafikuppgifter i förundersökningar och av de ”operativa” problem som de nuvarande reglerna på området skapar.

7.3 Bestämmelserna om bevarande av trafikuppgifter

7.3.1 Telelagen

I propositionen Ändringar i telelagen m.m. (prop. 1998/99:92 s. 29 f.) redogjorde regeringen för innehållet i det s.k. teledataskyddsdirektivet (97/66/EG) och nämnde bl.a. att syftet med direktivet var att genom en harmonisering av medlemsstaternas bestämmelser om behandling av personuppgifter säkerställa en likvärdig nivå på integritetsskyddet och en fri rörlighet inom gemenskapen för personuppgifter inom telekommunikationsområdet och för teleutrustning och teletjänster. I direktivet fanns angivet att uppgifter

om abonnenter och användare som teleoperatören behandlar för att koppla upp samtal skulle utplånas eller åtminstone avidentifieras vid samtalets slut. Nödvändiga uppgifter för fakturering av abonnenter och för betalning av samtrafikuppgifter fick dock behandlas under preskriptionstiden. I propositionen föreslog regeringen, mot bakgrund av innehållet i direktivet, vissa ändringar i telelagen.

Ändringarna trädde i kraft den 1 juli 1999 och innebar bl.a. följande.

Enligt huvudregeln i 49 § första stycket telelagen skulle uppgifter som gällde ett särskilt telemeddelande utplånas eller avidentifieras av teleoperatören vid samtalets slut eller när meddelandet nått mottagaren. Den skyldigheten gällde, enligt paragrafens andra stycke, inte för behandling av sådana uppgifter som var nödvändiga för fakturering av abonnenter och betalning av samtrafikavgifter till dess fordringen var betald eller preskriberad. Om abonnenten hade gett sitt samtycke fick sådana uppgifter behandlas för marknadsföring av teletjänster i den egna verksamheten.

Ytterligare undantag från kravet i 49 § första stycket telelagen om omedelbart utplånande eller avidentifiering av uppgifterna fanns i 50 § telelagen och gällde för det första meddelanden som omfattades av beslut om hemlig teleavlyssning eller hemlig teleövervakning. För det andra fanns undantag från det s.k. lagringsförbudet i den utsträckning det var nödvändigt för att förhindra eller avslöja obehörig användning av telenätet. Det tredje undantaget i 50 § telelagen avsåg det fallet att abonnenten begärde att störande samtal skulle spåras. Uppgifter som identifierade den uppringande abonnenten kunde då lagras och hållas tillgängliga av teleoperatören.

För de brottsutredande myndigheternas del förutsatte ett utlämnande av uppgifter med stöd av bestämmelserna i 47 § telelagen (motsvarande 6 kap. 22 § LEK) att uppgifterna fanns tillgängliga hos teleoperatörerna när de begärdes utlämnade. I det remissförfarande som föregick regeringens proposition om förändringarna i telelagen ansåg Rikspolisstyrelsen att skyldigheten att utplåna eller avidentifiera de historiska uppgifterna, i vart fall då teleavlyssning m.m. inte förevarit, skulle hindra polisens möjligheter att utreda brott. I propositionen 1998/99:92 (s. 33) nämnde regeringen att den hade viss förståelse för Rikspolisstyrelsens bedömning men konstaterade att det inte var möjligt att införa vidare undantag från skyldigheten att utplåna uppgifter. Mot bakgrund av Rikspolisstyrelsens remisskritik uttalade regeringen dock att det kunde finnas anledning att i samarbetet inom Europeiska unionens tredje pelare

återkomma till frågan om utnyttjande av teleuppgifter i brottsbekämpningssammanhang. Vid behandlingen i riksdagen anförde Trafikutskottet (1998/99:TU12 s. 7) att utskottet förutsatte att regeringen inom ramen för EU-samarbetet verkar för en effektiv brottsbekämpning och för riksdagen redovisar de resultat som därvid uppnås.

I en skrivelse till regeringen under hösten 2002 om tillgång till telekommunikation för polisens brottsutredande verksamhet anförde Rikspolisstyrelsen bl.a. följande om bevarande av trafikuppgifter (dnr Ju2002/7018/PO och RÄS-002-3668/02).

> Reglerna som möjliggör för Polisen att erhålla uppgifter från teleoperatörer är mycket betydelsefulla för det brottsutredande arbetet. Det är en olycklig ordning att uppgifterna samlas in för exempelvis faktureringsändamål samtidigt som lagstiftaren förutsätter att uppgifterna även kan komma att bearbetas i det brottsutredande arbetet. Polisens möjligheter att få tillgång till uppgifterna bör säkerställas genom nationell lagstiftning som ålägger teleoperatörer att spara uppgifter i syfte att de skall användas i det brottsutredande arbetet. Polisens bedömning är att uppgifterna måste sparas minst 12 månader.

I 22 § teleförordningen (1997:399) föreskrev regeringen vilka uppgifter rörande ett särskilt telemeddelande som fick behandlas till dess att fordran var betald eller preskriberad, om uppgifterna varit nödvändiga för fakturering av en abonnent eller för betalning av samtrafikavgifter (49 § andra stycket telelagen). Det rörde abonnentens teleadress, den anropades teleadress, samtalets art, samtalets starttidpunkt och längd eller den överförda datamängden, datum för samtalsanropet, det totala antalet enheter som skall debiteras för en redovisningsperiod, andra uppgifter om eller i samband med betalningen, såsom förskottsbetalning, avbetalning, betalningspåminnelse och avstängning samt typ av utrustning och abonnentutrustningens nummer eller annan identifikation.

7.3.2 Lagen om elektronisk kommunikation

Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elek-

tronisk kommunikation (direktivet om integritet och elektronisk kommunikation) trädde i kraft den 31 juli 2002 och ersatte det tidigare nämnda teledataskyddsdirektivet. Enligt regeringen genomfördes direktivet om integritet och elektronisk kommunikation huvudsakligen i lagen om elektronisk kommunikation (prop. 2002/03:110 s. 69 f. och 248). Artikel 6 i direktivet om integritet och elektronisk kommunikation reglerar behandlingen av trafikuppgifter. En trafikuppgift är enligt 6 kap. 1 § LEK alla uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. Någon motsvarande definition fanns inte i telelagen. Enligt förarbetena till lagen om elektronisk kommunikation (prop. 2002/03:110 s. 389 f.) torde begreppet trafikuppgifter avse samma slag av uppgifter som avsågs i 49 § telelagen, där det talades om uppgifter som angår ett särskilt telemeddelande.

Enligt artikel 15 i det angivna direktivet får medlemsstaterna genom lagstiftning begränsa omfattningen av de rättigheter och skyldigheter som anges i bl.a. artikel 6. Det får ske bl.a. när en sådan begränsning är nödvändig i ett demokratiskt samhälle samt lämplig och proportionell för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning och avslöjande av brott och åtal för brott. Begränsning kan bl.a. innebära att uppgifter får bevaras under en begränsad period.

Bestämmelserna om bevarande av trafikuppgifter finns främst i 6 kap. 5, 6 och 8 §§ LEK och motsvaras i huvudsak av 49 och 50 §§ telelagen. Huvudregeln framgår av 6 kap. 5 § LEK och innebär att trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver anmälningspliktig verksamhet, skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande.

Liksom telelagen tillåter lagen om elektronisk kommunikation 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 operatören också behandla uppgifterna för att bl.a. marknadsföra elektroniska kommunikationstjänster, om den abonnent eller användare som uppgifterna avser har samtyckt till det. Bestämmelsen i 6 kap. 6 § LEK kompletteras av 35 § förordningen om elektronisk kommunikation,

som anger att PTS får meddela närmare föreskrifter om vilka uppgifter som får behandlas enligt den bestämmelsen i lagen om elektronisk kommunikation (jfr 22 § den upphävda teleförordningen). PTS har hittills inte meddelat några sådana föreskrifter.

Undantag från reglerna om behandling av trafikuppgifter finns i 6 kap. 8 § LEK. Det rör för det första det 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 undantaget i bestämmelsen gäller i den utsträckning trafikuppgifterna är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Enligt regeringen (prop. 2002/03:110 s. 392) får uppgifterna inte sparas enligt det undantaget längre än vad som är nödvändigt för syftet. Längre än ett år bör enligt regeringen inte godtas, om det inte föreligger särskild anledning, som att tvist har uppkommit eller förundersökning inletts i ett särskilt fall. I propositionen nämnde regeringen också att den nu aktuella paragrafen 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 skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande finns i 6 kap. 13 § LEK. Operatören får enligt bestämmelsen temporärt åsidosätta skydd mot nummerpresentation för att spåra störande samtal. Det kan vara fråga om hotfulla samtal eller rena okynnessamtal. Om en abonnent begär spårning av sådana samtal, får operatören lagra sådana uppgifter som identifierar den anropande abonnenten och hålla dem tillgängliga för abonnenten på begäran.

I lagen om elektronisk kommunikation finns en särskild reglering om behandling av lokaliseringsuppgifter. Med lokaliseringsuppgifter avses uppgifter som visar den geografiska positionen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst (prop. 2002/03:110 s 260). En lokaliseringsuppgift kan vara en trafikuppgift och följer i så fall de regler som gäller för trafikuppgifter. Den behöver emellertid inte vara det (jfr 6 kap. 9 § LEK). Till lokaliseringsuppgifter som samtidigt är trafikuppgifter hör framför allt information om i vilken cell i ett cellulärt uppbyggt

mobilkommunikationssystem, som t.ex. GSM, som en användare befinner sig vid ett visst tillfälle när utrustningen utnyttjas.

Sådana lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter får enligt huvudregeln i 6 kap. 9 § LEK behandlas endast sedan de har avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen. Behandlingen får enligt bestämmelsen endast ske i den utsträckning och under den tid som krävs för tillhandahållandet av en tjänst där uppgifterna behövs.

7.4 Förslaget till rambeslut

I det internationella samarbetet mellan brottsbekämpande myndigheter har frågan om bevarande av trafikuppgifter varit en mycket angelägen fråga under ett flertal år. Vi nämnde nyss att Sverige tillsammans med Frankrike, Irland och Storbritannien inom ramen för EU-samarbetet har presenterat ett förslag till rambeslut för rådet. Rambeslutet är inte färdigförhandlat ännu. Syftet med förslaget är att trafikuppgifter skall bevaras av operatörer under viss tid så att uppgifterna finns tillgängliga för de brottsbekämpande myndigheterna i det internationella straffrättsliga samarbetet. Förslaget till rambeslut behandlar frågorna om att uppgifter skall bevaras, vilka uppgifter som skall bevaras och hur länge det skall ske. I det sammanhanget tas inte upp kostnadsansvaret och förutsättningarna för de brottsbekämpande myndigheterna att få del av uppgifterna, alltså de nationella reglerna motsvarande exempelvis hemlig teleövervakning i rättegångsbalken.

När det gäller frågan om vilka uppgifter som skall bevaras, omfattar rambeslutet uppgifter som genereras hos operatören, även om operatören själv inte har behov av att spara uppgifterna för eget ändamål. Det brukar sägas att uppgifterna svarar på frågorna VEM kommunicerade med vem, NÄR startade och slutade kommunikationen, VAR befann sig de som kommunicerade med varandra och HUR skedde kommunikationen. Uppgifter som inte genereras hos operatören faller utanför rambeslutets tillämpningsområde. Detsamma gäller de åtgärder som anses behövas för allmän säkerhet, försvar och nationell säkerhet.

Förslaget till rambeslut hade följande innehåll efter förhandlingar som ägde rum i mars 2005.

Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

Article 1

Scope and Aim

1. This Framework Decision aims to facilitate judicial cooperation in criminal matters by approximating Member States' legislation on the retention of [communication] data, generated or processed by providers of a publicly available electronic communications service or a public communications network, for the purpose of investigation, detection and prosecution of criminal offences.

2. This Framework Decision shall apply to all means of electronic communication, including in particular:

(a) Telephony excluding Short Message Services, Electronic Media Services and Multi Media Messaging Services.

(b) Short Message Services, Electronic Media Services and Multi Media Messaging Services provided as part of any telephony service.

(c) Internet Protocols including Email, Voice over Internet Protocols, world wide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice over broadband and subsets of Internet Protocols numbers - network address translation data.

3. This Framework Decision shall not apply to the content of exchanged communications, including information consulted using an electronic communications network.

3. This Framework Decision is without prejudice to:

– national rules on retention of [communication] data processed or generated by providers of a publicly available electronic communications service or a public communications network for the purpose of prevention of crime;

– the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;

– activities concerning public security, defence and national security (i.e. State security);

[– national rules relating to the retention of [communication] data types which are not held by communication service providers for business purposes.]

Article 2

Definitions

1. For the purpose of (…) this Framework Decision, the term '[communication] data' in this Framework Decision means:

(a) traffic data and location data as set out in Article 2 of the Directive 2002/58/EC (…).

(b) User data (…) relating to any user of a publicly available electronic communications service, for private or business purposes, without the user necessarily having subscribed to the service.

(c) Subscriber data (…) relating to any legal or natural person subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

2. [Communication] data to be retained for the purpose set out in Article 1 include:

(a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.

(b) Data necessary to identify the routing and destination of a communication.

(c) Data necessary to identify the time and date and duration of a communication.

(d) Data necessary to identify the telecommunication.

(e) Data necessary to identify the communication device or what purports to be the device.

(f) Data necessary to identify the location at the start and throughout the duration of the communication.

Article 3

Retention of [communication] data

1. Each Member State shall take the necessary measures to ensure that, for the purpose of providing judicial cooperation in criminal matters, communication data as referred to in Article 2(2) when generated or processed by providers of a publicly available electronic communications service or a public communications network is retained in accordance with the provisions of this Framework Decision.

2. Member States shall take appropriate measures for the purpose of the technical implementation of paragraph 1.

Article 4

Time periods for retention of [communication] data

1. Each Member State shall take the necessary measures to ensure that [communication] data referred to in Article 3

shall be retained for a period of 12 months following its generation. Relating to subscriber data, this period shall run from the end of the subscription.

2. By derogation from paragraph 1, any Member State may provide for retention of [communication] data referred to in Article 3 for longer periods of up to 36 months in accordance with national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

3. By derogation from paragraph 1, any Member State may provide for retention of [communication] data referred to in Article 3 for shorter periods of at least 6 months in relation to means of communication identified in Article 1(a)(b) and (c) should the Member State not find acceptable, following national procedural or consultative processes, the retention periods set out in paragraph 1 of this Article.

4. Any Member State which decides to make use of paragraph 3 must notify the Council and the Commission of the retention periods provided for with specification of the [communication] data concerned. Any such derogation must be reviewed annually.

Article 5

Data Security

Each Member State shall ensure that, regarding [communication] data retained under this Framework Decision, providers subject to the retention obligation must comply, as a minimum, to the following data security principles:

(a) the retained data shall be of the same quality as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or accidental loss, alteration,

unauthorised disclosure or access, and against all other unlawful forms of processing;

(c) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved;

Article 6

Access to retained [communication] data

Each Member State shall ensure that access to [communication] data retained under this Framework Decision shall be subject, as a minimum, to the following rules and shall establish judicial remedies in line with the provisions of Chapter III on 'Judicial remedies, liability and sanctions' of Directive 95/46/EC:

(a) data shall be accessed for specified, explicit and legitimate purposes by competent authorities on a case by case basis in accordance with national law and not further processed in a way incompatible with those purposes;

(a bis) the process to be followed in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law;

(a ter) (...)

(b) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are accessed. Data shall be processed fairly and lawfully;

(c) data accessed by competent authorities shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected or for which they are further processed;

(d) the confidentiality and integrity of the data shall be ensured;

(e) data accessed shall be accurate and, every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

Article 7

Request to access [communication] data for the purpose of judicial co-operation in criminal matters

A request made by a Member State to another Member State, for access to [communication] data referred to in Article 2, shall be made and responded to in accordance with the applicable instruments on judicial co-operation in criminal matters (...) . The requested Member State may make its consent to such a request for access to data subject to any conditions which would have to be observed in a similar national case.

Article 8

Implementation

Member States shall take the necessary measures to comply with this Framework Decision by […..June 2007] within two years following the date of adoption.

By the same date Member States shall transmit the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. The General Secretariat of the Council shall communicate to the Member States the information received pursuant to this Article.

The Commission shall by [….1st January 2008] submit a report to the Council assessing the extent to which the Member States have taken necessary measures in order to comply with this Framework Decision.

Article 9

Entry into force

This Framework Decision shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.

7.5 Behovet av tillgång till trafikuppgifter i brottsutredningar

7.5.1 Inledning

Teknikutvecklingen medför att elektroniska kommunikationstjänster utnyttjas i en ständigt ökande utsträckning och blir ett allt viktigare hjälpmedel för kontakt mellan personer. Mobiltelefoni och Internet är exempel på kommunikation som blir allt viktigare och som används i allt större omfattning. I våra direktiv nämns särskilt den snabba teknikutvecklingen och att målsättningen för vårt arbete bör vara att skapa en enhetlig reglering som kan stå sig över tiden. Vi berör också teknikutvecklingen på flera ställen i betänkandet och nämner bl.a. den s.k. konvergensen, alltså den utveckling som innebär att olika infrastrukturer och tekniker för överföring av kommunikation och tjänster, som telefoni, datakommunikation, radio och TV, ”smälter samman”. IP-telefoni är ett exempel på kommunikationsform som kan sudda ut gränserna mellan traditionell telefoni och datakommunikation.

I samband med att vi har behandlat olika frågor i betänkandet har vi nämnt trafikuppgifter i olika former. Sådana uppgifter genereras hos operatörerna varje gång någon t.ex. ringer ett telefonsamtal, kopplar upp sig på Internet eller slår på en mobiltelefon. Enligt Säkerhetspolisen är det svårt att sätta enhetliga benämningar på ”de tekniska identiteterna”, eftersom de benämns olika i olika elektroniska kommunikationsnät. Däremot är det möjligt att beskriva vilka typer av uppgifter som behövs i det brottsutredande arbetet. De olika typerna av uppgifter genereras hos operatörerna oavsett t.ex. abonnemang eller faktureringssätt. I samband med att behovet av uppgifterna diskuteras kan följande typer av trafikuppgifter anges

(de exempel som ges vid varje typ av uppgift utgör ingen komplett uppräkning).

- ✓ **”Avsändande” identitet**, som telefon- eller mobiltelefonnummer, IMSI- eller IMEI-nummer, e-postadress, IP-nummer och mac-adress
- ✓ **”Mottagande” identitet**, som telefon- eller mobiltelefonnummer, IMSI- eller IMEI-nummer, e-postadress, IP-nummer och mac-adress
- ✓ **Datum och klockslag**
- ✓ **Lokalisering**, som uppgift om var avsändande och mottagande identitet fanns i det elektroniska kommunikationsnätet under en viss tidsperiod
- ✓ **Andra uppgifter**, som antalet ringsignaler, färdväg, storlek och typ av tjänst

När vi tar upp behovet av trafikuppgifter gör vi det utifrån ett generellt synsätt. Vi går därmed inte in på frågor om värderingar av uppgifter vid användning av olika typer av kommunikationssätt, t.ex. vilka typer uppgifter som i allmänhet kan sägas vara mest eller minst viktiga i brottsutredningar av olika karaktär.

7.5.2 Hur stort är behovet?

Bedömning: Vid utredningar av grövre brott används trafikuppgifter på något sätt i nästan samtliga fall. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt.

Fram till den 1 oktober 2004 gav tvångsmedlet hemlig teleövervakning enligt 27 kap. 19 § RB de brottsutredande myndigheterna trafikuppgifter enbart om de telemeddelanden som förmedlades från beslutet om åtgärden, alltså framtida uppgifter eller s.k. realtidsuppgifter. Vi redogjorde i avsnitt 2.9 för innehållet i regeringens senaste redovisning till riksdagen av tillämpningen av bestämmelserna om hemlig teleövervakning (Skr. 2004/05:36). Där framgår bl.a. att tillstånd till tvångsmedlet lämnades i 645 fall under år 2003, att merparten av tillstånden (450 stycken) avsåg grovt narkotikabrott eller grov narkotikasmuggling samt att de övriga fallen avsåg främst mord, grovt rån, människorov, grov mordbrand, allmänfar-

lig ödeläggelse, grov penningförfalskning, grov våldtäkt, människohandel för sexuella ändamål, grovt barnpornografibrott, grov varusmuggling, grov stöld, grovt bedrägeri, grovt penninghäleri, grov urkundsförfalskning, grovt bokföringsbrott, grovt skattebrott och grovt miljöbrott. Av skrivelsen framgår också att övervakningen hade betydelse för förundersökningen i knappt 46 procent av fallen, att övervakningen avbröts i förtid i 14 procent av fallen på grund av t.ex. tekniska problem, att den misstänkte reste utomlands, abonnemanget upphörde eller den misstänkte greps för annat brott, att tillslag endast kunde ske mot andra än den misstänkte i sex procent av fallen och att förundersökningen lades ned i knappt 34 procent av fallen på grund av att brott inte kunde styrkas.

Regeringen konstaterade i den nämnda skrivelsen att bl.a. hemlig teleövervakning har visat sig vara ett värdefullt hjälpmedel i kampen mot den grova, många gånger organiserade brottsligheten. I avsnitt 9.4.1 lämnas uppgifter om den typen av brottslighet.

De trafikuppgifter som de brottsutredande myndigheterna får vid användning av hemlig teleövervakning är desamma som myndigheterna har möjlighet att erhålla genom utlämnande från operatörerna enligt lagen om elektronisk kommunikation (6 kap. 22 § första stycket 3 LEK). Utlämnande enligt den lagen omfattar uppgifter som angår ett särskilt elektroniskt meddelande, dvs. enbart historiska uppgifter, alltså uppgifter som har genererats hos operatörerna i tiden före det att begäran om utlämnande görs. Förutsättningarna för att begära ut sådana uppgifter har behandlats i bl.a. avsnitt 4.2.1. Som också har framhållits tidigare (avsnitt 4.2.5) saknas statistik på i hur många fall som de brottsutredande myndigheterna i dag begär uppgifter från operatörerna enligt lagen om elektronisk kommunikation. Vid hemlig teleavlyssning och hemlig teleövervakning sköter Säkerhetspolisen all kontakt med operatörerna medan begäran enligt lagen om elektronisk kommunikation görs ”mer formlöst” av framför allt Säkerhetspolisen, Rikskriminalpolisen, varje polismyndighet och Tullverket för sig. Enligt en grov uppskattning gjord av Säkerhetspolisen kan det röra sig om drygt 4000 fall årligen. Enligt Säkerhetspolisen kan den generella slutsatsen dras att historiska trafikuppgifter har en större betydelse i brottsutredningsverksamheten än vad realtidsuppgifter har.

Som vi påpekade i avsnitt 4.3.5 är trafikuppgifter ofta den absolut viktigaste nyckeln till att utredningar rörande grövre brott kan föras framåt. Uppgifterna används i princip i *varje* utredning rörande grova brott, som mord, människorov, grovt rån, grov mord-

brand, 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 brottslighet av den karaktär som nu är aktuell inleds ofta med en kontroll av de trafikuppgifter 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 trafikuppgifterna, 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, är det alltså 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 trafikuppgifter 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.

I detta sammanhang är det också viktigt att framhålla den brottslighet som på olika sätt kan relateras till Internet. Enligt uppgift från Rikskriminalpolisen är avsaknad av en skäligen misstänkt person 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 trafikuppgifter, eftersom de uppgifterna är det enda som kan länka samman målsäganden och gärningsmannen. Möjligheten att vara anonym på Internet ger också problem vid 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 annat verktyg vid brottsligheten. Det har också då mycket stor betydelse att de brottsutredande 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. Vi tar upp det sistnämnda problemet även i avsnitt 9 rörande hemlig dataavläsning.

Här måste också framhållas att den kraftigt ökade användningen av kryptering gör att betydelsen av tillgång till trafikuppgifter i brottsutredningarna ökar, eftersom krypteringen i princip innebär att de brottsutredande myndigheterna inte kommer åt innehållet i meddelanden genom hemlig teleavlyssning.

Det skall tilläggas att tillgång till trafikuppgifter från operatörer i Sverige är helt nödvändig även i det internationella samarbetet mellan brottsutredande myndigheter.

Det är vår bestämda uppfattning att betydelsen av att de brottsutredande myndigheterna får tillgång till trafikuppgifter i förundersökningar särskilt rörande grövre brott inte kan överskattas. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Det gäller inte minst i de fall där det från början saknas en skäligen misstänkt person.

Det måste poängteras att betydelsen av tillgången till trafikuppgifterna omöjligen kan uppskattas utifrån hur många gånger som uppgifterna åberopas som bevisning i domstol. I de fall tillgången till uppgifterna för utredningen framåt leder de oftast till att andra omständigheter och annan bevisning kan fås fram, vilka i sin tur ligger till grund för åtalet och åberopas i rättegången. Med andra ord är det ofta så att uppgifterna ”sätter polisen på spåret” och utgör en grundläggande vägledning för det vidare utredningsarbetet. Den information som kan fås från beslagtagna datorer eller mobiltelefoner är inte på minsta vis tillräcklig för att täcka det stora behov som finns hos de brottsutredande myndigheterna av tillgång till uppgifterna i nästan samtliga utredningar av grövre brott.

7.5.3 Hur gamla trafikuppgifter finns det behov av?

Bedömning: Det är av synnerlig vikt för det brottsutredande arbetet att trafikuppgifter finns tillgängliga under längre tid tillbaka än tolv månader.

Som framgick tidigare finns det ingen statistik på i hur många fall årligen som de brottsutredande myndigheterna begär uppgifter från operatörerna enligt lagen om elektronisk kommunikation. Det saknas därmed också statistik på hur gamla uppgifter som efterfrågas av myndigheterna. Från någon operatör har vi hört sägas att drygt 80 procent av förfrågningarna skulle röra uppgifter som inte är äldre än tre månader, att omkring tio procent skulle röra uppgifter som är mellan tre och sex månader gamla och att inte ens en procent av fallen skulle röra uppgifter som är mer än tolv månader gamla.

Det finns i och för sig ingen anledning att ifrågasätta att ärendena grovt fördelat sig på det sättet rörande en viss operatör under en viss tid. Frånsett att uppgifterna härrör från tiden före den senaste ändringen av bestämmelserna om hemlig teleövervakning, dvs. den 1 oktober 2004, belyser detta enligt Säkerhetspolisen av flera skäl inte det behov som finns hos de brottsutredande myndigheterna. Sedan skyldigheten att utplåna eller avidentifiera trafikuppgifter infördes i telelagen för snart sex år sedan har myndigheterna fått en bild av hur respektive operatör tillämpar bestämmelserna och vilka kostnader för de brottsutredande myndigheterna som är förbundna med ett utfående av uppgifterna. Varje operatör avgör själv om och i så fall hur länge trafikuppgifterna skall sparas för att de t.ex. ”krävs för abonnentfakturering” (6 kap. 6 § LEK) eller ”är nödvändiga för att förhindra eller avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst” (6 kap. 8 § 3 LEK). Variationen i bedömningarna hos operatörerna är enligt Säkerhetspolisen stor. Det gäller särskilt på Internetområdet, där den tid som operatörerna sparar uppgifter varierar kraftigt, från ett omedelbart raderande till ett bevarande under flera år. Möjligheten att få tillgång till de historiska uppgifterna i brottsutredningar blir ofta beroende av vilken operatör som är aktuell i det enskilda fallet.

Enligt Säkerhetspolisen begärs trafikuppgifter som är äldre än tre månader ofta inte ut, trots att det finns ett behov i förundersökningarna. Det beror på att det är välkänt hos de brottsutredande myndigheterna att vissa uppgifter inte tillhandahålls av den opera-

tör som är aktuell. Exempelvis utplånar vissa operatörer uppgifter om det inkommande samtalet omedelbart efter att samtalet har avslutats, vilket enligt Säkerhetspolisen innebär att en gärningsman kan känna sig relativt trygg när han exempelvis ringer till ett tilltänkt brottsoffer. Då kan det också nämnas att de större operatörerna har utformat blanketter som används av de brottsutredande myndigheterna när uppgifter begärs ut. På blanketterna anges hur gamla uppgifter som över huvud taget kan tillhandahållas av operatören. Trots detta har det i särskilda utredningar visat sig att äldre uppgifter har funnits tillgängliga hos den enskilde operatören.

Vilka trafikuppgifter som begärs från operatörerna är enligt Säkerhetspolisen också en kostnadsfråga. I några ärenden där äldre trafikuppgifter har efterfrågats, har operatören begärt två miljoner kronor per telefonnummer för att lämna ut uppgifterna. De brottsutredande myndigheterna har inte haft resurser att betala den ersättningen.

Säkerhetspolisen har också lagt till att den möjlighet som gavs fr.o.m. den 1 oktober 2004 att få även historiska trafikuppgifter vid hemlig teleövervakning, där straffskalan för det misstänkta brottet är lägre än vid utlämnande enligt lagen om elektronisk kommunikation och där bl.a. misstankar om dataintrång och barnpornografibrott omfattas, kommer att innebära ett klart ökat behov av att uppgifter sparas under lång tid.

Säkerhetspolisens uppfattning är att det är av synnerlig vikt för de brottsutredande myndigheterna att trafikuppgifter sparas under längre tid än tolv månader och då snarare 36 månader. Det gäller särskilt i utredningar av grov brottslighet, t.ex. grova våldsbrott, brott av organiserad karaktär och terroristbrott. I sådana fall kan planering och förberedelser pågå under mycket lång tid, kanske flera år, innan själva brottet genomförs. Säkerhetspolisen har gett som exempel att efter terroristattentaten i Madrid i mars 2004 efterfrågades trafikuppgifter från Sverige från år 1996. Som ytterligare exempel kan nämnas att i utredningen av den s.k. Nackabomben utgjorde historiska trafikuppgifter en mycket viktig anledning till att misstänkta personer kunde knytas till platsen för gärningen. De uppgifter som blev intressanta i utredningen var mer än ett och ett halvt år gamla. Endast en av operatörerna kunde ta fram så gamla uppgifter.

Vissa europeiska länder har redan en nationell lagstiftning om bevarandeskyldighet. Enligt uppgift är tiden för bevarandet satt till minst ett år i Belgien, maximalt ett år i Danmark och Frankrike, minst tre år i Irland, minst fyra år i Italien, tre månader i Nederlän-

derna, maximalt ett år i Polen och Spanien samt maximalt sex månader i Schweiz. I Storbritannien finns ett frivilligt åtagande hos operatörerna att spara trafikuppgifter i ett år.

Vi har kunnat konstatera från de exempel vi har fått, att de brottsutredande myndigheterna har behov av trafikuppgifter som är flera år gamla i utredningar av grova brott och att det finns flera orsaker till att operatörerna relativt sällan i dagsläget får förfrågningar på uppgifter som är äldre än tolv månader. De främsta skälen är givetvis att det finns en skyldighet för operatörerna att utplåna uppgifterna och att, när frågan om utlämnande blir aktuell, myndigheterna är medvetna om att utplånande måste ha skett och/eller att myndigheterna inte har möjlighet att av kostnadsskäl begära uppgifterna. Säkerhetspolisen har uppskattat att det finns behov av att få uppgifter äldre än tolv månader i några hundra förundersökningar årligen. Särskilt som det rör sig om grova brott där brottsligheten även många gånger kan sägas vara organiserad, instämmer vi i Säkerhetspolisens bedömning att det är av synnerlig vikt för det brottsutredande arbetet att uppgifter finns tillgängliga under längre tid tillbaka än tolv månader.

7.6 Problem med nuvarande ordning

Bedömning: Frånvaron av en bevarandeskyldighet för operatörerna medför många gånger stora problem för de brottsutredande myndigheterna med att få tillgång till de uppgifter som behövs. Det förhållandet leder i sin tur till allvarliga problem med effektiviteten i förundersökningsarbetet. Särskilt som det rör sig om utredningar av grövre brottslighet kan konsekvenserna från brottsbekämpningssynpunkt i längden bli oacceptabla.

Även i detta avsnitt har vi ett generellt sätt att beskriva frågorna. Vi går alltså inte in på vilka problem frånvaron av en viss typ av trafikuppgift kan innebära för olika brottsutredningar.

Lagen om elektronisk kommunikation anger som huvudregel att trafikuppgifterna skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektronisk meddelande (6 kap. 5 § LEK). Som undantag från den regeln anger lagen också att trafikuppgifterna får behandlas bl.a. om det krävs för operatörernas fakturering till dess att kundens fordran är betald eller preskriberad (6 kap. 6, 8 och 13 §§ LEK).

För direkt brottsutredande ändamål finns inte någon rätt att spara trafikuppgifterna annat än när ett beslut om hemlig teleavlyssning eller hemlig teleövervakning är fattat. I sådana fall är alltså de framtida uppgifterna, realtidsuppgifterna, ”säkrade” för de brottsutredande myndigheterna. Möjligheten att få tillgång till historiska trafikuppgifter som har genererats före det att tvångsmedelsbeslutet kom operatören till del, blir beroende av om operatörerna av andra skäl har kvar uppgifterna i sina system. Det gäller oavsett om det är fråga om att få tillgång till trafikuppgifterna inom ramen för hemlig teleövervakning eller genom en begäran enligt lagen om elektronisk kommunikation.

Det är alltså inte enbart skyldigheten att utplåna trafikuppgifter utan även den bedömning respektive operatör gör i fråga om den skyldigheten, t.ex. vid vilken tidpunkt som det inte längre av faktureringsskäl finns anledning att ha kvar uppgifterna, som sätter en gräns för vilka historiska uppgifter som de brottsutredande myndigheterna i praktiken har möjlighet att få del av. Operatörernas bedömningar av egna behov styr med andra ord tillgången till uppgifterna i brottsutredningar och i förlängningen möjligheterna att klara upp grövre brottslighet.

Säkerhetspolisen har uttryckt stora bekymmer för effektiviteten i brottsutredningsverksamheten med anledning av att någon bevarandeskyldighet inte finns föreskriven och har tillagt att så fort en historisk trafikuppgift inte kan lämnas ut från operatörerna riskerar det allvarliga konsekvenser för utredningsresultatet i den enskilda förundersökningen. Det skall dock framhållas att det är näst intill en omöjlighet att peka på enskilda förundersökningar eller uppskatta antalet förundersökningar där utredningsresultatet, till skillnad från hur det verkligen blev, hade blivit mer lyckat om en viss trafikuppgift hade varit tillgänglig.

Säkerhetspolisen har givit ett flertal exempel på förhållanden som skapar problem. Variationen är stor hos operatörerna när det gäller vilka trafikuppgifter som sparas och under vilken tid det sker. Det förekommer att sådana uppgifter som vissa operatörer sparar under mer än ett år utplånar andra operatörer omedelbart efter samtalet. För vissa av de operatörer som över huvud taget kan redovisa uppgifter om inkommande trafik rör det bara trafik från egna abonnenter. Hos operatörer som sparar uppgifter om utgående trafik, kan det gälla enbart sådana begränsade uppgifter som behövs för faktureringsändamål, vilket ofta inte är fallet med lokaliseringsuppgifter. När operatörer tillhandahåller förutbetalda tjänster (t.ex. genom anonyma kontantkort) finns det ofta ingen anledning

för dem att spara uppgifter över huvud taget. Dessutom kan viss teknik som används i dag hos operatörerna leda till att de brottsutredande myndigheterna inte kan få ut några uppgifter alls rörande viss kommunikation. Uppgifterna redovisas också på olika sätt hos operatörerna, vilket kräver stora resurser hos de brottsutredande myndigheterna för den tekniska tolkningen av informationen. Operatörerna har också till oss framfört vikten av att redovisningen av uppgifterna till de brottsutredande myndigheterna blir tydlig.

Till det kommer att vissa operatörer enligt Säkerhetspolisens uppfattning inte lämnar så kompletta uppgifter som skulle kunna tas fram ur operatörens system, vilket Säkerhetspolisen bedömer beror på att systemen inte är anpassade för begäran från de brottsutredande myndigheterna, att operatörerna saknar den tekniska kompetens som behövs för att få fram uppgifterna och att för lite resurser läggs på att t.ex. förenkla framtagandet av uppgifterna. Dessutom är de brottsutredande myndigheterna utlämnade till att lita på att det besked som lämnas från operatörerna är korrekt vad gäller vilka uppgifter som finns tillgängliga. Från en av de största operatörerna har vi hört sägas att det finns en hel del fall där man lämnar uppgifterna till de brottsutredande myndigheterna enbart om man får tillräckligt betalt, eftersom det arbete som kan behöva läggas ner hos operatören kan röra sig om några timmar och att detta kan betraktas som ren konsultverksamhet. Från operatörshåll har också sagts att så lite som möjligt kommer att göras för att lämna information till de brottsutredande myndigheterna, om operatörerna t.ex. skall lagra och lämna ut uppgifter utan ersättning.

Möjligheten att få tillgång till de historiska trafikuppgifterna i brottsutredningar blir som sagt ofta beroende av vilken operatör och även vilken teknik som är aktuell i det enskilda fallet. Den brottsling som med kunskap eller av ren slump utnyttjar, från hans sida sett, ”rätt” operatör och teknik har därmed stor möjlighet att undgå lagföring, medan andra kanske blir lagförda för brottsligheten. Enligt Säkerhetspolisen finns det till och med risk för att de länder som saknar nationell lagstiftning om bevarandeskyldighet för brottsbekämpande ändamål utnyttjas av kriminella organisationer som bas för deras verksamhet.

Det är mycket otillfredsställande att de brottsutredande myndigheterna inte kan få tillgång till historiska trafikuppgifter, trots att förutsättningarna för det är uppfyllda enligt reglerna om hemlig teleövervakning enligt rättegångsbalken och om utlämnande enligt lagen om elektronisk kommunikation. Tillgången till historiska uppgifter är av fundamental betydelse för brottsutredningsverk-

samheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Frånvaron av en bevarandeskyldighet för operatörerna medför många gånger stora problem för myndigheterna med att få tillgång till de uppgifter som behövs. Det förhållandet leder i sin tur till allvarliga problem med effektiviteten i förundersökningsarbetet. Särskilt som det rör sig om utredningar av grövre brottslighet kan konsekvenserna från brottsbekämpningssynpunkt i längden bli oacceptabla. Det uppstår även liknande effektivitetsproblem i de brottsutredningar som bedrivs i andra länder men där uppgifter från operatörer i Sverige efterfrågas. Det måste också tilläggas att mot bakgrund av regeringens förslag i lagrådsremissen den 3 mars 2005 Kostnadsansvar för hemlig teleavlyssning m.m., dvs. att operatörerna inte skall ha rätt till ersättning för verkställighetskostnader, finns en stor fara att problemen för de brottsutredande myndigheterna att få tillgång till uppgifterna snart kommer att framträda än mer tydligt.

8 Medverkan vid verkställigheten av vissa tvångsmedelsbeslut

8.1 Sammanfattning av förslagen

En bestämmelse skall införas i 27 kap. RB om att en enskild är skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning eller övervakning.

8.2 Nuvarande bestämmelser

De grundläggande reglerna om hemlig teleavlyssning och hemlig teleövervakning finns i 27 kap. 18 och 19 §§ RB. Bestämmelserna är teknikneutrala, dvs. oberoende av vilken teknik som används för överföring av telemeddelandena, och omfattar t.ex. såväl vanlig taltelefoni som mobiltelefoni och kommunikation via Internet. De tekniska förutsättningarna för att verkställa tvångsmedelsbesluten skiftar kraftigt beroende på bl.a. vilken typ av telefoni det är fråga om.

I 27 kap. 25 § första stycket RB finns en bestämmelse om verkställigheten av beslut om hemlig teleavlyssning och hemlig teleövervakning. Av paragrafen framgår att de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen får användas när rätten har lämnat tillstånd till tvångsmedlen.

Begreppet tekniskt hjälpmedel förekommer i flera sammanhang (se vårt förslag i avsnitt 3.5). År 1975 infördes det i 4 kap. 9 a och 9 b §§ BrB, med en innebörd som närmast avser avlyssnings- och inspelningsapparater, såsom mikrofoner, bandspelare och radiosändare. Samma uttryck återfinns i tryckfrihetsförordningen (2 kap. 3 §, jfr 6 §). Här avses såväl hårdvaror som datorprogram (SOU 1988:64 s. 134).

År 1988 föreskrevs i taxeringslagen att taxeringsrevisorn vid verkställighet av taxeringsrevision på begäran skulle ges tillfälle att själv använda terminal eller annat tekniskt hjälpmedel. I det sammanhanget uttalades i propositionens specialmotivering att rätten att ta del av handlingar innebar att granskaren också skall få tillgång till datorprogram. Innebörden av uttrycket tekniskt hjälpmedel berördes dock inte närmare (prop. 1987/88:65 s. 77). Av sammanhanget framgår dock att även datorprogram avsågs eftersom en terminal inte är användbar utan tillhörande program. Vid en översyn av tvångsmedlen på skatteområdet aktualiserade Lagrådet frågan om vad begreppet tekniskt hjälpmedel bör avse. I enlighet med Lagrådets förslag kom begreppet att innefatta även s.k. mjukvara, dvs. dataoperativsystem, bokföringsprogram, revisionsprogram och andra program som behövs för att granska ett material som finns lagrat på disk eller annat medium som bara kan läsas med hjälp av ADB (prop. 1993/94:151 s. 256 f.).

Vid ändringar år 1989 av bestämmelserna om telefonavlyssning föreskrevs i 27 kap. 18 § RB att telemeddelanden får tas upp genom ett "tekniskt hjälpmedel för återgivning av innehållet i meddelandet". Det uttryckssättet används även i dag i bestämmelsen. I sammanhanget berördes inte begreppets närmare innebörd. I praktiken skulle detta innebära att meddelandena spelades in på band. De författningsändringar som genomfördes år 1989 syftade emellertid till att också datorkommunikation skulle kunna avlyssnas och övervakas och sådana åtgärder kräver vanligtvis både dator och program.

Det allmänna är givetvis för sin verksamhet beroende av att få insyn i information som enskilda förfogar över. Myndigheter har i olika författningar bemyndigats att begära att enskilda lämnar vissa uppgifter, handlingar etc. till myndigheterna (se t.ex. 8 kap. 1 § LEK). Datastraffrättsutredningen gjorde i sitt betänkande (SOU 1992:110 s. 333 ff. 349 ff. och 405 ff.) en indelning av tvångsmedel i sådana fall där den enskilde medverkar aktivt respektive endast passivt. Avsikten med indelningen var att påvisa att den enskilde spelar olika roller beroende på vilket tvångsmedel som aktualiseras. Med passiv medverkan avsåg utredningen att enskilda förväntas att inte hindra eller annars motsätta sig vissa åtgärder som ett straffprocessuellt tvångsmedel omfattar. Som exempel nämndes regleringen rörande beslag, husrannsakan, hemlig teleavlyssning, hemlig teleövervakning och kvarstad. Aktiv medverkan menade utredningen kunde beteckna den enskildes roll vid edition och tillhandahållande av föremål vid syn samt vittnesplikten. För tydlighetens skull skall nämnas att gränsen för när krav kan ställas på enskilda att aktivt

medverka vid förundersökningar måste dras mellan de som är misstänkta för brott och andra.

Datastraffrättsutredningen föreslog bestämmelser om medverkan av tredje man. Den som skäligen kunde antas känna till funktionerna i ett visst system för automatisk informationsbehandling eller andra tekniska förutsättningar för åtkomst eller granskning av vissa data skulle enligt utredningen kunna föreläggas att genast tillhandahålla de handlingar och lämna de upplysningar som behövdes för verkställigheten. Utredningen föreslog också en lagreglering av rätten att använda tvång när tillträde för verkställighet vägras. I den föreslagna lagtexten angavs att om tillträde för verkställighet vägras får hus, rum eller slutet förvaringsställe öppnas med våld.

Uttrycket tekniskt hjälpmedel infördes år 1993 också i bestämmelsen om verkställighet i 27 kap. 25 § första stycket RB. Den närmare innebörden av uttrycket behandlades emellertid inte i Telelagsutredningens betänkande Telelag (SOU 1992:70) eller regeringens proposition 1992/93:200 om en telelag och en förändrad verksamhetsform för Televerket, m.m. Telelagsutredningen motiverade bestämmelsen i 27 kap. 25 § första stycket RB på följande sätt (se SOU 1998:46 s. 64 ff.).

> I 27 kap. rättegångsbalken anges, efter den ändring som redovisas ovan, inte uttryckligt vem som har att medverka vid verkställigheten av där avsedda tvångsmedel [Televerket nämndes tidigare uttryckligen i lagtexten]. Om det blir fråga om att ålägga enskilda att medverka till en verkställighet, krävs enligt 8 kap. 3 § regeringsformen att sådana åligganden meddelas genom lag. En bestämmelse behövs därför i rättegångsbalken om att erforderlig utrustning får anslutas, underhållas och återtas [Bestämmelsen ändrades år 1995 (prop. 1994/95:225) då orden ”anslutas, underhållas och återtas ersattes av ordet ”användas”]. Härav följer således en skyldighet för enskilda att biträda och lämna tillträde för polisen. I den mån det visar sig erforderligt kan verkställighetsföreskrifter till en sådan bestämmelse meddelas med stöd av 8 kap. 13 § regeringsformen, jfr dock 2 kap. 6 och 12 §§ regeringsformen.
>
> Det är min bedömning att de befordringsföretag, vilkas anläggningar i första hand kommer att behöva utnyttjas i samband med avlyssning eller övervakning kommer att medverka till att åtgärderna kan verkställas i den utsträckning som det behövs. Kravet på sekretess gör att det knappast kan

> bli aktuellt att genomföra en avlyssning om det i ett enskilt fall bedöms tveksamt om åtgärden kan hållas hemlig. Det kan gälla exempelvis om tvångsmedlet riktar sig mot någon som förfogar över den anläggning i vilken avlyssningsutrustningen skall kopplas in. Om verkställigheten hindras kan i vissa situationer bestämmelserna i 17 kap. brottsbalken om brott mot allmän verksamhet m.m. bli tillämpliga. Någon ytterligare reglering för att garantera verkställigheten av tvångsmedelsanvändningen torde mot bakgrund av det nu sagda inte behövas.

I prop. 1992/93:200 om den nya telelagen berördes bestämmelsen inte närmare. Departementschefen uttalade dock (s. 261), som svar på vad remissinstanserna framfört i fråga om verkställighetsregler, att, med tanke på den fortsatta beredningen av Datastraffrättsutredningens betänkande Information och den nya Informations-Teknologin (SOU 1992:110), var ”Telelagsutredningens förslag i detta hänseende för närvarande tillräckligt”.

I propositionen 1994/95:227 Hemlig teleavlyssning och hemlig teleövervakning (s. 29) uttalade regeringen att det inte råder någon tvekan om att bestämmelsen i 27 kap. 25 § första stycket RB även omfattar verkställighet med hjälp av datorprogram. Däremot ansåg regeringen i det sammanhanget att bestämmelsen borde förtydligas så att det skulle klart framgå att polisen får verkställa beslut om tvångsmedel på teleområdet inte bara genom att använda traditionell avlyssningsutrustning utan också genom att använda såväl hårdvaror som datorprogram.

Polisens befogenhet enligt rättegångsbalken att använda teknisk utrustning omfattar alltså inte bara ”traditionell avlyssningsutrustning” utan även datatekniska hårdvaror och datorprogram. Detta innebär inte att en operatör måste ta hänsyn till polisens möjligheter att verkställa ett tvångsmedelsbeslut. Även om beslutet som sådant medför en skyldighet för operatören att i viss mån medverka vid verkställigheten, innebär det inte någon skyldighet för denne att tillhandahålla utrustning eller tekniska lösningar i sin verksamhet och inte heller att biträda vid verkställigheten inom viss tid.

Under vårt arbete har frågan uppkommit om det bör finnas en författningsreglerad skyldighet för operatörerna att på olika sätt medverka vid verkställighet av tvångsmedelsbesluten. Som läget är i dag är polisen i praktiken beroende av operatörernas vilja att hjälpa till. I prop. 1994/95:227 (s. 29 f.) uttalade regeringen följande.

> Frågan om vilka befogenheter som kan härledas ur ett beslut om tvångsmedel har diskuterats i olika sammanhang. Riksdagens justitieutskott har i denna fråga med anledning av en motion om befogenheten att ta med någon för blodprov uttalat bl.a. att det av en lagstadgad rätt att bruka ett tvångsmedel i åtskilliga fall måste följa en befogenhet att också vidta visst ingrepp eller andra åtgärder som är nödvändiga för att rätten att bruka tvångsmedlet inte skall bli ändamålslös (bet. 1983/84:JuU27 s. 40). Det ligger i sakens natur att användandet av tvångsmedel kan innebära ett visst intrång utöver vad som följer av själva tvångsmedlet och att detta får godtas. Lika självklart är att även utomstående kan drabbas av effekterna av ett tvångsmedel (jfr SOU 1994:131 s. 269).
>
> De verkställighetsfrågor som aktualiseras torde i praktiken kunna lösas inom ramen för de befogenheter som följer redan av föreliggande reglering. Inte heller frågan om tredje mans medverkan torde vid den praktiska tillämpningen ha vållat några särskilda svårigheter. I vart fall bör dessa frågor, som kan bli aktuella vid all tvångsmedelsanvändning, behandlas i ett större sammanhang än inom ramen för tvångsmedlen på teleområdet. Någon särskild reglering av dessa frågor föreslås därför inte i detta lagstiftningsärende.

Vi behandlar frågor om anpassningsskyldigheten i avsnitt 6. Enligt 6 kap. 19 § LEK innebär den skyldigheten att operatörerna bl.a. skall bedriva verksamheten så att tvångsmedelsbeslut kan verkställas och så att verkställandet inte röjs. När anpassningsskyldigheten infördes i telelagen berörde regeringen även frågan om medverkan och uttalade följande (prop. 1995/96:180 s. 20).

> En annan fråga som aktualiserats i promemorian och som också tagits upp av några remissinstanser är frågan om teleoperatörernas roll när beslut om hemlig teleavlyssning och hemlig teleövervakning skall verkställas och om vilka befogenheter som rent allmänt kan härledas ur ett beslut om tvångsmedel. Användandet av tvångsmedel innebär alltid ett visst intrång utöver vad som följer av själva tvångsmedlet. Lika självklart är det att även utomstående kan drabbas av effekterna av ett tvångsmedel. Det är däremot inte lika klart vad som gäller om tredje mans medverkan vid verkställighet av ett tvångsmedel.

> Denna allt annat än okomplicerade fråga aktualiseras emellertid vid all tvångsmedelsanvändning och måste därför enligt regeringens mening behandlas i ett större sammanhang än inom ramen för tvångsmedlen på teleområdet. Den tveksamhet som finns på området förorsakar inte några andra praktiska problem vid verkställigheten av beslut om hemlig teleavlyssning och hemlig teleövervakning än de som behandlas i detta ärende.

I en skrivelse till regeringen under hösten 2002 om tillgång till telekommunikation för polisens brottsutredande verksamhet anger Rikspolisstyrelsen följande rörande skyldigheten för operatörer att biträda vid verkställighet av tvångsmedelsbesluten (dnr Ju2002/7018/PO och RÄS-002-3668/02).

> De telemeddelanden och uppgifter som Polisen får tillgång till genom hemlig teleavlyssning och hemlig teleövervakning kan komma att användas som bevisning i brottmål. Höga krav måste därför alltid ställas på teknik och handhavande vid verkställighetsåtgärden så att inte utrymme lämnas för tvekan om att uppgifterna är fullständiga och korrekta.
>
> Eftersom den miljö där verkställighet skall genomföras blir allt mer tekniskt avancerad är en förutsättning för att Polisen skall kunna verkställa beslut i enlighet med rättegångsbalken att Polisen får vägledning från berörd operatör. Behovet av särskild vägledning medför att verkställigheten kan bli fördröjd, vilket alltid kan vara till men för det brottsutredande arbetet. Särskilt allvarligt är detta i brådskande fall, t.ex. när åklagaren fattat beslut enligt specialbestämmelsen i 5 § andra stycket lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål. Teknikutvecklingen medför också att allt högre krav måste ställas på de tekniska hjälpmedel som Polisen använder. Det kan i dag förekomma att verkställighet av ett domstolsbeslut inte är tekniskt möjligt att genomföra därför att teleoperatören inte anpassat sin verksamhet. Det finns avsevärd risk för att detta problem ökar i takt med teknikutvecklingen.
>
> Till följd av samtrafik och andra former av tillträde kommer de tjänster som mindre operatörer tillhandahåller att gå via de stora operatörernas nät vid förmedling av telemeddelanden. Om Polisen direkt kunde vända sig till de operatörer som tillhandahåller näten, skulle verkställigheten ske avsevärt

snabbare. Även om en verksamhet är anpassad så att hemlig teleavlyssning och hemlig teleövervakning kan ske hos en operatör som tillhandahåller ett nät, är dock verkställigheten i dessa fall ofta inte möjlig eftersom de operatörer som tillhandahåller näten anser sig obehöriga att verkställa beslut avseende andra än sina egna abonnenter. Detta aktualiserar frågan om vilken omfattning ett tvångsmedelsbeslut har och i vilken omfattning tredje man är skyldig att medverka vid verkställighet av aktuella tvångsmedel. Såvitt Rikspolisstyrelsen kan se är frågan ännu obesvarad. Det skulle dock ha stor betydelse om ett tvångsmedelsbeslut i sig innebär att en teleoperatör är skyldig att möjliggöra verkställighet av beslutet, jämfört med att operatören bara i mindre grad är skyldig att medverka vid verkställighet. Detta gäller även beträffande telemeddelanden som härrör från andra operatörers abonnenter.

När Rikspolisstyrelsen gav in skrivelsen till regeringen gällde telelagens reglering om anpassningsskyldighet. Telelagen har därefter ersatts av lagen om elektronisk kommunikation. Rikspolisstyrelsen har påtalat att skrivningarna rörande tveksamheten hos operatörerna om behörigheten att verkställa beslut avseende andra än sina egna abonnenter var en följd av bestämmelserna i telelagen. Lagen om elektronisk kommunikation skiljer på anpassningsskyldighet för nät och tjänst. Som en följd av det upplever Rikspolisstyrelsen att det i dag inte finns något problem i detta, eftersom den som tillhandahåller ett allmänt kommunikationsnät är anpassningsskyldig enligt 6 kap. 19 § LEK och därmed också behörig att verkställa beslut som rör andra operatörers abonnenter i nätet.

8.3 Våra överväganden

Förslag: En bestämmelse skall införas i 27 kap. RB om att en enskild är skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning eller övervakning.

Som framgått anges i 27 kap. 25 § första stycket RB att de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen får användas av de brottsutredande myndigheterna. Med det uttrycket avses bl.a. att de tekniska hjälpmedlen får anslutas, underhållas och

återtas, vilket tidigare också framgick av paragrafens ordalydelse. Av detta följer alltså att enskilda (i praktiken operatörerna) har en skyldighet att biträda och lämna tillträde för polisen. Enligt uppgift från Rikspolisstyrelsen är detta i dagsläget inte tillräckligt för att garantera en effektiv verkställighet av tvångsmedelsbesluten. I stället menar Rikspolisstyrelsen att det bör ställas krav på en mer aktiv medverkan från operatörerna när en sådan begärs.

En mer aktiv medverkan kan bestå i allt från att lämna information om funktioner och andra tekniska förutsättningar som är nödvändiga för att kunna verkställa tvångsmedelsbesluten till att tillhandahålla teknisk utrustning. Som exempel kan nämnas att operatören lämnar uppgift om

- vilka tjänster som tillhandahålls,
- nätets uppbyggnad och konstruktion,
- logiska och fysiska punkter för inkoppling och
- avgränsningar som säkerställer att inte större ingrepp än nödvändigt sker.

Avsikten med upplysningarna, särskilt i det sistnämnda hänseendet, är, förutom att möjliggöra verkställigheten, att begränsa integritetsintrånget genom att det blir klart för de brottsutredande myndigheterna var en lämplig avlyssningspunkt finns där endast den misstänktes trafik passerar. På så sätt behöver polisen inte använda sållningsinstrument för att få fram rätt tekniskt hjälpmedel (det som nu benämns teleadress). Att operatören skall tillhandahålla teknisk utrustning innebär att operatören ställer utrustning till förfogande för polisen som operatören själv har och som på grund av systemets utformning är lämplig att använda i sammanhanget.

Frågan om aktiv medverkan är inte densamma som frågan om anpassningsskyldighet, som tas upp i avsnitt 6 (se 6 kap. 19 § LEK). Vi utvecklar innebörden av den skyldigheten i det angivna avsnittet men kan nämna att i samband med att anpassningsskyldigheten infördes uttalade regeringen i proposition 1995/96:180 Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning (s. 25), att anpassningsskyldigheten inte kan vara begränsad till anpassningar i systemen varje gång ett beslut om tvångsmedel skall verkställas utan att det i stället bör vara fråga om en generell skyldighet som hänför sig till konstanta egenskaper i telesystemet. Regeringen menade att telesystemet vid varje givet tillfälle bör innehålla de egenskaper som behövs för att ett beslut om avlyssning eller övervakning genast skall kunna verkställas. Den närmare innebörden av anpassningsskyldigheten blir enligt regeringen i praktiken ett krav på att operatörerna skall använda sig av

tekniska hjälpmedel som har vissa egenskaper som skall garantera att operatörerna över huvud taget kan tillhandahålla polisen relevant information vid tvångsmedelsbeslut och att operatörerna skall vidta de personella och organisatoriska dispositioner som krävs för att hantera hjälpmedlen.

Skyldigheten att medverka måste i praktiken ses helt skild från anpassningsskyldigheten och rör kravet på att operatörerna vidtar andra åtgärder efter begäran om aktiv medverkan vid verkställigheten av tvångsmedelsbesluten. Exempel på det kan som sagt vara att lämna information om funktioner, tillhandahålla teknisk utrustning och vidta de personella och organisatoriska dispositioner som är nödvändiga för verkställighet inom kort tid av respektive tvångsmedelsbeslut.

Av artikel 6.1 i det tidigare nämna auktorisationsdirektivet (se avsnitt 2.6 och 6.5) och del A punkten 11 i bilagan till direktivet framgår att villkor som möjliggör avlyssning för behöriga nationella myndigheter får uppställas för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Sådana villkor skall vara objektivt motiverade med avseende på det nät eller den tjänst som berörs, samt öppet redovisade, icke-diskriminerande och proportionella (prop. 2002/03:110 s. 268, 437 och 442).

Även en reglering av skyldigheten att medverka vid verkställighet syftar till att möjliggöra laglig avlyssning. En medverkan från operatörernas sida skall aldrig kunna ersätta anpassningsskyldigheten enligt 6 kap. 19 § LEK, som i sig garanterar en effektivitet vid verkställighet av tvångsmedelsbesluten. Skyldigheten att medverka skall ses som ett separat krav vid sidan av denna och får inte påverka bedömningen av om en viss anpassningsåtgärd skall vidtas. Skyldigheten att medverka träffar samtliga som tillhandahåller nät och tjänster där meddelandena får bli föremål för beslut om avlyssning och övervakning.

Från Rikspolisstyrelsen har det alltså framförts att kravet på medverkan bör lagregleras utöver vad som i dag kan anses följa av 27 kap. 25 § första stycket RB. En slutsats som tidigare har dragits och som framgår av de citerade förarbetena har varit att det inte skulle finnas några praktiska problem med den gällande ordningen, där en mer aktiv medverkan från operatörerna inte är reglerad. Rikspolisstyrelsen menar dock att den slutsatsen numera inte är riktig och har förklarat att för att genomföra avlyssnings- och övervakningsåtgärder behöver de brottsutredande myndigheterna få uppgifter från operatörerna bl.a. om detaljer i respektive opera-

törs system. Det gäller särskilt mot bakgrund av den snabba tekniska utvecklingen som bl.a. innebär att tekniker och tjänster smälter samman.

Anpassningsskyldigheten enligt 6 kap. 19 § LEK träffar inte alla verksamheter där verkställighet av avlyssnings- och övervakningsbeslut kan förekomma. I dag finns olika begränsningar i anpassningsskyldigheten. Vissa begränsningar kommer att finnas även om vårt förslag rörande den skyldigheten genomförs. Rikspolisstyrelsen har påtalat att ett krav på medverkan vid verkställighet av tvångsmedelsbesluten från operatörer även med begränsad anpassningsskyldighet kan vara nödvändigt för att garantera att avlyssning eller övervakning kan genomföras. I sådana fall kan ett krav på medverkan från operatörens sida med exempelvis upplysningar göra verkställigheten möjlig, något som framstår som en i sammanhanget mer enkel och billig lösning än en genomförd anpassning.

Rikspolisstyrelsen har dessutom problem med servicenivån hos många operatörer, särskilt vad gäller den tid som åtgår från beställningen av åtgärden till dess att tvångsmedelsbeslutet kan börja verkställas. Det kan få allvarliga följder för brottsutredningarna, speciellt i brådskande ärenden. I samband med att vi behandlade anpassningsskyldigheten (avsnitt 6) kunde vi konstatera att arbetet med anpassningskraven har varit lågt prioriterat hos många operatörer. Huvudorsakerna till detta är att anpassningsskyldigheten i dagsläget i många fall är otydligt reglerad och att operatörerna måste stå för de kostnader som anpassningsåtgärderna kräver. Vi föreslår ingen ändring i det sistnämnda hänseendet.

Mot den bakgrunden och särskilt med tanke på regeringens förslag nyligen i lagrådsremissen den 3 mars 2005 Kostnadsansvar för hemlig teleavlyssning m.m. om att den som bl.a. lämnar ut innehållet i och uppgifter om avlyssnade eller övervakade meddelanden inte har rätt till ersättning för det (jfr SOU 2003:74 s. 249 ff.), finns det ett stort behov av att tydliggöra operatörernas skyldighet att medverka vid verkställigheten. Vi vill i det sammanhanget erinra om den inställning vi har hört från operatörerna, nämligen att det som skall göras gratis läggs det inga resurser på och att operatörerna kommer att göra så lite som möjligt om man inte får ersättning för sitt arbete.

Rikspolisstyrelsen har också tillagt att en reglering av operatörernas medverkan behövs för att det skall stå klart vilka skyldigheter och kostnader operatören har och påtar sig. Det gäller särskilt i

operatörens kontakter med såväl brottsutredande myndigheter som kunder.

Även om kontakterna mellan de brottsutredande myndigheterna och de flesta operatörer sker i ett bra samförstånd, är vi övertygade om att frånvaron av ett reglerat krav på medverkan från operatörernas sida vid verkställighet av tvångsmedelsbesluten i dagsläget skapar problem för de brottsutredande myndigheterna i en annan omfattning och av annan karaktär än som var fallet tidigare. Vi kan se att de problemen kommer att bli större om regeringens förslag i den nämnda lagrådsremissen om kostnadsansvaret blir verklighet. I remissen har regeringen markerat principen om operatörernas ansvar och i slutänden abonnenternas ansvar för kostnader på området.

Vi föreslår därför en mer tydlig reglering av skyldigheten att medverka och bedömer att detta kommer att leda till en i många fall mer effektiv verkställighet och därmed till en effektivare brottsutredningsverksamhet utan att någon egentlig ökning av intrånget i den enskildes integritet uppstår. Snarare finns det stor möjlighet att den information som ges från operatören till polisen leder till att risken för integritetsintrång hos tredje man minskar. En annan förväntad positiv effekt är att medverkan från operatörerna normalt innebär en begränsning av riskerna för skador på operatörernas tekniska utrustning. Dessutom ökar förutsättningarna för att uppgifterna kommer myndigheterna till del på enklast möjliga sätt. Även om det varken är möjligt eller lämpligt att precisera i lagtext vad som skall innefattas i skyldigheten att medverka vid verkställigheten, borde enbart det klargörandet som en reglering i sig innebär leda till vissa effektivitetsvinster även hos operatörerna, utan att det blir fråga om några stora tillkommande kostnader vid sidan av det kostnadsansvar som finns i dag och som kan förväntas bli ålagt operatörerna i en framtid (se förslaget i den nämnda lagrådsremissen).

Vi föreslår alltså att en mer tydlig bestämmelse om krav på medverkan vid beslut om avlyssning och övervakning skall införas i rättegångsbalken. Något principiellt skäl av avgörande betydelse mot att reglera kravet på medverkan i dessa specifika fall utan att samtidigt behandla frågan om medverkan av enskilda vid andra tvångsmedelsbeslut kan vi inte se.

Som har framgått rör kravet på medverkan i första hand en skyldighet att lämna information, att tillhandahålla teknisk utrustning och att snabbt vidta nödvändiga åtgärder från det att verkställigheten har beställts av polisen. Vi har diskuterat att införa en tids-

gräns för medverkan, alltså för den tid inom vilken operatören har att medverka genom att påbörja verkställighetsåtgärderna. För samtliga operatörer skulle en skälig tidsgräns kunna vara en timme från polisens begäran om medverkan under kontorstid (kl. 8-17). Det är i högsta grad rimligt att de operatörer som har personella resurser avdelade för drift- och nätövervakning även under annan tid har samma tidsmässiga krav på sig att medverka även under den tiden. Eftersom förhållandena varierar så mycket hos operatörerna har vi kommit fram till att det i vart fall i dagsläget inte bör införas någon generell tidsgräns för medverkan. För närvarande är det i stället tillräckligt att begreppet ”genast” används i lagtexten, bl.a. för att markera att det som huvudregel inte får röra sig om mer än någon timmes väntetid för de brottsutredande myndigheterna.

För att myndigheternas arbete särskilt på det brottsutredande området skall bli verkningsfullt behövs många gånger föreskrifter om tvång för den som inte efterkommer lagfästa krav på t.ex. uppgiftsskyldighet eller handlingars tillgänglighet. Vi ser dock ingen anledning i dagsläget att komplicera den föreslagna regleringen med sådana bestämmelser utan utgår från att operatörerna ändå medverkar på det sätt som är tänkt. I annat fall måste frågan om påtryckningsmedel övervägas.

9 Hemlig dataavläsning

9.1 Sammanfattning av förslagen

– Hemlig dataavläsning skall införas som nytt tvångsmedel.
– Med hemlig dataavläsning avses att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål.
– Bestämmelser om hemlig dataavläsning skall tas in i en ny lag, vars giltighetstid till en början begränsas till fem år.
– Domstol skall pröva frågor om hemlig dataavläsning på ansökan av åklagaren.
– Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig dataavläsning.
– Hemlig dataavläsning skall få äga rum vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff,
3. brott enligt 4 kap. 9 c § brottsbalken (dataintrång), brott enligt 16 kap. 8 § brottsbalken som inte är att anse som ringa (hets mot folkgrupp), brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa (barnpornografibrott), eller
4. annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år.

forts.

– Hemlig dataavläsning skall få äga rum, om
1. någon är skäligen misstänkt för brottet,
2. åtgärden är av synnerlig vikt för utredningen, och
3. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.
– I förtydligande syfte skall det av lagtexten uttryckligen framgå att rätten får föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.
– Även om det inte finns någon person som är skäligen misstänkt skall hemlig dataavläsning få äga rum om det är av synnerlig vikt för utredningen att dataavläsning sker av information i informationssystem som har använts eller används vid brottet. Hemlig dataavläsning i sådana fall får äga rum endast om åtgärden syftar till att fastställa vem som skäligen kan misstänkas för brottet.
– I fall där det finns en skäligen misstänkt person får hemlig dataavläsning endast avse informationssystem som det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av. Avser åtgärden informationssystem i någon annans stadigvarande bostad, får hemlig dataavläsning äga rum endast om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.
– Ett beslut om hemlig dataavläsning skall gälla under en viss tid. Tiden får inte bestämmas längre än vad som är nödvändigt och får inte överstiga en månad från dagen för beslutet.
– Ett beslut om hemlig dataavläsning får innefatta rätt för den brottsutredande myndigheten att i hemlighet bereda sig tillträde till en plats som annars särskilt skyddas mot intrång i syfte att installera de tekniska hjälpmedlen.
– Ett tekniskt hjälpmedel som har installerats skall återtas eller göras obrukbart så snart det kan ske efter det att tiden för tillståndet gått ut eller tillståndet hävts. När hjälpmedlet har återtagits eller gjorts obrukbart, skall rätten underrättas om det.
– Vid genomförande av hemlig dataavläsning får olägenhet eller skada inte förorsakas utöver vad som är oundgängligen nödvändigt.
– Hemlig dataavläsning skall inte få ske av sådana meddelanden mellan den misstänkte och hans försvarare som avses i 27 kap. 22 § RB. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer. **forts.**

– Om det vid hemlig dataavläsning har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avläsning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller
2. det finns särskilda skäl.

– Om det har kommit fram uppgifter om förestående brott, får uppgifterna användas för att förhindra brott.
– En upptagning som har gjorts vid hemlig dataavläsning skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 27 kap. 12 § första stycket RB.
– De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brott. De skall därefter förstöras.
– Hemlig dataavläsning skall omfattas av de särskilda regler som finns i

1. lagen med särskilda bestämmelser om tvångsmedel i vissa brottmål (1952 års tvångsmedelslag),
2. lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m., och i
3. lagen om särskild utlänningskontroll.

– Regeringen skall årligen till riksdagen redovisa de brottsutredande myndigheternas tillämpning av bestämmelserna om hemlig dataavläsning.

9.2 Inledning

9.2.1 Vårt uppdrag

I våra huvuddirektiv (Dir. 2000:90, se *bilaga 1)* sägs att det finns anledning för oss att överväga om det behövs författningsändringar som kan förbättra möjligheterna att förhindra, avslöja, utreda eller lagföra brott och att detta inte minst gäller brott av organiserad

eller annars allvarlig karaktär. Vi har tidigare lagt fram flera förslag i detta syfte, framför allt i betänkandet Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74).

Under vårt arbete med frågorna i tilläggsdirektiven (Dir. 2003:145, se *bilaga 2*) rörande elektronisk kommunikation har det från både åklagare och polis (Säkerhetspolisen och Rikskriminalpolisen) framförts att det finns ett stort behov av ett nytt hemligt tvångsmedel i Sverige efter den modell som kallas dataavläsning och som för några år sedan infördes i Danmark. Metoden, som är tillåten att använda även i andra europeiska länder (särskilt inom ramen för hemlig teleavlyssning) samt i exempelvis USA och Canada, har en nära anknytning till de tvångsmedel som vi i övrigt behandlar i detta betänkande och innebär i korthet att de brottsutredande myndigheterna har möjlighet att få information om innehållet i en dator och hur den används. Mot bakgrund av innehållet i framför allt våra huvuddirektiv har vi beslutat att ta upp den frågan och behandla den i detta betänkande.

9.2.2 Den danska lagstiftningen om dataavläsning

Sedan några år finns möjlighet för de brottsutredande myndigheterna i Danmark att använda det hemliga tvångsmedlet dataavläsning. I förarbetena till lagstiftningen nämner Justitsministeriet att det finns olika möjligheter att få tillgång till icke offentlig information, som kommunikation där datorer används och till dokument som finns i datorer. Det kan ske främst genom motsvarigheterna till de svenska tvångsmedlen hemlig teleavlyssning, hemlig teleövervakning, beslag och husrannsakan. Justitsministeriet påpekade i lagförslaget att det framför allt på grund av tekniska förhållanden (t.ex. kryptering) och risken för att den pågående verkställigheten av tvångsmedlet avslöjas, inte i alla fall är möjligt eller lämpligt att utnyttja sådana metoder. Justitsministeriet menade i sina överväganden att polisen bl.a. i ljuset av terrorangreppen i USA den 11 september 2001 har behov av att i samband med utredning av allvarliga brott kunna löpande registrera eller avläsa innehållet i och användningen av t.ex. bestämda datorer.

Bestämmelsen om dataavläsning finns i Retsplejeloven § 791 b, som lyder på följande sätt.

Aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning) kan foretages, såfremt
1) der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3,
2) indgrebet må antages at være af afgørende betydning for efterforskningen, og
3) efterforskningen angår en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af straffelovens § 180, § 183, stk. 1 og 2, § 183 a, § 186, stk. 1, § 187, stk. 1, §§ 191, 192 a eller 237.

Stk. 2. Indgreb som nævnt i stk. 1 må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.

Stk. 3. Afgørelse om dataaflæsning træffes af retten ved kendelse. I kendelsen angives det informationssystem, som indgrebet angår. I øvrigt finder reglerne i § 783, stk. 1, 3. og 4. pkt., samt stk. 2 og 3, tilsvarende anvendelse.

Stk. 4. Efterfølgende underretning om et foretaget indgreb sker efter reglerne i § 788, stk. 1, 3 og 4. Underretningen gives til den, der har rådigheden over det informationssystem, der har været aflæst efter stk. 1. I øvrigt finder reglerne i § 782, stk. 2, §§ 784, 785, 789 samt 791 tilsvarende anvendelse.

Som framgår av lagtexten finns ett misstanke- och ett s.k. indikationskrav. Enligt första stycket första och andra punkterna krävs dels att det finns en bestämd grund till att anta att informationssystemet används av en misstänkt i samband med viss grövre kriminalitet, dels att åtgärden kan antas vara av avgörande betydelse för utredningen.

De brott vid vilka dataavläsning kan användas och som anges i första stycket tredje punkten är vissa allvarliga brott som bl.a. kan tänkas utgöra led i eller ha annat samband med terrorhandlingar. Det rör forbrydelser mod statens selvstændighed og sikkerhed (kapitel 12), forbrydelser mod statsforfatningen og de øverste statsmyndigheder mv. (kapitel 13), kvalificeret brandstiftelse (§ 180), forvoldelse af sprængning og spredning af skadevoldende luftarter, jernbaneulykke m.m. (§ 183, stk. 1 og 2), flykapring (§ 183 a), for-

voldelse af fare for menneskers liv eller helbred ved at tilsætte vandbeholdninger sundhedsfarlige stoffer mv. (§ 186, stk. 1), tilsætte gift eller andre lignende stoffer til ting, som er bestemt til forhandling eller udbredt benyttelse mv. (§ 187, stk. 1), grove narkotikaforbrydelser (§ 191), særligt grove våbenlovsovertrædelser (§ 192 a) samt drab (§ 237).

En proportionalitetsprincip finns i bestämmelsens andra stycke. Enligt tredje stycket är det rätten som beslutar om dataavläsning. Fjärde stycket reglerar underrättelse i efterhand om tvångsmedelsanvändningen, vilket är en ordning som i Danmark gäller även vid exempelvis hemlig teleavlyssning.

Det har inte gått att få några precisa uppgifter från danskt håll om tillämpningen av det nya tvångsmedlet, särskilt inom den danska motsvarigheten till Säkerhetspolisen.

9.3 Nuvarande tvångsmedelsbestämmelser

Vissa tvångsmedel kan användas för att få tillgång till ”innehållet” i datorer. Här skall lämnas en redogörelse för dessa regler i rättegångsbalken.

9.3.1 Hemlig teleavlyssning och hemlig teleövervakning

Tidigare i betänkandet har bestämmelserna i 27 kap. RB om hemlig teleavlyssning och hemlig teleövervakning behandlats utförligt. Hemlig teleavlyssning innebär att telemeddelanden som befordras eller har befordrats till eller från ett telefonnummer, en kod eller annan teleadress i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet. Vid användning av tvångsmedlet får brottsutredande myndigheter tillgång till innehållet i telemeddelanden. Ett telemeddelande är ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare (6 kap. 19 § tredje stycket LEK). Definitionen av hemlig teleavlyssning omfattar därmed bl.a. innehållet i elektronisk post som befordras såväl före som efter rättens beslut. Det gäller även elektronisk post som har befordrats och som finns lagrad hos operatören på en server (e-postbrevlåda, se prop. 2002/03:74 s. 39). Även överföringar av datafiler med hjälp av t.ex. FTP (File Transfer Protocol) liksom överföringar från hemsi-

dor, nyhetsgrupper och chatkanaler är telemeddelanden som kan avlyssnas med hjälp av hemlig teleavlyssning. Genom hemlig teleövervakning är det möjligt för de brottsutredande myndigheterna att få uppgifter om telemeddelandena, t.ex. vilka e-postadresser som har varit aktuella vid kommunikationen.

9.3.2 Beslag

Bestämmelser om beslag finns i 27 kap. RB och i olika specialförfattningar. Objektet för beslag är enligt rättegångsbalken ”föremål”. Enligt huvudregeln i 27 kap. 1 § RB får föremål tas i beslag, om det skäligen kan antas ha betydelse för utredning om brott. Ett föremål får också tas i beslag om det skäligen kan antas ha frånhänts någon genom brott eller vara förverkat på grund av brott. Beslag får användas oberoende av brottets beskaffenhet och kan riktas mot såväl misstänkta som andra. Beslag får dock beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse.

Ett beslut om beslag anses innebära en rätt att även undersöka föremålet. Om undersökningen emellertid omfattar utrymmen eller åtgärder som det i normala fall krävs ett beslut om annat tvångsmedel för att få tillgång till, måste beslagsbeslutet kompletteras med ett sådant beslut. Om exempelvis en bil tas i beslag, krävs det alltså ett beslut om husrannsakan för att bilens innanmäte skall få undersökas (SOU 1995:47 s. 351). Likaså krävs det ett beslut om hemlig teleavlyssning för att de brottsutredande myndigheterna skall få ta del av innehållet i telemeddelanden som *inte* finns lagrade i en beslagtagen mobiltelefon. Dock lagras SMS-meddelanden i allmänhet i mottagarens telefon, liksom det avsända meddelandet lagras i avsändarens telefon.

I 27 kap. 1 § andra stycket RB anges att vad som stadgas om föremål i kapitlet, skall gälla även för skriftliga handlingar, om inte annat är föreskrivet. Avsikten med bestämmelsen är att förtydliga att skriftliga handlingar kan tas i beslag även när anledningen till beslaget är att skriftens innebörd är av betydelse som bevis, nämligen då som skriftligt bevis. Bestämmelser om skriftligt bevis finns i 38 kap. RB. Om en skriftlig handling åberopas som skriftligt bevis enligt de bestämmelserna är det handlingens skrivna tankeinnehåll, eller med andra ord skriftens innebörd som har bevisvärde. Skulle bevisvärdet hänföra sig till fingeravtryck på ett brev, papperskvali-

teten eller liknande, utgör detta inte något skriftligt bevis (Ekelöf, Rättegång 4 s. 169). Den skriftliga handlingen kan då i stället förebringas för syn enligt 39 kap. RB. Begreppet skriftlig handling i beslagskapitlet har alltså en direkt anknytning till bevisreglerna. Med ”skrift” i reglerna om skriftligt bevis avsågs ursprungligen språkliga tecken och siffror. I vilken form skriften förekommer, på papper eller t.ex. på en film eller ett fotografi, saknar betydelse (Gärde m.fl., Nya rättegångsbalken s. 526). Fitger menar att det i dag är tillräckligt att skriften finns på t.ex. magnetband, skiva, tråd eller liknande (Rättegångsbalken 3 s. 38:3).

Reglerna om beslag i 27 kap. RB är tillämpliga bara på den handling som har tagits i beslag, inte på de kopior som polisen eventuellt har tagit av handlingen (SOU 1995:47 s. 197). Därför kan det knappast sägas ha förekommit något beslag över huvud taget om polisen bara har skrivit av eller kopierat en upphittad handling eller kopierat en datafil som blivit tillgänglig genom husrannsakan. En annan sak är att den brottsutredande myndigheten, t.ex. om innehavaren av en dator protesterar, kan ha anledning att i stället ta en hårddisk i beslag och sedan genast återlämna en kopia av hårddisken. Genom att det då har skett ett beslag kan den enskilde begära att domstol prövar beslutet (27 kap. 6 § RB, se Fitger, Rättegångsbalken 2 s. 27:10 och 27:22, jfr NJA 1977 s. 573).

Det är med andra ord informationsbäraren som sådan som är ”föremålet”, dvs. objektet för beslag, också i de fall det är informationen som är av intresse, oavsett om informationen finns t.ex. i en hårddisk, på en datadiskett eller på en server.

Skriftliga handlingar får enligt 27 kap. 2 § RB inte tas i beslag om de kan antas innehålla uppgifter som ett vittne, t.ex. advokater, läkare och psykologer, med stöd av 36 kap. 5 § RB kan vägra att uttala sig om. Det gäller under förutsättning att handlingen innehas av den som omfattas av vittnesskyddsreglerna eller av den till vars förmån tystnadsplikten gäller. Förbudet mot att ta handlingar med uppgifter som motsvarar befrielse från vittnesplikten i beslag gäller enligt 27 kap. 2 § RB endast skriftliga handlingar. Begreppet föremål används alltså inte i bestämmelsen. I nu aktuellt avseende skulle alltså den teknik som används för att bevara uppgifterna, t.ex. traditionellt skriftliga handlingar jämfört med en datadiskett eller cd-skiva, kunna avgöra om beslagsförbudet i 27 kap. 2 § RB skall gälla.

Skriftliga meddelanden mellan den misstänkte och någon närstående till honom, eller meddelanden mellan sådana närstående, får inte tas i beslag, om meddelandet påträffas hos någon av dessa

personer (27 kap. 2 § RB). Beslagsförbudet gäller dock inte om utredningen avser brott för vilket det inte är föreskrivet lägre straff än fängelse i två år. I bestämmelsen talas inte om föremål eller skriftlig handling utan om skriftliga meddelanden. Om avsikten med bestämmelsen inte är att begreppet skriftligt meddelande skall omfatta andra upptagningsformer än pappershandlingar, kan det även i detta fall uppkomma en skillnad i skyddet beroende på vilken teknik som används för att framföra meddelandet.

I 27 kap. 3 § RB föreskrivs att brev, telegram eller andra försändelser som finns hos post- eller telebefordringsföretag får tas i beslag, om det för brottet är föreskrivet fängelse i ett år eller däröver. Bestämmelsen är tillämplig från det att en försändelse har lämnats in för befordran till dess att den har avlämnats till adressaten (Fitger, Rättegångsbalken 2 s. 27:14) och får tillämpas endast om försändelsen hade kunnat tas i beslag hos mottagaren. Är det fråga om försändelser i traditionell mening kan det föremålet givetvis tas i beslag enligt dessa regler. Det innebär också att om beslag är uteslutet på grund av vad som föreskrivs i 27 kap. 2 § RB får beslag inte ske enligt detta lagrum.

Det kan i sammanhanget nämnas att regeringen i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74 s. 45 f.) gjorde bedömningen att ”uppgifter om telemeddelanden” som finns *hos en operatör* inte kan hämtas in med stöd av reglerna om beslag. Bakgrunden till det ställningstagandet är att det har förekommit att de brottsutredande myndigheterna har använt tvångsmedlen husrannsakan och beslag eller editionsföreläggande för att få tillgång till uppgifter om telemeddelanden hos operatörer (se avsnitt 2.4.4).

I 27 kap. 9 § RB föreskrivs att rätten får förordna att en försändelse som kommer in till ett befordringsföretag skall hållas kvar till dess frågan om beslag är avgjord. Bestämmelsen avser att underlätta att ta försändelser i beslag. Föremålet för ett sådant förordnande kan, såsom i 27 kap. 3 § RB vara såväl ett paket som ett brev eller annan försändelse. Om beslag är uteslutet på grund av 27 kap. 2 § RB, får denna bestämmelse inte tillämpas.

I 27 kap. 12 § RB finns restriktioner om närmare undersökning av post- eller telegrafförsändelser, handelsböcker och andra enskilda handlingar, och om öppnande av brev och annan sluten handling. Bestämmelsen omfattar endast skriftliga handlingar och alltså inte försändelser av annat innehåll, t.ex. lösa föremål (Gärde m.fl., Nya rättegångsbalken s. 373). Bestämmelsen innebär att om ett brev eller t.ex. bokföringsmaterial tas i beslag, får endast rätten,

undersökningsledaren eller åklagaren eller en särskilt anlitad sakkunnig, t.ex. revisor, granska handlingen. Bestämmelsen är inte uttryckligen tillämplig när uppgifter motsvarande exempelvis handelsböcker eller traditionella telegrafförsändelser i stället finns på en informationsbärare som lagrat information optiskt eller magnetiskt, t.ex. en cd-skiva (se SOU 1995:47 s. 185). Elektronisk post som lagrats i en hårddisk omfattas inte heller av denna bestämmelse. Det torde numera höra till undantagen att handelsböcker av det slag som avses i 27 kap. 12 § RB finns i form av en traditionell skriftlig handling. Mer vanligt förekommande är att motsvarande uppgifter finns lagrade t.ex. i en dators hårddisk.

Den som har en skriftlig handling som kan antas ha betydelse som bevis är skyldig att förete den (38 kap. 2 § RB). Denna editionsplikt tar sikte på det tankemässiga innehållet i en handling, alltså på samma sätt som bestämmelserna om skriftligt bevis. Högsta domstolen har i ett avgörande konstaterat att ”det förhållandet att de aktuella uppgifterna är lagrade på data /utgör/ inte hinder att utskrifter avseende uppgifterna görs till föremål för edition” (NJA 1998 s. 829). Tingsrättens beslut innebar att ett säkerhetsföretag ålades att förete datautskrifter som innehöll utdrag från bolagets statuslogg avseende en viss larmanläggning. I tingsrättens skäl, till vilka hovrätten anslöt sig, anges att skriftlig handling i den mening som avses i 38 kap. 2 och 4 §§ RB inte utgörs endast av skrifter i traditionell mening, utan att det skall vara tillräckligt att uppgifterna finns t.ex. på film, magnetband eller datamedium.

Avgörandet får tolkas på så sätt att det i rättspraxis har godtagits att data, dvs. uppgifter som endast finns lagrade på datamedium, i sig kan vara föremål för edition (se Fitger, Rättegångsbalken 3 s. 38:3). I litteraturen har det ansetts att det genom rättsfallet klargjorts att datalagrad information kan tvingas fram med editionsföreläggande (Heuman i Juridisk Tidskrift 1999/2000 nr 1 s. 158). Avgörandet skulle också kunna tolkas så att Högsta domstolen ansett att en skriftlig handling enligt editionsreglerna även skulle kunna vara en s.k. potentiell handling, eller uppgifter som finns endast i form av data som lagrats i ett separat, elektroniskt dokument. Högsta domstolen har dock i beslutet anfört att det är utskrifterna som är föremålet för editionsbeslutet.

Föremål som kan antas ha betydelse som bevis, t.ex. skriftliga handlingar som inte är skriftliga bevis utan åberopas på grund av något annat än det tankemässiga innehållet, kan också bli föremål för edition, men då enligt bestämmelserna om syn i 39 kap. RB. I

39 kap. 5 § RB anges att vad som föreskrivs i 38 kap. 2 § RB skall gälla om det är fråga om att förete en skriftlig handling för syn.

I detta sammanhang nämns inte något om bestämmelserna rörande beslag i grundlagarna.

9.3.3 Husrannsakan

Om det förekommer anledning att brott har förövats, på vilket fängelse kan följa, får husrannsakan genomföras i hus, rum eller annat slutet förvaringsställe. Det får ske för att eftersöka föremål som är underkastade beslag eller för att utröna omständigheter som kan få betydelse för utredningen av ett brott (28 kap. 1 § RB). Det sagda innebär bl.a. att om föremålet omfattas av beslagsförbud (27 kap. 2 §) får husrannsakan inte genomföras för att söka efter föremålet. För husrannsakan hos den misstänkte krävs att denne är skäligen misstänkt. Husrannsakan får även företas hos annan om det finns synnerlig anledning att anta att det genom husrannsakan skall påträffas föremål som skall tas i beslag eller att annan utredning om brottet kan vinnas. Husrannsakan hos annan får också företas om brottet har förövats där eller om den misstänkte har gripits där.

Husrannsakan kan äga rum såväl i bostäder som på arbetsplatser och andra ställen. Några begränsningar i fråga om vilka lokaler som får genomsökas finns inte. Husrannsakan kan således, om förutsättningarna i övrigt är uppfyllda, göras var helst det finns t.ex. en dator (se beträffande lokaler även 28 kap. 3 § RB).

För husrannsakan gäller samma allmänna begränsning som för beslag, nämligen att husrannsakan får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse (28 kap. 3 a § RB).

Bestämmelserna om husrannsakan trädde i kraft långt före det att det var allmänt förekommande att enskilda, eller ens företag eller myndigheter hade tillgång till datorer. Det finns med andra ord inga särregler om undersökning av datorer. Under en husrannsakan kan det givetvis bli aktuellt att genomsöka en dator för att finna t.ex. elektroniska dokument. En sökning av information i persondatorer och hårddiskar får ske av företrädare för de brottsutredande myndigheterna vid en husrannsakan utan ytterligare beslut. Polisen anses alltså berättigad att under en husrannsakan söka efter information i en dator, lika väl som polisen kan läsa de handlingar som påträffas under husrannsakan (SOU 1995:47 s. 184).

9.4 Hemlig dataavläsning – ett nytt tvångsmedel

9.4.1 Hemlig dataavläsning införs som nytt tvångsmedel

Förslag: Hemlig dataavläsning skall införas som nytt tvångsmedel.

Med hemlig dataavläsning avses att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål.

Något om behovet av nya utredningsmetoder

I vårt betänkande Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74 s. 61 ff.) redogjorde vi särskilt för hoten från organiserad brottslighet och extremism och nämnde bl.a. vilka brottsområden där kriminaliteten ofta betraktas som organiserad: narkotikabrott inklusive smuggling av dopningsmedel och läkemedel, smuggling av alkohol och tobak, bedrägerier, ekonomisk brottslighet, illegal handel med stulna fordon, rån och stölder (inklusive häleri) bl.a. riktade mot åldringar, människosmuggling, utpressning, förfalskning, penningtvätt, mord, misshandel, olaglig vapenhandel och handel med kvinnor inklusive koppleri (se även slutrapporten från juni 2004 ”Organiserad kriminalitet, grov narkotikabrottslighet” av den nationella narkotikapolitiska samordningen Mobilisering mot narkotika, S 2002:03).

I Rikskriminalpolisens rapport Organiserad brottslighet i Sverige 2004 (RKP KUT rapport 2004:5c) framgår bl.a. följande. Totalt sett bedöms 98 grupperingar/nätverk vara involverade i organiserad brottslighet i Sverige. De flesta grupperingar består av färre än tio personer medan en del nätverk består av upp till 35 personer. EU:s definition av organiserad brottslighet bygger på elva kriterier, varav minst sex måste vara uppfyllda för att brottsligheten skall anses som organiserad. Kriterierna är följande (de första fyra är obligatoriska).

1. Samarbete med fler än två personer
2. Lång eller obegränsad utsträckning i tiden
3. Misstanke om allvarliga kriminella handlingar
4. Strävan efter vinning och/eller makt
5. Egna tilldelade uppgifter

6. Någon form av disciplin och kontroll
7. Verksamhet på internationell nivå
8. Användande av våld eller hot
9. Användande av affärsmässiga strukturer
10. Deltagande i penningtvätt
11. Otillbörlig påverkan

I Rikskriminalpolisens rapport utvecklas också vissa av den organiserade brottslighetens aktiviteter under följande rubriker.

1. Ekonomisk brottslighet – skattebrott (skalbolag, svart arbetskraft, handel med varor och tjänster inom EU, handel med livsmedel inom EU, handel med telefonkort inom EU och bilinförsel från annat EU-land)
2. Investeringsbedrägeri
3. Narkotika (smuggling och försäljning)
4. Smuggling av alkohol och tobak
5. Våld (i den brottsliga verksamheten, inom nätverket och mellan nätverk)
6. Olaglig invandring – människosmuggling
7. Illegala avfallstransporter
8. Handel med stulna fordon
9. Rån och stöld/tillgrepp
10. Vapen

Rikskriminalpolisen anger i rapporten att det är svårt att uttala sig om den geografiska spridningen av den organiserade brottsligheten i Sverige men konstaterar att den förekommer i hela landet med en koncentration till större städer i södra och mellersta Sverige. Det framgår också av rapporten att en betydande andel av grupperingarna har en internationell koppling. Majoriteten av medlemmarna i nätverken är både bosatta och aktiva i Sverige. Enstaka smugglingsnätverk är dock till största delen baserade i utlandet och verkar mot Sverige.

Rikskriminalpolisen har också givit ut rapporten Systemhotande brottslighet i Sverige 2004 (RKP KUT rapport 2004:9b). Av rapporten framgår att den organiserade brottslighetens systemhotande verksamheter är utpressning och korruption för vinning samt systematisk påverkan på myndigheter, rättskedjan och media för att skydda gruppen. Av rapporten framgår också följande. I dagsläget är utpressning mot det lokala näringslivet och mot privatpersoner en etablerad och omfattande verksamhet bland vissa grupper. Kor-

ruption är ett problem under uppsegling. Påtryckningar i form av våld och hot mot myndighetspersoner inom rättskedjan liksom mot målsägande och vittnen är satt i system. I det systemhotande sammanhanget kan olika kategorier urskiljas, nämligen s.k. 1% MC-gäng och deras supportergäng, fängelsegäng och gängbildningar i förorter samt etniskt sammansatta ligor och nätverk.

Rikskriminalpolisen konstaterar också följande i den sist nämnda rapporten. Dagens organiserade brottslighet i Sverige är i högsta grad gränsöverskridande och en del av ett internationellt system. Även om endast omkring tio procent av de grupper som i dag är aktiva i Sverige huvudsakligen är hemmahörande i utlandet, har marknaden internationaliserats. Svenska kriminella grupper har möjlighet att göra storskaliga affärer över hela Europa. Även nya handelsvaror, som tobak, vapen, människor och miljöfarligt avfall, har utökat den organiserade brottslighetens verksamhetsområden. Pengar kan forslas genom utländska banksystem och den nya globala informationsteknologin utnyttjas för brottslig verksamhet.

I lagrådsremissen Hemlig avlyssning m.m. från april 2000 uttalade sig regeringen bl.a. om behovet av nya utredningsmetoder på följande sätt (s. 35 f.).

> Brottsligheten totalt sett har i och för sig inte ökat under senare år. Utvecklingen av den mer allvarliga brottsligheten är dock djupt oroande. Den är mer välorganiserad, utstuderad och tar sig allt mer farliga former. Vi har under senare år sett allt fler exempel på brottslighet som riktar sig direkt mot fundamenten för det civiliserade samhället – rättsordningen och de demokratiska institutionerna. Grovt våld och grova hot har riktats mot poliser, vittnen, politiker, fackföreningsledare och andra. Denna brottslighet är inte sprungen ur tillfälliga förvillelser utan är välorganiserad och bedrivs ofta i hägnet av mer eller mindre väl sammanhållna extremistiska nätverk.
>
> Också den internationella utvecklingen har bidragit till ett ökat hot från den allvarliga och organiserade brottsligheten. Öppnare gränser för människor och kapital kan utnyttjas för exempelvis grov narkotikabrottslighet och spritsmuggling i stor skala. Sådan brottslighet kan skapa enorma vinster för gärningsmännen. Priset får betalas av offren bl.a. i form av drogberoende och andra skador. Också för samhället i stort är brottslighet av detta slag farligt, inte minst eftersom den i sina spår genererar annan allvarlig brottslighet.

Det är en av de mest centrala uppgifterna för statsmakterna att skydda samhället och medborgarna mot allvarlig brottslighet. Om den tillåts breda ut sig drabbas inte bara offren utan tilltron till och förtroendet för hela rättsväsendet kan rubbas. Allvarliga brott måste därför i så stor utsträckning som det över huvud taget är möjligt klaras upp och beivras. Mot denna bakgrund är det också statsmakternas skyldighet att se till att de brottsutredande myndigheterna har tillräckliga medel och metoder för att effektivt kunna förebygga och beivra brott.

Förundersökning av sådan allvarlig brottslighet som nu nämnts ställer givetvis särskilda krav vad avser arbetsmetoder och liknande. Det finns vid dessa utredningar ofta förutsättningar för att använda hemliga tvångsmedel, såsom hemlig teleavlyssning och hemlig kameraövervakning. Även om dessa hjälpmedel är betydelsefulla hjälpmedel i kampen mot denna form av brottslighet kan det ifrågasättas om de i dag är tillräckliga. De kriminella anpassar sig till de arbetsmetoder polisen har. Den som planerar brott kan undvika att samtala om det i en telefon som kan avlyssnas och möten sker inte på öppna platser där t.ex. en dold kamera kan dokumentera händelseförloppet. Polis och åklagare är i stället beroende av annan bevisning, inte minst vittnen och målsäganden, för att binda en misstänkt till brottet. Det förekommer emellertid allt oftare att vittnen och målsägande inför rättegångar utsätts för våld och hot om våld. Muntlig bevisning är påverkbar genom hot och andra yttre påfrestningar till skillnad från teknisk bevisning i form av t.ex. en upptagning av ett samtal.

Europol redovisar varje år en rapport om organiserad brottslighet. Av rapporten från år 2003 (Eu Organized crime report, 2530-130 Europol) framgår följande (se slutrapporten Organiserad kriminalitet, grov narkotikabrottslighet s. 50 f.). Organiserad brottslighet är ett expanderande problem inom EU och utgör ett allvarligt hot mot unionen. Man blandar allt oftare svart och vit verksamhet, deltar i offentliga upphandlingar med prisdumpningar och tvättar pengar från brott på ett allt mer sofistikerat sätt. Narkotikahandel utgör en mycket viktig grundsten i den organiserade brottsligheten som finns i eller verkar mot Europa. Oaktat detta så ser man från alla medlemsländer att kriminella grupper arbetar inom flera områden, både geografiskt och med olika brottstyper t.ex. handel med droger, vapen, människor och stöldgods samt ekonomiska brott

och penningtvätt. Man gör i allt större utsträckning en risk- och vinstbedömning, dvs. minsta risk till största förtjänst. Internationaliseringen av de kriminella gruppernas verksamhet är mycket tydlig och man driver ofta sin kriminella verksamhet i strukturer som påminner om företag. Den organiserade brottsligheten är ofta organiserad i tre nivåer: strategisk, operativ och taktisk nivå. De olika nivåerna behöver inte finnas i samma land utan kan verka internationellt, dvs. huvudkontoret kan finns i ett land, produktionen i ett annat land och konsumenterna i ett tredje land. För att klara att kommunicera med varandra använder man ofta modern teknologi, såsom olika former av informationsutbyte via Internet, de olika mobiltelefonnäten och satellittelefoner.

Som har framgått har den allmänna internationaliseringen under senare år bl.a. medfört att den kvalificerade kriminaliteten har blivit alltmer gränsöverskridande till sin karaktär. Därigenom kan också förutsättningarna för de kriminella att operera i Sverige sägas ha blivit bättre. Att ingripa mot den brottsligheten är en synnerligen angelägen uppgift för de brottsbekämpande myndigheterna.

En viktig fråga i det sammanhanget rör IT och särskilt Internetanvändning (se slutrapporten Organiserad kriminalitet, grov narkotikabrottslighet s. 52 f.). Användningen av den tekniken har ökat kraftigt de senaste åren och allt talar för att denna utveckling fortsätter. Man skulle kunna säga att vi i dag lever i ett genomdatoriserat samhälle. En sådan utveckling får i högsta grad konsekvenser för brott och brottsbekämpning.

Internet fungerar som en viktig informationskälla och som en global mötesplats, där man i olika miljöer kan knyta kontakt med andra personer. Det är således numera utan tvekan så att den organiserade brottsligheten söker sig till mer ”säkra” kommunikationsformer än telefoner och utnyttjar modern teknik och använder IT som ett effektivt arbetsredskap i verksamheten. Det förekommer också att de personer som begår mindre kvalificerade brott tar den tekniken till hjälp. Utvecklingen kommer att fortsätta i samma takt som medborgarnas och då även de kriminellas kompetens i IT-frågor ökar.

I Internetsammanhang använder de kriminella både öppna miljöer, som är tillgängliga för vem som helst, och mer slutna miljöer, till vilka bara ett begränsat antal personer har tillträde. I vissa av dessa miljöer träffas samma personer regelbundet för att utbyta information. En viktig omständighet som ökar Internets attraktionskraft i dessa sammanhang är möjligheten att kommunicera på ett relativt anonymt och säkert sätt. Anonymiteten och säkerheten

(främst frågan om kryptering) är vid sidan av globaliseringen och mobiliteten stora utmaningar som den IT-relaterade brottsligheten ställer upp för rättsväsendet.

Om den kvalificerade brottsligheten med dess struktur, inriktning och tillvägagångssätt skall kunna bekämpas, är det helt nödvändigt att de brottsbekämpande myndigheterna bl.a. har möjlighet att använda effektiva arbetsmetoder, inte minst med anknytning till IT. Det är inte vår uppgift att göra en översyn av hela straff- och processrätten och bedöma om och i så fall på vilket sätt bestämmelserna behöver anpassas till informationstekniken. Däremot har vi mot den angivna bakgrunden och vårt uppdrag i stort ansett att det är mycket angeläget att se på frågan om att införa bestämmelser om dataavläsning i svensk rätt efter den modell som finns i Danmark. Metoden kan i flera andra länder i Europa användas inom ramen för respektive lands motsvarighet till tvångsmedlet hemlig teleavlyssning.

Vad skulle dataavläsning innebära?

Som utvecklas nedan är bakgrunden till en diskussion kring dataavläsning de mycket stora svårigheter som finns i brottsutredningar med krypterad information och liknande i datorer och det faktum att det är lätt att vara anonym vid användning av informationsteknik. Dataavläsning som metod kan innebära att de brottsbekämpande myndigheterna i hemlighet sänder en viss mjukvara till en dator. Den mjukvaran, en s.k. programkod, ger sedan myndigheterna uppgifter om vilken information som finns i datorn och hur datorn används. Myndigheterna kan alltså läsa av informationen, t.ex. innan den förs vidare via trådbunden eller trådlös förbindelse. Vilken information det är fråga om i det enskilda fallet och hur informationen skall levereras till myndigheten beror på vad myndigheten har bestämt vid utformningen av mjukvaran. Det är alltså möjligt att i viss utsträckning precisera och begränsa vilken information man vill ha uppgift om och om informationen skall skickas till myndigheten via radio, över Internet eller t.ex. lagras på olika sätt i datorn för att sedan tas ut vid exempelvis framtida husrannsakan och beslag. Dataavläsning kan också innebära att hård- eller mjukvara med liknande funktion placeras i den informationsbärande utrustningen genom ett fysiskt ingrepp, t.ex. vid ett hemligt intrång i en persons bostad eller på dennes arbetsplats.

Vilket behov finns av dataavläsning och framstår metoden som effektiv?

En första grundläggande förutsättning för att ge de brottsbekämpande myndigheterna möjlighet att använda dataavläsning är att det kan presenteras ett påtagligt behov av åtgärden och att metoden framstår som effektiv.

Bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning har funnits under lång tid. Under den tiden har teknikutvecklingen varit oerhört kraftig och mycket snabb. Det är självklart att de allra senaste nyheterna på teknikområdet utnyttjas som verktyg i särskilt grov brottslig verksamhet. Det är helt nödvändigt för samhället att myndigheterna inte hamnar hjälplöst efter utan, inom ramen för att ett godtagbart integritetsintrång, får rätt att använda brottsutredande metoder som är effektiva och anpassade till den tekniska situation som råder vid varje givet tillfälle. Frågan om att införa dataavläsning måste alltså ses i ljuset av den pågående teknikutvecklingen och särskilt de grovt kriminellas förmåga att hela tiden ”ligga i framkant” och utnyttja allt mer ”säkra” kommunikationsformer och modern teknik i sin verksamhet.

Det största behovet av dataavläsning finns vid brottslighet som innehåller organisation och planering. Särskilt vid organiserad eller annan allvarlig brottslighet är ofta vissa av de deltagande personerna utomordentligt skickliga i användningen av datorer. De utnyttjar sina kunskaper fullt ut för att genom olika åtgärder via datorerna gömma information, hålla sig anonyma och undgå upptäckt.

Den snabba tekniska utvecklingen medför att det i dagsläget finns stora problem i brottsutredningar med att få fram uppgifter ur datorer eller avlyssna meddelanden mellan datorer. Det gäller särkilt när den informationen är skyddad av kryptering eller när program används som på annat sätt döljer information. I ett ständigt ökande antal brottsutredningar påträffas krypterad information i form av enskilda filer eller i en viss yta av lagringsutrymmet (exempelvis en dators hårddisk).

Mycket kortfattat kan följande nämnas om kryptering. Ett sätt att förhindra obehöriga från att läsa ett meddelande är att förvanska klartexten så att endast en behörig person kan läsa den. Det kallas att kryptera klartexten och man får då en s.k. kryptotext. En krypteringsalgoritm kan liknas vid ett recept på hur man skall förvanska en klartext. Ett sådant recept kan ha många varianter eller s.k. nycklar. Om två personer skall kommunicera måste de komma överens om både algoritm och nyckel. Nyckeln håller man hemlig

men inte nödvändigtvis algoritmen. När en person vet både algoritm och nyckel, kan denne omvandla kryptotext till klartext. Det kallas för att dekryptera kryptotexten. En kryptotext kan bland annat forceras genom att olika nycklar prövas till dess att klartexten hittas. Ett nödvändigt villkor för att en algoritm skall kunna skyddas mot insyn är att det finns många nycklar till algoritmen. Om det t.ex. endast finns tio nycklar, är det lätt att dekryptera kryptotexten med de tio möjliga nycklarna och på det sättet hitta det riktiga meddelandet. Dekrypteras meddelandet manuellt kanske det räcker med några tusen nycklar för att det skall bli omöjligt att dekryptera alla möjliga meddelanden inom rimlig tid. När som i dagsläget datorer används för förmedling av information och för kryptering och dekryptering måste antalet nycklar vara nästan ofattbart många. Som exempel kan nämnas att för snart tio år sedan hade den kanske mest kända algoritmen omkring 72.058.000 miljarder nycklar.

Det är välkänt bland kriminella vilka arbetsmetoder polisen har och inte har och den kunskapen utnyttjas för att göra den brottsliga verksamheten så effektiv som möjligt. Problemen accelererar i och med att användarvänligheten i kryptosystem och liknande ökar. Programapplikationer för den enskilde datoranvändaren finns i dag både till försäljning och tillgängliga för att ladda ner kostnadsfritt från Internet. Exempel på kommersiella program är PGP (Pretty Good Privacy) och BestCrypt. Kremlin är ett exempel på gratisprogram. Dessutom utvecklas fortlöpande nya, än mer avancerade program. Vanliga standardprodukter levereras i dag i stor omfattning med funktioner för kryptering, som också används som en marknadsföringsåtgärd av företag som tillhandahåller kommunikationstjänster via Internet för att kunden skall garanteras fullgod informationssäkerhet. Det finns en kraftigt ökande medvetenhet hos allmänheten om möjligheten att skydda sig från ”insyn” genom t.ex. krypteringsprogram. Många företag ser t.ex. kryptering som en nödvändighet i konkurrensen med andra företag.

I informationsbärande utrustning bearbetar användaren informationen ”öppet” innan den sparas och eventuellt krypteras. Kryptering i samband med kommunikation kan ske dels genom att operatören skyddar överföringen genom att kryptera den, dels genom att användaren själv krypterar, vilket kan ske oavsett om operatören gör det eller inte. För att de brottsbekämpande myndigheterna skall kunna få fram och förstå den annars krypterade informationen krävs att den, av någon anledning, finns även i klartext eller att myndigheten får tillgång endera till datorn när krypteringen är

”upplåst” eller till det hemliga lösenord och/eller de PIN-koder som används som krypteringsnycklar eller som ger åtkomst till krypteringsnycklar. Att detta sker är mycket ovanligt i dagsläget. I några få fall har krypteringen dock kunnat forceras när krypterad information har påträffats i beslagtagna datorer (i form av enskilda filer eller utrymmen på hårddisken).

Även om det saknas statistik på området kan det konstateras att den utbredda användningen av krypteringsprogram och andra program för att dölja information leder till att det är mer regel än undantag att de brottsbekämpande myndigheterna inte får tillgång till information som finns i datorer i utredningar rörande kvalificerad brottslighet. Det finns program som är konstruerade så att de t.ex. raderar information vid en viss tidpunkt och program som har dold information till vissa personer i annan öppen information. Det finns också möjlighet för personer att ha ”ospårbara” kontakter via datorer i tillfälliga nätverk.

En användning av dataavläsning skulle innebära att de brottsbekämpande myndigheterna skulle ha betydligt lättare att komma runt problemet med krypterad information och andra liknande tillvägagångssätt och därmed få framgång i utredningar.

Hemlig teleavlyssning används i brottsutredningar för att få tillgång till innehållet i ett telemeddelande. Den metoden kan inte användas för dekryptering utan fångar enbart upp de krypterade meddelandena. Det gäller såväl elektronisk post, medsända filer som exempelvis Internettelefoni (Voice over IP – VoIP). För att få tillgång till innehållet okrypterat behöver informationen fångas upp redan i den dator eller annan anordning som används för uppkoppling mot Internet.

Ett annat och minst lika stort problem är möjligheten för dem som agerar i brottsliga syften att vara anonyma vid användning av informationsteknik. Enligt uppgift från Rikskriminalpolisen är t.ex. avsaknad av en skäligen misstänkt person det normala utgångsläget i utredningar av Internetrelaterad brottslighet. Det är möjligt för de brottsbekämpande myndigheterna att knyta ett handlande på Internet till en viss IP-adress och även få uppgift från operatören om vilket abonnemang som kan knytas till den IP-adressen vid en viss tidpunkt. En uppgift om abonnemanget säger dock ingenting säkert om vem som satt vid datorn och agerade vid den aktuella tidpunkten. En användning av dataavläsning skulle innebära att de brottsbekämpande myndigheterna kan identifiera personen genom andra ageranden på Internet.

Med anledning av de kriminella personernas allt mer avancerade sätt att utnyttja modern teknik och den snabba tekniska utvecklingen står det klart att de brottsbekämpande myndigheterna, som ett mycket värdefullt komplement till de övriga tvångsmedlen, behöver ha möjlighet att genomföra de åtgärder som dataavläsning innebär. Det finns knappast några alternativa sätt att få fram den gömda informationen på. Enligt uppgift används motsvarande tillvägagångssätt av brottsbekämpande myndigheter i vissa länder standardmässigt inför exempelvis husrannsakningar, eftersom myndigheterna annars bedömer sig vara chanslösa inför den grövre brottslighetens metoder.

Polisen har av operativa skäl inte velat lämna ut allt för detaljerad information om utredningar där krypterad information har påträffats. För att ändå peka på några av de brott och brottstyper där polisen har påträffat krypterad information kan följande enstaka exempel nämnas.

- ✓ Under hösten 1999 sköts en person till döds utanför sin bostad. Tre män med nazistiska sympatier greps. I en av de senare dömdas datorer påträffades en krypterad del av datorns hårddisk.
- ✓ I samband med de s.k. Göteborgskravallerna vid EU-toppmötet år 2001 gjordes ett tillslag mot den s.k. sambandscentralen som drevs av ett dussintal personer. Från centralen upplystes personer som befann sig i centrala Göteborg, där kravallerna pågick, om polisens rörelser. Det skedde via dator och SMS-meddelanden. I en dator som beslagtogs påträffades två krypterade delar av hårddisken.
- ✓ I ett fall med omfattande försäljning av narkotika hittade polisen ett antal krypterade filer med anknytning till ”affärsverksamheten”.
- ✓ I ett nätverk av pedofiler laddades mängder av barnpornografi till en gemensam area på Internet. Man skickade sedan länkar till de servrar där materialet, som var krypterat flera gånger, fanns. Barnpornografiska filmer delades inte sällan upp i ett antal olika paket och varje paket krypterades sedan med Kremlin eller PGP eller med båda programmen.
- ✓ En för bedrägeri misstänkt person var anställd i ett större industriföretag och brotten hade utförts med hjälp av en dator som tillhandahölls av arbetsgivaren. Datorn var försedd med ett krypteringsskydd på s.k. BIOS-nivå, dvs. all

information på hårddisken var krypterad och kunde bara öppnas med rätt lösenord.

Att verkställa ett beslut om dataavläsning kan visserligen vara förenat med praktiska och tekniska problem. Av stor betydelse i sammanhanget är emellertid att det står klart att dataavläsning i många fall kan leda till att avgörande omständigheter kommer fram och att betydelsefull bevisning säkras i kvalificerade brottsutredningar. Om dataavläsning i det enskilda fallet används effektivt medför det utan tvekan en ökad möjlighet att fler brottsutredningar leder till åtal och fällande dom. Det finns också anledning att framhålla att dataavläsning i många fall kräver en del förberedelseinsatser, vilket talar för att metoden endast skulle användas i de fall de brottsbekämpande myndigheterna är övertygade om att avläsningen kommer att tillföra viktig information. I stort sett finns den utrustning och kunskap som behövs tillgänglig för de brottsbekämpande myndigheterna.

Även om det inte har gått att få några precisa uppgifter om tillämpningen av dataavläsning i Danmark, är alla som vi har talat med helt överens om att rätt använd i det enskilda fallet skulle metoden innebära ett effektivt medel i brottsbekämpningen. Det överensstämmer helt med vår bedömning. Hur metoden bör genomföras på det mest effektiva sättet, t.ex. i valet mellan hård- och mjukvara, blir givetvis beroende av omständigheterna i det enskilda fallet. Vi har fått uppgifter om effektiviteten i olika avseenden med kan av sekretesskäl inte redogöra för dessa. Användning av dataavläsning innebär, precis som för de befintliga hemliga tvångsmedlen, alltid en risk för att verkställigheten röjs. Vi har fått beskrivet även vilka röjningsrisker som finns och sätten att reducera dessa. Inte heller i den delen går det att avslöja några detaljer. Det går ändå att konstatera att de riskerna inte alls är så framträdande att det påverkar effektiviteten i sådan grad att det finns avgörande skäl mot att metoden införs.

Att hemlig teleavlyssning och hemlig teleövervakning i och för sig fortfarande är värdefulla och framgångsrika hjälpmedel i kampen mot den grova brottsligheten framgår bl.a. av regeringens skrivelse 2004/05:36.

Ger intresset av att upprätthålla ett starkt skydd för den personliga integriteten utrymme för att tillåta dataavläsning?

Även om vi har funnit att det finns ett stort behov av dataavläsning som brottsbekämpande metod och att metoden är effektiv, återstår det att överväga om metoden kan motiveras från integritetssynpunkt.

Det är en svår uppgift att avväga integritetsintresset (se vidare avsnitt 2.8) mot nödvändigheten av att myndigheterna har effektiva metoder för bl.a. brottsutredning. Det ligger i sakens natur att varje tvångsmedel innefattar ett integritetsintrång. Samtidigt måste beaktas att detta intrång ofta är blygsamt i jämförelse med den kränkning som offren för den allvarliga brottsligheten måste utstå. Ju allvarligare och ju mer svårutredd som brottsligheten blir, desto mer tvingas statsmakterna tillåta i form av tvångsåtgärder i brottsbekämpningen. Det kan aldrig accepteras att brottsligheten tar överhanden och att statsmakterna kapitulerar inför utvecklingen av en allt mer avancerad och förslagen brottslighet.

Dataavläsning innebär som framgått att det alltid måste ske ett visst intrång för att genomföra åtgärden. Intrånget kan endera bestå i att de brottsbekämpande myndigheterna i hemlighet sänder en viss mjukvara till en dator. Den mjukvaran ger sedan myndigheterna information i olika avseenden om vad som finns i datorn och hur datorn används. Dataavläsning kan också innebära att hård- eller mjukvara med samma funktion placeras i datautrustningen genom ett fysiskt ingrepp, t.ex. vid ett hemligt intrång i en persons bostad eller på dennes arbetsplats.

Varje tvångsmedelsanvändning medför ett ingrepp i den enskildes integritet och det kan naturligtvis diskuteras vilket av de nuvarande tvångsmedlen som innefattar de största riskerna för den personliga integriteten. De allmänt sett mest kännbara tvångsmedlen från integritetssynpunkt bör dock anses vara hemlig teleavlyssning och hemlig kameraövervakning. Regeringen uttalade bl.a. följande i propositionen Hemlig kameraövervakning (prop. 1995/96:85 s. 22).

> Hemlig teleavlyssning och användning av dolda övervakningskameror företer stora likheter även med avseende på omfattningen av det intrång i den personliga integriteten som kan bli följden av tvångsmedelsanvändningen. Enligt regeringens mening kan övervakning med dold övervakningskamera i vissa situationer vara ett väl så ingripande tvångsmedel

som hemlig teleavlyssning. Om t.ex. kameran riktas mot ett fönster i en bostad och därigenom registrerar vad som försiggår i någons hem kan detta uppfattas som ett minst lika stort intrång som om någons telefon avlyssnas. Om en kamera installeras utanför ett politiskt partis lokaler, ett hotell som frekventeras av prostituerade eller en porrklubb torde tvångsmedlet från integritetssynpunkt kunna jämställas med hemlig teleavlyssning. Genom avlyssning kan innehållet i ett samtal, och därigenom en persons åsikter m.m., dokumenteras i sin helhet men en övervakningskamera kan registrera ett snabbt och omfattande händelseförlopp, vilket i efterhand kan granskas i detalj. I båda fallen är dokumentationen sådan att den i regel inte kan ifrågasättas. Vidare är den genomslagskraft som en bild har när den når offentligheten oomstridd. Regeringen delar utredningens uppfattning att enskilda personer – i t.ex. sådana situationer som har berörts i det föregående – i allmänhet kan uppfatta det som lika besvärande om informationen finns bevarad på film som om det finns en ljudupptagning bevarad.

Omfattningen av det integritetsintrång som skulle bli följden om dataavläsning användes kan vara svår att uppskatta generellt och blir naturligtvis beroende av omständigheterna i det enskilda fallet. I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte kommer att bli större än vid hemlig teleavlyssning och hemlig kameraövervakning, där samtal avlyssnas och personen är föremål för övervakning genom fjärrstyrda kameror. De sistnämnda tvångsmedlen bör i de flesta fall anses innefatta en mer total kontroll av och insyn i en persons förehavanden än vad dataavläsning innebär. Dessutom bör det i de fallen typiskt sett finnas en större risk för att personer som är ovidkommande för en brottsutredning drabbas av ett integritetsintrång genom att de t.ex. blir avlyssnade vid en telefonkontakt med en misstänkt person eller blir filmade på en plats där kameraövervakning pågår. Det kan tilläggas dels att ett hemligt intrång i en persons bostad eller på en arbetsplats för att placera den utrustning som krävs för dataavläsning inte kan anses mer integritetskänsligt än en s.k. hemlig husrannsakan (se 28 kap. 7 § andra stycket RB), dels att ett samtidigt verkställande av flera tvångsmedel mot samma person givetvis leder till att integritetsintrånget ökar avsevärt, något som måste beaktas när beslut skall fattas om metoden och under verkställigheten av tvångsmedlen.

Bör dataavläsning införas som nytt tvångsmedel?

Av vad som nyss har redovisats framgår att det finns ett stort behov av att kunna använda dataavläsning för vissa fall i den brottsbekämpande verksamheten. Ofta rör det situationer där det i princip inte finns någon möjlighet att på annat sätt skaffa fram avgörande uppgifter och bevisning rörande grova brott. Det är mycket angeläget att de brottsbekämpande myndigheterna får rätt att använda moderna tekniska metoder för att kunna bekämpa t.ex. den grova narkotikabrottsligheten och annan allvarlig brottslighet. Som också har framgått av de uppgifter vi har, framstår metoden som effektiv.

Samtidigt råder det inget tvivel om att en användning av dataavläsning innebär ett integritetsintrång. Med hänsyn till vad som har redovisats rörande behovet och effektiviteten av dataavläsning är det dock enligt vår mening klarlagt att det skulle innebära en så stor vinst för bekämpningen av den allvarliga brottsligheten att det inte är försvarligt att avstå från att införa en möjlighet för de brottsbekämpande myndigheterna att använda metoden. Det integritetsintrång som typiskt sett uppkommer vid användning av dataavläsning är alltså med hänsyn till vad som redovisades tidigare inte så stort att det får hindra en lagstiftning på området.

Vi lägger därför fram förslag om dataavläsning som nytt straffprocessuellt tvångsmedel och benämner detta hemlig dataavläsning. Med hemlig dataavläsning bör avses att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel.

En reglering av användning av hemlig dataavläsning måste omgärdas av sådana rättssäkerhetsgarantier som säkerställer att bestämmelserna inte kan missbrukas och att allmänheten kan ha tilltro till de myndigheter som tillämpar regleringen. Tvångsmedelsregleringen måste omgärdas av tydliga och strikta ramar för att det inte skall kunna misstänkas att regelsystemet kommer att utnyttjas utöver vad det skall tillåta. Bestämmelserna måste även utformas på ett sådant sätt att de kan accepteras av allmänheten som ett nödvändigt redskap för de brottsbekämpande myndigheterna i kampen mot den grövre kriminaliteten. Regleringen måste också innefatta ett starkt skydd för den personliga integriteten. Det är av avgörande betydelse att undvika att personer som är ovidkommande för en brottsutredning får sin integritet kränkt. Det är också viktigt att i möjligaste mån begränsa det integritetsintrång som den misstänkte utsätts för.

Det är självklart att hemlig dataavläsning som ett straffprocessuellt tvångsmedel skall användas under förundersökning. En särskild fråga är om tvångsmedlet även bör kunna användas på ett tidigare stadium, alltså innan en förundersökning har inletts, under vad som kan betecknas som ett spaningsstadium eller i kriminalunderrättelseverksamhet. Behovet av att kunna använda tvångsmedel i ett sådant mer preventivt syfte, alltså inte enbart för att utreda brott utan även för att förhindra brott, har framförts till regeringen i olika sammanhang (se t.ex. SOU 2002:87 s. 386). Behovet har främst rört Säkerhetspolisens område. Frågan om att eventuellt tillåta en mer preventiv användning av de nuvarande tvångsmedlen bereds för närvarande inom Justitiedepartementet. Vi avstår därför från att behandla frågan om användning av hemlig dataavläsning utanför en förundersökningssituation (se dock avsnitt 9.4.13 rörande lagen om särskild utlänningskontroll). En annan sak är att användningen av hemlig dataavläsning i vissa fall kan leda till att brottet inte kommer till fullbordan. På det sättet får dataavläsningen en preventiv bieffekt, som i det enskilda fallet kan vara av stort värde (jfr prop. 1988/89:124 s. 42 och prop. 1995/96:85 s. 26 f.).

I den referensgrupp som är knuten till beredningen har samtliga ledamöter anslutit sig till förslaget att införa tvångsmedlet hemlig dataavläsning. I några enskildheter finns dock olika meningar inom referensgruppen. Till det återkommer vi nedan (se avsnitten 9.4.3, 9.4.4 och 9.4.9 rörande underrättelseskyldighet i efterhand, den s.k. straffvärdeprincipen och rätten till tillträde).

9.4.2 Lagteknisk lösning

Förslag: Bestämmelser om hemlig dataavläsning skall tas in i en ny lag, vars giltighetstid till en början begränsas till fem år.

Förslaget om hemlig dataavläsning innebär att ett nytt tvångsmedel införs där bl.a. ny teknik kommer att användas i brottsutredningar. Det kan konstateras att det finns ett stort behov av metoden och att den framstår som effektiv. Närmare detaljer i de frågorna är inte helt enkla att bedöma innan tvångsmedlet har tillämpats under en tid. Därför bör lagstiftningen om hemlig dataavläsning, i vart fall till en början, vara tidsbegränsad. De nya bestämmelserna bör därför inte tas in i rättegångsbalken utan i en särskild lag. Utformningen av bestämmelserna bör i så stor utsträckning som möjligt ansluta till den reglering som finns i dag rörande hemlig teleavlyss-

ning och hemlig kameraövervakning. Tillämpningsområdet bör vara utformat så att tvångsmedlet används endast vid misstanke om grov brottslighet (se avsnitt 9.4.4). Det innebär att hemlig dataavläsning inte kommer att kunna användas i ett större antal fall. För att det senare skall finnas ett fullgott underlag för en utvärdering av bestämmelserna och för en bedömning av frågan om lagen bör ges förlängd giltighetstid eller t.ex. permanentas, bör lagens giltighetstid sättas något längre än vad som annars hittills skett, t.ex. i fråga om lagen om hemlig kameraövervakning. Till det kommer att de brottsutredande myndigheterna behöver viss tid för att utarbeta metoder och verktyg för genomförandet. Vi bedömer att giltighetstiden till en början bör vara i vart fall fem år.

9.4.3 Domstolsprövning och offentliga ombud

Förslag: Domstol skall pröva frågor om hemlig dataavläsning på ansökan av åklagaren.

Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig dataavläsning.

I tvångsmedelssammanhang är det viktigt att skapa fullgoda rättsskyddsgarantier. Vi har berört dessa frågor på flera ställen i betänkandet (se t.ex. avsnitt 2.8). Frågan har också tagits upp i den referensgrupp som är knuten till vårt arbete. Att det finns kontrollmekanismer i form av medverkan av domstol och offentliga ombud är av central betydelse vid användning av de mest integritetskänsliga tvångsmedlen. Allmänt sett kan det också diskuteras metoder för kontroll i efterhand, alltså i första hand underrättelseskyldighet mot den enskilde. Den frågan diskuterades av Buggningsutredningen (SOU 1998:46 s. 427 ff.) och i den efterföljande lagrådsremissen (s. 102 ff.). I båda sammanhangen drogs den slutsatsen att övervägande skäl talade mot att föreslå en sådan regel men att frågan borde övervägas på nytt i annat sammanhang. Vi har bedömt att det inte är aktuellt att överväga frågan nu, utan att det får ske i ett annat sammanhang än i detta betänkande.

En ledamot i den referensgrupp som är knuten till beredningen har ansett att det som i Danmark bör finnas en skyldighet att i efterhand underrätta den som har varit föremål för tvångsmedelsanvändningen om att den har ägt rum samt att den personen skall ha möjlighet att vid icke fällande dom erhålla skadestånd i likhet med vad som gäller vid frihetsberövanden.

Det är domstolen som i dag fattar beslut om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Det är som sagt angeläget att skapa fullgoda rättsskyddsgarantier även när det gäller användning av hemlig dataavläsning. Rätten att besluta om ett tvångsmedel är då av central betydelse. Liksom för de andra nämnda tvångsmedlen är det mindre lämpligt att överlåta den rätten till de myndigheter som skall verkställa besluten respektive leda de aktuella förundersökningarna. Beslutanderätten bör därför ligga på domstol också för hemlig dataavläsning. Besluten kommer då att fattas av det organ som är så fristående från förundersökningen som möjligt. Ansökan till tingsrätten om tillstånd till åtgärden får göras av åklagaren.

Principerna om rollfördelningen mellan domstol och åklagare gör sig inte gällande när ett tvångsmedelsbeslut skall hävas. I likhet med vad som gäller i liknande fall bör åklagaren kunna häva ett beslut om tillstånd till hemlig dataavläsning om det inte längre finns skäl för det. Samma skyldighet bör gälla för domstolen.

Sedan den 1 oktober 2004 gäller att offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig teleavlyssning och hemlig kameraövervakning (27 kap. 26-30 §§ RB och 4 § lagen om hemlig kameraövervakning samt prop. 2002/03:74). Hemlig dataavläsning är precis som hemlig teleavlyssning och hemlig kameraövervakning ett integritetskänsligt tvångsmedel. Även i sådana ärenden bör därför ett offentligt ombud medverka vid domstolen för att bevaka enskildas integritetsintressen.

Vi föreslår i avsnitt 4.2 att skyldigheten enligt lagen om elektronisk kommunikation för operatörer att i vissa fall lämna ut uppgifter som angår ett särskilt elektroniskt meddelande till brottsutredande myndighet skall upphävas. De brottsutredande myndigheternas tillgång till uppgifterna skall uteslutande regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning. Som en följd av det förslaget kom vi i avsnitt 4.3 fram till att det behöver finnas en möjlighet för åklagare att i brådskande fall fatta vissa interimistiska beslut om tvångsmedel.

Vi har övervägt frågan om att ge åklagare rätt att i sådana situationer fatta beslut även om hemlig dataavläsning. Ibland kan det enda sättet att använda tvångsmedlet vara att sända en mjukvara till en dator när personen använder Internet. Det kan t.ex. vara oklart var datorn rent fysiskt befinner sig eller så är ett hemligt intrång inte möjligt av andra skäl. Har polisen fått tips om en omedelbart förestående narkotikaaffär på Internet skulle många gånger den enda möjligheten att få fram bevisning vara att omgående sända

mjukvaran till den aktuella datorn. Att invänta ett domstolsbeslut i sådana situationer kan leda till att bevisningen går förlorad.

Som framgår av redogörelsen i avsnitt 4.3 rörande de tidigare överväganden som varit om åklagares rätt att fatta interimistiska beslut om tvångsmedel, bör det i princip krävas att det presenteras ett påtagligt behov av en sådan möjlighet innan den införs. Vi har full förståelse för att det kan uppkomma situationer med anknytning till hemlig dataavläsning som kräver omedelbara åtgärder från de brottsutredande myndigheternas sida, för att inte avgörande bevisning skall gå förlorad. Hemlig dataavläsning är dock ett integritetskänsligt tvångsmedel som det i dagsläget dessutom finns relativt begränsad erfarenhet av. Det är svårt att uttala sig om hur påtagligt behovet kommer att bli av sådana åklagarbeslut. Vi har därför kommit fram till att inte föreslå en rätt för åklagare att fatta interimistiska beslut om hemlig dataavläsning. Behovet av en sådan ordning får belysas efter att de brottsutredande myndigheterna har tillämpat tvångsmedlet under en tid.

Vi hänvisar till avsnitt 9.4.13 när det gäller möjligheten för åklagare att fatta beslut enligt bl.a. 1952 års tvångsmedelslag.

9.4.4 Vid vilka brott skall hemlig dataavläsning få äga rum?

Förslag: Hemlig dataavläsning skall få äga rum vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff,
3. brott enligt 4 kap. 9 c § brottsbalken (dataintrång), brott enligt 16 kap. 8 § brottsbalken som inte är att anse som ringa (hets mot folkgrupp), brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa (barnpornografibrott), eller
4. annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år.

Hemlig dataavläsning skall få användas av brottsutredande myndigheter under en förundersökning. I dag får hemlig teleavlyssning och hemlig kameraövervakning användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år samt när det är fråga om försök, förberedelse eller stämpling till sådant brott, om gärningen är belagd med straff. Tvångsmedlen

får sedan den 1 oktober 2004 användas även vid annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år (en s.k. straffvärdeventil, se 27 kap. 18 § RB och 2 § lagen om hemlig kameraövervakning).

Hemlig dataavläsning är främst avsedd att användas mot den grova brottsligheten. Utgångspunkten är därför att enbart de allvarligaste brotten bör omfattas av tillämpningsområdet. Vid utformningen av regler för när hemlig dataavläsning skall få äga rum finns det med hänsyn till den integritetskänsliga karaktären skäl att vara i princip lika restriktiv som vid hemlig teleavlyssning och hemlig kameraövervakning (jfr dock nedan rörande bl.a. barnpornografibrott).

Givetvis kan graden av integritetsintrång variera mycket beroende på bl.a. vilket informationssystem som dataavläsning skall avse, vilken information som de brottsutredande myndigheterna vill få ut av metoden och hur tvångsmedlet kommer att drabba tredje man. Därför kan det diskuteras om kravet på brott av viss svårhet skall ställas i relation till hur dataavläsningen är tänkt att gå till. Det är dock svårt att förutsäga vilken grad av intrång i den personliga integriteten som kan bli följden av att dataavläsning används. Detta gäller oavsett hur avläsningen utförs. Det finns också risk för att det uppstår praktiska svårigheter och att regleringen blir otydlig och svår att tillämpa. På grund av detta och då bestämmelserna om hemlig teleavlyssning och hemlig kameraövervakning inte innehåller någon differentiering av straffskalorna i förhållande till det tänkta integritetsintrånget, avstår vi från att lägga fram något sådant förslag (jfr prop. 1995/96:85 s. 24).

Det är lämpligt att regleringen för när hemlig dataavläsning får äga rum utformas på i princip samma sätt som för hemlig teleavlyssning och hemlig kameraövervakning. Därmed bör hemlig dataavläsning i grunden förutsätta att det för brottet inte är föreskrivet lindrigare straff än fängelse i två år. Som exempel på brott som då skulle omfattas av tillämpningsområdet kan nämnas mord, dråp, människorov som inte är mindre grovt, människohandel för sexuella ändamål som inte är mindre grovt, grovt rån, mordbrand som inte är mindre allvarlig och allmänfarlig ödeläggelse som inte är mindre allvarlig samt grova brott mot rikets inre och yttre säkerhet. En avgränsning av tillämpningsområdet till ett minimistraff på två års fängelse enligt brottets straffskala innebär också att grovt narkotikabrott och grov narkotikasmuggling faller direkt under tillämpningsområdet. Narkotikabrott utgör många gånger en plattform för annan, organiserad brottslighet. Informationssystem an-

vänds i det sammanhanget bl.a. för att knyta kontakter och utbyta information med personer som ingår i distributionskedjan. Behovet av att kunna använda hemlig dataavläsning har vi uppfattat som särskilt framträdande just vid utredningar rörande sådana brott. Det är alltså fråga om så grova brott att intresset av att kunna använda hemlig dataavläsning för att få brottet utrett i princip undantagslöst måste anses väga tyngre än motstående intressen (jfr prop. 1988/89:124 s. 41 och prop. 1995/96:85 s. 25). Självklart måste lagstiftningen utformas så att tillräckliga hänsyn tas till den enskildes intressen i varje situation.

Det är också angeläget att kunna använda dataavläsning när misstanken rör straffbara fall av försök, förberedelse och stämpling till brott som har ett minimistraff på fängelse i två år. Det finns ofta minst lika starka skäl att få använda hemlig dataavläsning i dessa brottutredningar som när det gäller fullbordade brott. Exempelvis skulle en möjlighet att ingripa på ett tidigt stadium kunna leda till att allvarliga brott hindras från att fullbordas. Liksom vid bl.a. hemlig teleavlyssning och hemlig kameraövervakning skall alltså även straffbara fall av försök, förberedelse och stämpling till de brotten kunna ligga till grund för hemlig dataavläsning.

Hemlig teleövervakning får genomföras vid förundersökning angående brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader och vid förundersökning angående narkotikabrott och narkotikasmuggling samt vid vissa fall av försöks-, förberedelse- och stämplingsbrott (27 kap. 19 § RB). Sedan den 1 oktober 2004 anges särskilt i bestämmelsen att hemlig teleövervakning får genomföras även vid förundersökning angående dataintrång (4 kap. 9 c § BrB) och barnpornografibrott som inte är att anse som ringa (16 kap. 10 a § BrB). Straffskalan för dataintrång är böter eller fängelse i högst två år och för barnpornografibrott som inte är ringa fängelse i högst två år. För grovt barnpornografibrott är straffskalan fängelse mellan sex månader och fyra år.

Som har framgått medger informationstekniken att personer relativt enkelt kan vara anonyma och dölja sina förehavanden vid brottslighet. Det leder till svårigheter för de brottsutredande myndigheterna att utreda dataintrång där personer försöker komma åt information som de inte har behörighet till. Det kan exempelvis röra interna fall av behörighetsöverskridanden inom myndigheter eller företag och externa fall där avancerade ”hackare” bereder sig tillgång till information av t.ex. konkurrensskäl eller andra ekonomiska skäl. Det är enligt vår mening angeläget att de brottsutredande myndigheterna har möjlighet att använda hemlig dataavläs-

ning även vid dataintrång så att myndigheterna får en effektiv möjlighet att bekämpa sådan brottslighet, som blir allt mer vanlig.

Det finns ett mycket stort behov av att kunna använda hemlig dataavläsning vid utredningar av barnpornografibrott, även om straffvärdet enbart i yttersta undantagsfall når upp till två års fängelse. Barnpornografibrott är speciellt så till vida att enbart ett innehav av visst material kan utgöra brott. De som begår den typen av brott har därigenom ett stort intresse av att ta bort eller dölja sådant material i syfte att undgå upptäckt. Det är mycket vanligt att kryptering används i dessa sammanhang i stället för att materialet raderas, eftersom materialet upplevs av brottslingarna som allt för ”värdefullt” för att förstöras. Likaså finns det ett uppenbart intresse av att dölja sin identitet. Om det blir möjligt att använda hemlig dataavläsning vid misstankar om barnpornografibrott skulle förundersökningarna i betydligt fler fall än i dag kunna bli framgångsrika, t.ex. genom att information om bilderna i en persons dator påträffas och bevisningen säkras. Dessutom skulle polisen mer effektivt kunna upptäcka hur bilderna skickas mellan personer i olika ”nätverk” eller s.k. pedofilringar. Vi har fått beskrivet hur husrannsakningar och beslag i sådana utredningar inte lett till framgång eftersom bevisningen förstörts före polisens tillslag eller skyddats av kryptering som inte gått att forcera. Detta skulle kunna undvikas om hemlig dataavläsning blev möjlig att använda vid den brottsligheten. Vi menar att behovet av hemlig dataavläsning vid barnpornografibrott är så stort att det är angeläget att tvångsmedlet kan användas även vid sådana brott. Integritetsskäl bör inte hindra en sådan regel även om straffvärdet vid den typen av brottslighet inte överstiger två års fängelse.

En av Säkerhetspolisens uppgifter är det s.k. författningsskyddet, dvs. att förebygga och avslöja hot mot rikets inre säkerhet (se särskilt 18 kap. BrB). Det brukar uttryckas att hot mot rikets inre säkerhet avser verksamhet som syftar till att med våld, hot eller tvång ändra vårt statsskick, förmå beslutande politiska organ eller myndigheter att fatta beslut i en viss riktning eller hindra enskilda medborgare från att utöva sina fri- och rättigheter. Säkerhetspolisens uppgift på det området är i första hand inriktad på åtgärder mot grupper av individer som visat att de är beredda att använda våld eller hot om våld i syfte att nå egen politisk vinning eller grupper som kan befaras stödja sådana aktiviteter. Det gäller främst grupper med kopplingar till den s.k. vit makt-miljön och den autonoma miljön. Vit makt-miljön är ett samlingsbegrepp för organisationer eller liknande och enskilda individer med gemensamma hö-

gerextrema ideologiska värderingar. Den centrala idén inom miljön handlar om att bevara en mänsklig ras bestående av enbart vita, icke-judiska, heterosexuella personer.

Såväl åklagare som leder förundersökningar om brott med kopplingar till högerextremism som Säkerhetspolisen har framfört till oss att det finns ett behov av hemlig dataavläsning vid misstankar om hets mot folkgrupp enligt 16 kap. 8 § BrB. ”Normalfall” av det brottet ger enligt bestämmelsen fängelse i högst två år medan ringa brott ger böter. För grova brott är straffskalan fängelse mellan sex månader och fyra år.

Vi har fått beskrivningar dels av hur brottet hets mot folkgrupp begås på Internet, dels av hur de högerextrema grupperna annars använder informationstekniken för att på olika sätt planera och organisera sådan brottslighet. I den verksamheten utnyttjas polisens svårigheter att komma åt krypterad information. Vi har också fått uppgifter om fall där polisen inte har nått framgång i utredningar på grund av den datatekniska kompetens som finns i grupperna, vilket resulterat i att förundersökningarna har lagts ned i brist på bevis.

Det är en angelägen uppgift att bekämpa hets mot folkgrupp. På samma sätt som för dataintrång och barnpornografibrott kan det konstateras att behovet av hemlig dataavläsning i den brottsutredande verksamheten är stort och att förundersökningarna skulle bli framgångsrika i betydligt fler fall än i dag om hemlig dataavläsning fick användas vid misstankar om hets mot folkgrupp. Vi föreslår därför en sådan reglering.

Särskilt i samband med frågan om användning av hemlig dataavläsning vid dataintrång, barnpornografibrott och hets mot folkgrupp bör det påpekas att det givetvis på vanligt sätt blir upp till domstolen att bl.a. utifrån integritetsskäl göra noggranna överväganden i frågan om tillstånd till hemlig dataavläsning skall ges i det enskilda fallet.

Det finns andra fall där det brott som förundersökningen avser är så allvarligt att hemlig dataavläsning bör få äga rum, trots att den undre gränsen i straffskalan inte når upp till två års fängelse. Bl.a. har Ekobrottsmyndigheten påtalat ett behov av att kunna använda hemlig dataavläsning vid grov ekonomisk brottslighet. Behovet finns även vid exempelvis grova smugglingsbrott och andra typer av brott av organiserad karaktär. Hemlig dataavläsning skall därför kunna äga rum även när straffvärdet för det enskilda brottet kan antas överstiga fängelse i två år. Det bör med andra ord finnas en straffvärdeventil även för hemlig dataavläsning. Regeringen uttalade

i samband med att straffvärdeventilen infördes för hemlig teleavlyssning och hemlig kameraövervakning att den skulle användas restriktivt (prop. 2002/03:74 s. 35). Detta gäller givetvis också i samband med beslut om hemlig dataavläsning. Vi hänvisar till avsnitt 9.4.13 när det gäller frågan om hemlig dataavläsning vid brott som omfattas av 1952 års tvångsmedelslag.

Inom den referensgrupp som är knuten till beredningen har ett par ledamöter ifrågasatt om det bör finnas en sådan straffvärdeventil vid hemlig dataavläsning. Som skäl för den ståndpunkten har de åberopat dels att det är fråga om en tidsbegränsad lagstiftning och att det då kan finnas skäl att gå fram med en mer begränsad reglering, dels att straffvärdebedömningar är svåra att göra. Det kan emellertid konstateras att liknande regler som bygger på straffvärdebedömningar redan finns vid hemlig teleavlyssning och hemlig kameraövervakning. Vi anser därför i likhet med referensgruppens majoritet att det inte bör finnas något hinder mot att ta med en sådan regel.

9.4.5 Brottsmisstankens styrka och behovet av åtgärden m.m.

Förslag: Hemlig dataavläsning skall få äga rum, om

1. någon är skäligen misstänkt för brottet,
2. åtgärden är av synnerlig vikt för utredningen, och
3. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.

I förtydligande syfte skall det av lagtexten uttryckligen framgå att rätten får föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.

Brottsmisstankens styrka

I rättegångsbalken förekommer olika uttryckssätt för att ange en viss grad av sannolikhet för att någon gjort sig skyldig till brott. En förhållandevis låg grad av misstanke uttrycks genom att någon kan misstänkas för brott (23 kap. 9 § RB). En högre grad av misstanke ligger i att någon är skäligen misstänkt. När någon är på sannolika skäl misstänkt för brott föreligger en ännu högre grad av misstanke. Valet av misstankegrad är av betydelse för hur effektivt det ak-

tuella tvångsmedlet blir i den brottsutredande verksamheten och för omfattningen av de integritetskränkningar som tvångsmedlet kan komma att medföra. De två intressena måste som alltid vägas mot varandra och det måste finnas en rimlig balans.

I dag gäller för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning att tvångsmedlen får användas när utredningen har kommit så långt att det finns någon som är skäligen misstänkt för det brott förundersökningen avser (27 kap. 20 § första stycket RB och 3 § första stycket 1 lagen om hemlig kameraövervakning). Det kravet gäller även för flera andra tvångsmedel. Hemlig kameraövervakning kan dock även användas i situationer när det inte finns någon som är skäligen misstänkt i syfte att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats (3 a § lagen om hemlig kameraövervakning). Som framgått föreslår vi i avsnitt 4.3 att även hemlig teleövervakning (övervakning) skall få användas under vissa förutsättningar i fall där det saknas en skäligen misstänkt person.

Liksom för de jämförbara tvångsmedlen bör en förutsättning för användning av hemlig dataavläsning som huvudregel (se vidare avsnitt 9.4.6) vara att en viss person är skäligen misstänkt för något av de brott för vilka hemlig dataavläsning får beslutas. En högre misstankegrad skulle innebära att tvångsmedlet blir ineffektivt och skulle bl.a. motverka allmänhetens starka intresse av att allvarliga brott klaras upp. Det skall också nämnas att det inte finns rimliga skäl att differentiera kravet på misstanke, t.ex. så att misstankegraden är lägre när risken för integritetsintrång hos tredje man är minimal. Innebörden av begreppet skäligen misstänkt bör vara densamma som vid hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Detta innebär också att skälig misstanke om annan delaktighet än direkt gärningsmannaskap i ett brott som får föranleda hemlig dataavläsning kan läggas till grund för ett tillstånd till tvångsmedlet, t.ex. medhjälp till grovt narkotikabrott eller anstiftan till mord.

Synnerlig vikt för utredningen

Att åtgärden skall vara av synnerlig vikt för utredningen utgör en grundläggande förutsättning för tillstånd till hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning (27 kap. 20 § första stycket RB och 3 § första stycket 2 lagen om hemlig kameraövervakning). I likhet med den ordningen bör kravet på synnerlig

vikt gälla även för beslut om hemlig dataavläsning. Därmed får åtgärden vidtas endast när andra åtgärder som står till buds under förundersökning inte är tillräckliga eller det av annan anledning är av synnerlig vikt för utredningen att avläsningen sker. Regeringen bedömde i lagrådsremissen från april 2000 (s. 48 f.) rörande bl.a. buggning att uttalandena om uttryckets innebörd i prop. 1988/89:124 (s. 44 f.) fortfarande var aktuella. Där uttalade regeringen följande (se även prop. 1995/96:85 s. 29).

> 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 beträffade de upplysningar som avlyssningen kan ge. Dessa får sålunda inte inskränka sig till obetydliga detaljer, som man kan båda 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 frågan 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 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.

Uttalandet bör i allt väsentligt kunna vara vägledande för hur uttrycket synnerlig vikt för utredningen bör uppfattas vid prövningen av ärenden om hemlig dataavläsning. Med hänsyn till att åtgärden kan vara integritetskänslig bör alternativa metoder övervägas omsorgsfullt. Det förhållandet att något alternativ står till buds, bör, lika lite som för andra tvångsmedel, inte automatiskt leda till att tillstånd nekas.

Proportionalitetsprincipen

Som nämndes i avsnitt 2.8.2 gäller tre allmänna principer för all tvångsmedelsanvändning; ändamåls-, behovs- och proportionalitetsprinciperna. Vi upprepar inte vad principerna innebär men vill som exempel på tillämpning av proportionalitetsprincipen (se t.ex. 27 kap. 1 § tredje stycket RB för hemlig teleavlyssning och hemlig teleövervakning samt 3 § första stycket 3 lagen om hemlig kameraövervakning) nämna att domstolen ställer upp ett inskränkande villkor för verkställigheten.

Proportionalitetsprincipen bör komma till uttryck även i lagtexten rörande hemlig dataavläsning. Domstolen skall göra en avvägning mellan skälen för åtgärden och de olägenheter som åtgärden kan förorsaka den misstänkte eller något annat motstående intresse. I detta fall innebär det en avvägning mellan intresset av att utreda det brott som misstanken avser och de risker för en kränkning av den personliga integriteten som en användning av dataavläsning innebär, såväl för den misstänkte som för tredje man. Av sådana skäl kan domstolen liksom vid t.ex. avlyssning enligt 27 kap. 18 § RB besluta om inskränkande villkor i tillståndet. Det kan röra exempelvis vilka tvångsmedel som får verkställas samtidigt mot en misstänkt person, vilka eller vilka delar av ett informationssystem som verkställigheten får avse och vilket intrång som får ske för att genomföra åtgärden.

Vi föreslår att det i förtydligande syfte skall finnas en uttrycklig bestämmelse i 27 kap. 21 § andra stycket RB som anger att rätten i beslut om avlyssning eller övervakning får föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när. En sådan bestämmelse bör finnas även rörande hemlig dataavläsning.

Proportionalitetsprincipen skall tillämpas också under verkställighetsstadiet, vilket innebär att även polisen har att beakta den efter att tillstånd har givits till tvångsmedlet (se 8 § polislagen).

9.4.6 Undantag från kravet på skäligen misstänkt person

Förslag: Även om det inte finns någon person som är skäligen misstänkt skall hemlig dataavläsning få äga rum om det är av synnerlig vikt för utredningen att dataavläsning sker av information i informationssystem som har använts eller används vid brottet. Hemlig dataavläsning i sådana fall får äga rum endast om åtgärden syftar till att fastställa vem som skäligen kan misstänkas för brottet.

Enligt nuvarande bestämmelser är det en förutsättning för att hemlig teleavlyssning och hemlig teleövervakning skall kunna äga rum att det går att peka ut någon som skäligen misstänkt för ett brott (27 kap. 20 § första stycket RB). Vi föreslog i avsnitt 4.3 att hemlig teleövervakning (övervakning enligt 27 kap. 19 § RB) under vissa förutsättningar skall kunna användas även när det saknas en skäligen misstänkt person. Såväl i Buggningsutredningens betänkande Om buggning och andra hemliga tvångsmedel (SOU 1998:46) som i den efterföljande lagrådsremissen föreslogs en liknande reglering.

Sedan den 1 oktober 2004 är det möjligt att använda hemlig kameraövervakning trots att det inte finns någon som är skäligen misstänkt för brottet. Förslaget kommer ursprungligen från Buggningsutredningen som i sitt betänkande (SOU 1998:46 s. 391 ff.) föreslog att hemlig kameraövervakning skulle få användas om det av särskild anledning kunde förväntas att åtgärden leder till att brottet klaras upp. I propositionen till den nämnda ändringen av lagen om hemlig kameraövervakning hänvisar regeringen till Buggningsutredningen och anger bl.a. följande (prop. 2002/03:74 s. 41 f.).

> Det finns ett antal situationer där det av utredningsskäl vore angeläget att kunna använda hemlig kameraövervakning när det inte finns någon som är skäligen misstänkt för ett känt brott. Man kan t.ex. tänka sig att det i ett bostadsområde har anlagts flera bränder och att det finns ett tydligt mönster i förfarandet men det inte är möjligt att ringa in en viss person som skäligen misstänkt för att ha anlagt bränderna. Man kan också tänka sig upprepade försök till mord på vårdhem, där

gärningarna har begåtts genom manipulationer med respiratorutrustning eller genom att det lagts gift i medicinburkar. Det är självklart att det ur brottsutredningssynpunkt skulle vara värdefullt om tillstånd till hemlig kameraövervakning kunde beviljas i liknande fall. En användning av hemlig kameraövervakning skulle kunna bidra till att brottet eller brotten klaras upp och förhindra att flera allvarliga brott begås. Mot denna bakgrund anser utredningen att det finns ett påtagligt behov av att kunna använda hemlig kameraövervakning även när misstanken om brott inte kan hänföras till en viss person. Utredningen föreslår därför att hemlig kameraövervakning skall få användas även när det inte finns någon skäligen misstänkt.

Som utredningen funnit bör tillämpningsområdet för hemlig kameraövervakning utvidgas. Regeringen delar utredningens uppfattning att hemlig kameraövervakning i vissa fall skall få användas trots att det inte finns någon som är skäligen misstänkt för brottet. Det skall vara av synnerlig vikt för utredningen att övervakningen sker. Syftet med åtgärden bör därmed i allmänhet vara att gärningsmannen kan påträffas på bar gärning.

Till skillnad från utredningen anser regeringen att möjligheten bör begränsas till den plats där brottet begåtts eller omgivningarna till en sådan plats. Det finns enligt regeringens mening annars en risk för att tvångsåtgärden kan komma att användas i brottsförebyggande syfte. Åtgärden är då typiskt sett inte något tvångsmedel och bör inte behandlas inom ramen för tvångsmedelsregleringen. Om syftet med en dold övervakning endast är brottsförebyggande eller om den dolda övervakningen sker endast av hänsyn till allmän ordning och säkerhet får frågan i stället prövas enligt lagen om allmän kameraövervakning. Det är därför motiverat att behålla länsstyrelsens möjlighet att medge undantag från upplysningsplikten i speciella situationer.

Vi nämnde i avsnitt 9.4.1 att de två huvudsakliga skälen för att införa hemlig dataavläsning var problemen med dels krypterad information i datorer och liknande dels möjligheten att vara anonym vid användning av informationsteknik. I många fall finns båda dessa problem samtidigt. Anonymitetsproblemet bottnar i det förhållandet att även om de brottsutredande myndigheterna lyckas knyta en

IP-adress till ett visst abonnemang, det ändå många gånger är osäkert om den som står bakom abonnemanget också är den som har suttit vid datorn vid det tillfälle som myndigheterna är intresserade av. Det kan t.ex. röra köp och försäljning av narkotika samt tillfällen för spridning och konsumtion av barnpornografi. Genom att använda hemlig dataavläsning kan de brottsutredande myndigheterna lyckas identifiera en person som skäligen misstänkt för brottsligheten. Av effektivitetsskäl är det därför nödvändigt att hemlig dataavläsning får äga rum även i de fall när det saknas en skäligen misstänkt person. Av hänsyn till det integritetsintrång som uppkommer är det, som en parallell till bestämmelserna om hemlig kameraövervakning, rimligt att föreskriva att hemlig dataavläsning i dessa fall endast får avse ett informationssystem som har använts eller används vid brottet och att åtgärden endast får syfta till att fastställa vem som skäligen kan misstänkas för brottet.

9.4.7 Sambandet mellan en misstänkt och informationssystemet

Förslag: I fall där det finns en skäligen misstänkt person får hemlig dataavläsning endast avse informationssystem som det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av. Avser åtgärden informationssystem i någon annans stadigvarande bostad, får hemlig dataavläsning äga rum endast om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.

Hemlig dataavläsning innebär som framgått tidigare att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel. Ett beslut om hemlig dataavläsning skall avse ett eller flera angivna informationssystem. Eftersom syftet med tvångsmedlet i normalfallet är att avläsa information som kan knytas till en skäligen misstänkt person är det naturligt att det bör finnas en viss koppling mellan den misstänkte och det eller de informationssystem som skall omfattas av tvångsmedelsbeslutet. Det gäller särskilt som det är fråga om ett integritetskänsligt tvångsmedel.

I den aktuella frågan finns paralleller till frågan om den misstänktes anknytning till viss plats vid användning av hemlig kameraövervakning. Enligt 3 § andra stycket lagen om hemlig kameraövervakning får den åtgärden endast avse en sådan plats där den misstänkte

kan antas komma att uppehålla sig. På liknande sätt föreslog Buggningsutredningen att buggning endast skulle få avse en sådan plats där den misstänkte kunde antas komma att uppehålla sig (SOU 1998:46 s. 406 ff.). Utredningen hänvisade till propositionen rörande hemlig kameraövervakning där regeringen angav följande (prop. 1995/96:85 s. 31, se även s. 39).

> Det nu anförda talar för att tillstånd till hemlig kameraövervakning i stället bör knytas till en viss plats. Det kan naturligtvis röra sig om flera olika platser och antalet platser bör också kunna utvidgas genom nya beslut. Av avgörande betydelse är emellertid att det finns en koppling till den misstänkte. Som tidigare redovisats får åtgärden endast avse den som är skäligen misstänkt för brott. Detta innebär nu inte att den misstänkte ständigt måste uppehålla sig på platsen och således finnas med på bild. Ett sådant krav skulle reducera användningsområdet i alltför stor utsträckning. Det bör dock kunna antas att han så småningom besöker den plats som skall övervakas. Det bör vara tillräckligt att det är fråga om ett kort besök. Om det emellertid från början står klart att den misstänkte aldrig besöker en plats som i sig är av intresse i förundersökningen, t.ex. en lägenhet i en utredning om grovt koppleri, bestående i uthyrning av lägenheten, bör användning av dolda övervakningskameror inte komma i fråga.

Regeringen ansåg dock i den efterföljande lagrådsremissen rörande buggning att kravet på samband mellan den misstänkte och platsen skulle sättas högre och skrev följande (s. 52).

> Regeringen anser att nivån på antagandet att den misstänkte skall besöka den plats som skall avlyssnas bör sättas högre än vad som enligt nu gällande regler gäller för hemlig kameraövervakning. I och för sig kan det hävdas att det vore tillräckligt att rätten med tillämpning av proportionalitetsprincipen i samband med beslutet om hemlig avlyssning utfärdar särskilda restriktioner, t.ex. av innebörd att utrustningen endast får vara i funktion under den tid den misstänkte faktiskt befinner sig på platsen. Regeringen bedömer emellertid det angeläget att en mer restriktiv syn på användningen av tvångsmedlet uttryckligen framgår av de grundläggande förutsättningarna för användningen av hemlig avlyssning. För att hemlig avlyssning skall få ske bör det ske en noggrann

> prövning av sannolikheten för att den misstänkte kommer att befinna sig på just den platsen någon gång under den tid som beslutet avser. Det kan t.ex. via hemlig teleavlyssning ha framkommit att den misstänkte nämnt att han avser att bege sig till en viss plats. Ett annat exempel är att den misstänkte har ett återkommande engagemang på en viss plats. Ett sådant högre krav på sambandet mellan den misstänkte och platsen som skall avlyssnas kan enligt regeringen lämpligen formuleras med att det finns ”särskild anledning att anta” att den misstänkte kommer att uppehålla sig på platsen (jfr 28 kap. 2 a § rättegångsbalken). Detta innebär givetvis inte att bedömningen enligt proportionalitetsprincipen inte skall göras med sedvanlig noggrannhet.

Regeringen föreslog alltså att buggning liksom hemlig kameraövervakning endast skulle få avse en plats där det finns särskild anledning att anta att den misstänkte skulle komma att uppehålla sig.

Den syn på frågan om den misstänktes anknytning till viss plats som kommer till uttryck i de nämnda förarbetsuttalandena har enligt vår mening bäring även när det gäller hemlig dataavläsning och frågan om det aktuella informationssystemets anknytning till den misstänkte. Det bör alltså finnas ett krav på att hemlig dataavläsning endast får avse informationssystem som det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av.

En annan fråga som togs upp av regeringen i den nämnda lagrådsremissen (s. 52 ff.) rörande buggning var om det skulle ställas högre krav på anknytning mellan platsen och den misstänkte när buggning skulle verkställas i annan stadigvarande bostad än den misstänktes. Regeringen föreslog att det borde ställas upp ett högre krav på antagandet att den misstänkte befinner sig på platsen i sådana fall. I likhet med vad som föreskrivs i vissa fall vid husrannsakan (se 28 kap. 2 § RB) kom regeringen fram till att buggning i tredje mans stadigvarande bostad skulle få tillåtas endast om det fanns ”synnerlig anledning att anta” att den misstänkte skulle komma att uppehålla sig på platsen. Som exempel nämnde regeringen att det genom yttre spaning kommit fram omständigheter som entydigt pekar på att den misstänkte, som annars har ett kringflackande liv och är svår att nå, varje vecka en viss tidpunkt besöker en bekant. Ett annat exempel som nämndes var att den misstänkte hade beställt en tågbiljett i syfte att besöka och bo hos en bekant en tid. Regeringen underströk samtidigt att det alltid

skulle vara ett krav att det var av synnerlig vikt för utredningen att åtgärden kom till stånd och att rätten mot bakgrund av proportionalitetsprincipen kunde meddela särskilda föreskrifter om bl.a. tidpunkter för avlyssningen.

Även i detta fall är det rimligt att särskilt av integritetsskäl göra en koppling mellan förslaget till reglering av buggning och användningen av hemlig dataavläsning. Det bör därför finnas en bestämmelse som anger att om åtgärden avser informationssystem i någon annans stadigvarande bostad, får hemlig dataavläsning äga rum endast om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.

De krav som nu har nämnts om sambandet mellan den misstänkte och det informationssystem som tillståndet avser utgör tillsammans med främst de förhållanden att hemliga dataavläsning i princip endast får avse grova brott, att åtgärden som huvudregel endast får avse den som är skäligen misstänkt, att åtgärden måste vara av synnerlig vikt för utredningen och att bl.a. proportionalitetsprincipen skall tillämpas, tillräckliga garantier för att tvångsmedlet endast kommer att användas i de fall där det kan anses befogat.

9.4.8 Tillståndstiden m.m.

Förslag: Ett beslut om hemlig dataavläsning skall gälla under en viss tid. Tiden får inte bestämmas längre än vad som är nödvändigt och får inte överstiga en månad från dagen för beslutet.

Som framgick tidigare är det rätten som skall pröva om förutsättningarna för användning av hemlig dataavläsning är uppfyllda. Denna prövning kan sägas innefatta två led. Det ena ledet hänför sig till en prövning om samtliga rekvisit, så som de kommit till uttryck i lagtexten, föreligger i det enskilda fallet. Den prövningen avser t.ex. brottets svårhetsgrad, den grad av misstanke som får anses föreligga och om åtgärden är av synnerlig vikt för utredningen. Det andra ledet innehåller en mer allmän lämplighetsbedömning där bl.a. proportionalitetsprincipen skall beaktas. Rätten skall här ta ställning till exempelvis om vad som står att vinna med åtgärden motiverar densamma.

De faktiska förutsättningarna för att få tillstånd att använda hemlig dataavläsning i en viss brottsutredning kan naturligtvis komma att ändras över tiden i takt med att förundersökningen fortskrider och utredningsläget förändras. Det är angeläget att be-

stämmelserna om tvångsmedlet ger garantier för att det inte används om vissa förhållanden, som har utgjort en nödvändig förutsättning för domstolens tillstånd, har ändrats. Sådana garantier uppnås bäst genom en med vissa tidsintervaller återkommande domstolsprövning av meddelade tillstånd. Frågan är då hur länge ett tillstånd skall gälla innan domstolen skall pröva frågan på nytt.

För tillstånd att hämta in framtida uppgifter (realtidsuppgifter) vid hemlig teleavlyssning och hemlig teleövervakning samt för tillstånd till hemlig kameraövervakning gäller i dag att tillståndstiden inte får bestämmas längre än nödvändigt och att den inte får överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket RB och 4 § andra stycket lagen om hemlig kameraövervakning). När rätten bestämmer tiden för ett tillstånd kan den således ange att tillståndet endast gäller för en kortare period än en månad. Tillståndet kan också förenas med andra villkor. Tillståndstiden räknas från dagen för rättens beslut och rätten kan alltså inte bestämma att tillståndet skall gälla t.ex. först fr.o.m. en vecka efter beslutet och därefter i en månad. Det förekommer att rätten får ompröva, eller förnya, tillståndsbeslut på grund av att åklagaren före tillståndstidens utgång kommer in med en begäran om förlängning avseende samma brott och samma misstänkta person. Det anses då att ju längre tid som tillståndet gällt utan att förundersökningen förts framåt, desto mer restriktiv bör domstolens prövning bli (jfr prop. 1995/96:85 s. 40).

I fall när intrång måste göras för att placera ut det tekniska hjälpmedlet vid hemlig dataavläsning får det antas att det ofta kommer att krävas omfattande förberedelser för att det skall vara möjligt att genomföra utan att väcka uppmärksamhet eller på annat sätt avslöja verksamheten. Det är uppenbart att en kortare tillståndstid än en månad bl.a. i sådana fall blir alltför kort och skulle hänvisa åklagaren till att genast begära förlängning av tillståndstiden, vilket inte är en lämplig ordning. Inte heller har det framkommit något som tyder på att det skulle finnas behov av längre tillståndstider än en månad vid hemlig dataavläsning. Tiden bör därför överensstämma med ordningen för de andra nämnda tvångsmedlen, dvs. högst en månad åt gången. Detta skall dock inte hindra att de brottsutredande myndigheterna vid verkställigheten får tillgång till information i informationssystemet som så att säga redan fanns där när tillståndet gavs, alltså en slags historiska uppgifter.

Som framgår av avsnitt 9.4.5 föreslår vi dessutom att det uttryckligen i lagtexten anges att rätten får föreskriva villkor för att tillgo-

dose intresset av att enskildas integritet inte i onödan träds för när. Vi lämnar samma förslag rörande avlyssning och övervakning enligt 27 kap. 21 § andra stycket RB.

9.4.9 Tillträde till platsen m.m.

Förslag: Ett beslut om hemlig dataavläsning får innefatta rätt för den brottsutredande myndigheten att i hemlighet bereda sig tillträde till en plats som annars särskilt skyddas mot intrång i syfte att installera de tekniska hjälpmedlen.

Ett tekniskt hjälpmedel som har installerats skall återtas eller göras obrukbart så snart det kan ske efter det att tiden för tillståndet gått ut eller tillståndet hävts. När hjälpmedlet har återtagits eller gjorts obrukbart, skall rätten underrättas om det.

Vid genomförande av hemlig dataavläsning får olägenhet eller skada inte förorsakas utöver vad som är oundgängligen nödvändigt.

De informationssystem som förslaget om hemlig dataavläsning tar sikte på kommer i de allra flesta fall att vara placerade så att de finns i utrymmen som allmänheten inte har tillträde till och som är skyddade mot intrång, t.ex. bostäder och arbetsplatser. Vi har tidigare beskrivit att hemlig dataavläsning kan verkställas genom att den brottsutredande myndigheten i hemlighet sänder en viss mjukvara till en dator. Den s.k. programkoden ger sedan myndigheterna uppgifter om vilken information som finns i datorn och hur datorn används. Dataavläsning kan också innebära att hård- eller mjukvara med liknande funktion placeras i datautrustningen genom ett fysiskt ingrepp, t.ex. vid ett intrång i en persons bostad eller på dennes arbetsplats. Det ligger i tvångsmedlets natur att ett sådant intrång måste göras i hemlighet.

Ett tillstånd till hemlig dataavläsning måste, om tvångsmedlet skall kunna användas effektivt, i vissa fall kunna verkställas genom att det tekniska hjälpmedlet placeras i datautrustningen genom ett fysiskt ingrepp. Därför behöver tillståndet kunna innehålla en befogenhet att få tillträde till den plats eller det utrymme där informationssystemet är beläget för att de tekniska hjälpmedlen skall kunna installeras. En sådan befogenhet blir närmast att jämföra med ett beslut om husrannsakan. Det skulle dock strida mot ändamålsprincipen om polisen vidtog husrannsakan i samband med tillträde enligt bestämmelsen om hemlig dataavläsning eller tvärtom. Som regeringen yttrade i samband med lagrådsremissen rörande

buggning, har åklagaren, om han anser att det krävs hemligt tillträde till platsen, att i sin framställning till rätten närmare utveckla skälen för det. Det kan dock inte krävas att åklagaren vid begäran om tillstånd närmare skall ange exakt var det tekniska hjälpmedlet skall placeras, t.ex. i vilket rum informationssystemet är beläget som de brottsutredande myndigheterna behöver få tillgång till. Även om åklagaren inte är skyldig att närmare ange sådana fakta, kan rätten i ett tillståndsbeslut ge föreskrifter i den saken.

Ett par ledamöter i den referensgrupp som är knuten till beredningen har ansett att de brottsutredande myndigheterna inte skall ges rätt att få tillträde till exempelvis bostäder och arbetsplatser för att placera sådan utrustning som krävs för hemlig dataavläsning. Vi har emellertid, med hänsyn till de mycket restriktiva förutsättningarna som vi föreslår för användning av tvångsmedlet hemlig dataavläsning (se bl.a. avsnitten 9.4.4, 9.4.5 och 9.4.7) och de tillstånds- och rättssäkerhetskrav som ställs upp (se bl.a. avsnitt 9.4.3), ansett – i likhet med referensgruppens majoritet – att myndigheterna bör kunna ges ett sådan rätt när domstol gett tillstånd till tvångsmedlet.

Det tekniska hjälpmedlet måste också återtas, om det inte på annat sätt kan göras obrukbart. Återtagandet skall därmed också tas in i bedömningen av frågan om hemlig dataavläsning skall tillåtas eller inte, eftersom även ett återtagande ofta kommer att kräva ett hemligt intrång. Fråga uppstår då om vid vilken tidpunkt det tekniska hjälpmedlet skall återtas. Ett tillstånd till användning av ett tvångsmedel gäller självfallet under den tid som anges i beslutet, så länge som förutsättningar för tillstånd fortfarande finns. Det tekniska hjälpmedlet får givetvis inte installeras innan rätten har fattat beslut om hemlig dataavläsning och verkställigheten får inte pågå utöver tillståndstiden. Det kan dock inte krävas att de brottsutredande myndigheterna under den tid som tillståndet avser även skall ta bort den tekniska utrustningen. En sådan åtgärd kräver bl.a. en hel del planering för att kunna genomföras utan upptäckt.

När det tekniska hjälpmedlet som har installerats inte längre får användas skall det alltså tas bort, vilket bör ske så snart som möjligt. I stället för att återta hjälpmedlet bör det dock finnas en rätt att i stället göra det obrukbart, om tekniken medger detta och det skulle vara lämpligare i ett visst fall.

Vid hemlig teleavlyssning krävs inte att det sker intrång för att starta eller avbryta avlyssningen. Operatörernas nödvändiga medverkan vid den verkställigheten innebär bl.a. att polisen kan värja sig mot obefogade anklagelser om omfattande eller otillbörlig avlyssning (se SOU 1998:46 s. 341). Det kan framstå som angeläget

även vid hemlig dataavläsning att det finns en slags yttre kontroll av att verkställighet inte fortgår t.ex. efter det att tillståndet har upphört. På samma sätt som regeringen föreslog i lagrådsremissen rörande buggning menar vi att det är lämpligt att föreskriva att domstolen skall underrättas av åklagaren när det tekniska hjälpmedlet har tagits bort eller gjorts obrukbart. Detta är, som regeringen uttalade, ett administrativt okomplicerat sätt att skapa en kontroll. Skulle någon underrättelse inte komma in, faller det närmast på det offentliga ombudet att agera.

Givetvis bör endast sådan olägenhet eller skada som är nödvändig få förorsakas vid verkställigheten. Detta bör, liksom vid husrannsakan (se 28 kap. 6 § första stycket RB), särskilt föreskrivas i lagen om hemlig dataavläsning. De brottsutredande myndigheterna skall alltså vid verkställigheten av hemlig dataavläsning vara skyldiga att se till att tvångsmedlet orsakar minsta möjliga skada.

9.4.10 Undantag för avläsning av meddelanden mellan den misstänkte och hans försvarare

Förslag: Hemlig dataavläsning skall inte få ske av sådana meddelanden mellan den misstänkte och hans försvarare som avses i 27 kap. 22 § RB. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer.

Enligt 36 kap. 5 § tredje stycket RB får rättegångsombud, biträden eller försvarare inte höras som vittnen om vad som anförtrotts dem för uppdragets fullgörande, om inte den misstänkte medger det. Det gäller oavsett brottets beskaffenhet. Det gäller också vare sig ombudet är advokat eller inte. Mot bakgrund av den bestämmelsen finns regeln i 27 kap. 22 § RB om att hemlig teleavlyssning inte får ske av telefonsamtal eller andra telemeddelanden mellan den misstänkte och hans försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant samtal eller meddelande, skall avlyssningen avbrytas. Upptagningar eller uppteckningar skall, i den mån de omfattas av förbudet, omedelbart förstöras. Det kan nämnas att det i förarbetena sades att paragrafen inte kommer att få betydelse annat än i några enstaka fall, eftersom det hör till undantagssituationerna att en försvarare har utsetts när avlyssningen aktualiseras (prop. 1988/89:124 s. 68). Någon motsvarighet till be-

stämmelsen finns inte för hemlig teleövervakning och hemlig kameraövervakning.

I den lagrådsremiss som följde på Buggningsutredningens förslag föreslog regeringen att avlyssningsförbudet i 27 kap. 22 § RB skulle utökas till att omfatta telefonsamtal eller andra telemeddelanden där någon som yttrar sig, på grund av vissa bestämmelser i 36 kap. 5 § RB om undantag från vittnesplikten, inte skulle ha kunnat höras som vittne om det som sagts eller på annat sätt uttryckts. Förslaget, som rörde exempelvis advokater, läkare och präster, har inte lett till lagstiftning.

Som nämndes i avsnitt 4.2.4 avstod regeringen i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74) från att i det sammanhanget behandla vissa frågor rörande hemlig teleavlyssning och hemlig teleövervakning som Buggningsutredningen tidigare hade tagit upp. Det rörde bl.a. frågan om ett utvidgat förbud mot att avlyssna vissa samtal. Regeringen angav i dessa delar att frågorna hänger samman med en eventuell lagstiftning om hemlig avlyssning (buggning) och om hanteringen av överskottsinformation (se vidare avsnitt 9.4.11). För att inte föregripa beredningen av dessa frågor lade regeringen inte fram några förslag i de delarna i det sammanhanget (prop. 2002/03:74 s. 12).

Förslaget till reglering av hemlig dataavläsning innebär att ett nytt hemligt tvångsmedel införs genom vilket det blir möjligt för de brottsutredande myndigheterna att till en del få sådan information som annars erhålls genom hemlig teleavlyssning. Regeringen har nyligen lagt fram ett förslag till reglering av överskottsinformation vid användning av hemliga tvångsmedel (prop. 2004/05:143). I det förslaget berörs inte frågan om förbudet mot att avlyssna vissa samtal. I avvaktan på resultatet av den vidare beredningen av den frågan har vi valt att föreslå att lagstiftningen skall innehålla en bestämmelse som motsvarar den som finns för hemlig teleavlyssning (27 kap. 22 § RB). Det innebär alltså att hemlig dataavläsning inte får ske av meddelanden mellan den misstänkte och hans försvarare. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer.

9.4.11 Överskottsinformation

Förslag: Om det vid hemlig dataavläsning har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avläsning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller
2. det finns särskilda skäl.

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

Vid användning av hemliga tvångsmedel kan det komma fram uppgifter som inte har något som helst samband med det brott som har legat till grund för tvångsmedelsbeslutet. Uppgifterna kan dock i stället vara av betydelse för utredningen av ett annat begånget brott eller för att förhindra nya brott. De kan beröra den person som förundersökningen gäller eller andra personer som är ovidkommande i det sammanhanget. Det kan också röra sig om uppgifter som inte har samband med något brott men som är av betydelse i ett annat sammanhang och då främst för andra myndigheter, exempelvis sociala myndigheter. I vad mån sådan överskottsinformation får utnyttjas är inte generellt reglerat i lag även om frågan ändå inte kan sägas vara helt oreglerad.

Som nämndes i bl.a. avsnitt 9.4.10 har regeringen nyligen lagt fram ett förslag om reglering av de brottsbekämpande myndigheternas användning av överskottsinformation som framkommer vid användning av hemliga tvångsmedel. Bestämmelserna avser användning av informationen för såväl brottsutredande som brottsförebyggande ändamål (prop. 2004/05:143).

Förslaget innebär att överskottsinformation om annat brott än det som låg till grund för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning normalt skall få användas för att utreda det brottet. Beträffande överskottsinformation om mindre allvarliga brott föreslås dock en viss begränsning. En förundersökning om ett sådant mindre brott skall få inledas på grund av överskottsinformationen endast om fängelse i ett år eller däröver är föreskrivet för brottet och det kan antas att brottet inte föranleder endast böter eller om det finns särskilda skäl. Uppgifter om förestående brott föreslås få användas för att förhindra brott (se försla-

get till 27 kap. 23 a § RB och 6 a § lagen om hemlig kameraövervakning).

Hemlig dataavläsning är, som framgår av begreppet i sig, ett hemligt tvångsmedel. Det verkställs alltså utan att den berörde har vetskap om att det sker. Liksom vid övriga hemliga tvångsmedel är det givet att det även i det fallet kan komma fram uppgifter som är att beteckna som överskottsinformation. Den typ av reglering som regeringen har föreslagit för hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning måste finnas även vid användning av hemlig dataavläsning.

9.4.12 Hantering av inhämtad information

Förslag: En upptagning som har gjorts vid hemlig dataavläsning skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 27 kap. 12 § första stycket RB.

De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brott. De skall därefter förstöras.

Det material som tas upp vid hemlig dataavläsning måste givetvis granskas för att det skall gå att pröva om materialet har betydelse för en pågående utredning. Från integritetssynpunkt är det av vikt att den granskningen sker så fort som möjligt och att den personkrets som utför granskningen begränsas. I 27 kap. 24 § första stycket RB föreskrivs att upptagningar och uppteckningar som sker vid hemlig teleavlyssning skall granskas snarast möjligt. Motsvarande bestämmelse för upptagning vid hemlig kameraövervakning finns i 7 § första stycket lagen om hemlig kameraövervakning. I båda fallen gäller att 27 kap. 12 § första stycket RB skall tillämpas vid granskningen. Det sistnämnda innebär att det i normala fall endast är rätten eller åklagaren som har rätt att granska materialet.

Det finns ingen anledning att föreskriva andra regler för granskning av upptagning vid hemlig dataavläsning än som i dag finns för hemlig teleavlyssning och hemlig kameraövervakning. En upptagning som har gjorts vid hemlig dataavläsning bör därför granskas snarast möjligt. Vid en sådan granskning skall 27 kap. 12 § första stycket RB tillämpas.

Som nämndes i avsnitt 4.2.4 och 9.4.10 avstod regeringen i propositionen 2002/03:74 från att i det sammanhanget behandla vissa frågor rörande hemlig teleavlyssning och hemlig teleövervakning som Buggningsutredningen tidigare hade tagit upp. Det rörde bl.a. hanteringen av inhämtad information. Regeringen angav att frågorna hänger samman med en eventuell lagstiftning om hanteringen av överskottsinformation. För att inte föregripa beredningen av dessa frågor lade regeringen inte fram några förslag i de delarna i det sammanhanget (prop. 2002/03:74 s. 12).

I det förslag som regeringen nyligen har lagt fram om reglering av de brottsbekämpande myndigheternas användning av överskottsinformation behandlas även frågor om hantering av inhämtad information vid hemlig teleavlyssning och hemlig kameraövervakning (prop. 2004/05:143). Förslaget innehåller dels vissa ändringar av bestämmelserna i 27 kap. 24 § andra stycket RB och 7 § andra stycket lagen om hemlig kameraövervakning, dels tillägg i form av ett tredje stycke i respektive paragraf. I våra fortsatta överväganden utgår vi från att förslaget är gällande rätt.

I de delar upptagningar och upptecknings vid hemlig teleavlyssning är av betydelse från brottsutredningssynpunkt, skall de enligt 27 kap. 24 § andra stycket RB bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna och upptecknings är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brott. Därefter skall upptagningarna och upptecknings förstöras. Enligt tredje stycket i samma paragraf får brottsutredande myndigheter dock alltid behandla uppgifter från upptagningar och upptecknings i enlighet med vad som är särskilt föreskrivet i lag.

I 7 § andra stycket lagen om hemlig kameraövervakning föreskrivs samma sak vad gäller sådana upptagningar som gjorts vid verkställigheten av det tvångsmedlet, dock med det tillägget att upptagningar som saknar betydelse från brottsutredningssynpunkt skall förstöras omedelbart efter granskningen. Regeringen tar i prop. 2004/05:143 upp frågan om en motsvarande regel bör finnas även för hemlig teleavlyssning i 27 kap. 24 § RB men avfärdar detta med att ange i huvudsak följande (s. 44). Det är svårt att vid varje särskilt tidpunkt under en brottsutredning bedöma vilken information som är av betydelse från utredningssynpunkt och vilken som inte är det. En sådan bedömning kan, som JO har påpekat, i många fall sannolikt inte göras förrän utredningen är slutförd och i vissa fall först när rättegången har avslutats (jfr prop. 1988/89:124 s. 69).

Med en sådan regel finns det en risk för att polisen förstör material som senare hade kunnat visa sig vara av värde för utredningen av det brott som föranlett tvångsmedelsanvändningen. Det bör därför, liksom i dag, finnas ett utrymme för de brottsbekämpande myndigheterna att dröja med förstörandet av upptagningarna och upptecknin garna.

Även vid hemlig dataavläsning bör det finnas bestämmelser som motsvarar 27 kap. 24 § andra och tredje styckena RB. Det innebär alltså att de delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brottet. De skall därefter förstöras. Det finns stor risk för att de negativa effekter för brottsbekämpningen som regeringen nämner för hemlig teleavlyssning även uppkommer vid hemlig dataavläsning. Mot den bakgrunden skall det inte heller för hemlig dataavläsning finnas en regel som anger att upptagningar som saknar betydelse från brottsutredningssynpunkt skall förstöras omedelbart efter det att de har granskats.

9.4.13 Vissa övriga lagar med bestämmelser om hemlig dataavläsning

Förslag: Hemlig dataavläsning skall omfattas av de särskilda regler som finns i

1. lagen med särskilda bestämmelser om tvångsmedel i vissa brottmål (1952 års tvångsmedelslag),
2. lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m., och i
3. lagen om särskild utlänningskontroll.

Lagen med särskilda bestämmelser om tvångsmedel i vissa brottmål (1952 års tvångsmedelslag)

1952 års tvångsmedelslag gäller vid förundersökning om brott som har ansetts vara särskilt allvarliga för landets säkerhet. Den omfattar vissa allmänfarliga brott, t.ex. sabotage och grovt sabotage. Dessutom omfattas mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage samt flygplatssabota-

ge, om något av dessa brott innefattar sabotage. Därutöver omfattar lagen dels vissa högmålsbrott (brott mot rikets inre säkerhet) som uppror och olovlig kårverksamhet, dels vissa brott mot rikets (yttre) säkerhet, som spioneri. Lagen gäller också för terroristbrott enligt lagen (2003:148) om straff för terroristbrott och för försök, förberedelse och stämpling till de nämnda brotten, om sådan gärning är straffbar (1 §).

I förhållande till regleringen i rättegångsbalken innebär 1952 års tvångsmedelslag utvidgade möjligheter för Säkerhetspolisen att använda tvångsmedlen häktning, beslag, kvarhållande av försändelse, hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning (2-5 §§). Lagen innebär således utökade möjligheter att ingripa mot brott som rör rikets säkerhet eller som är av allmänfarlig natur.

Som har framgått föreslår vi att hemlig dataavläsning som huvudregel skall få äga rum vid utredning av brott som har ett minimistraff på två års fängelse och vid annat brott om det kan antas att brottets straffvärde överstiger fängelse i två år (se avsnitt 9.4.4). Flera av de brott som räknas upp i 1952 års tvångsmedelslag träffas inte av den regleringen. Samtliga de brott som räknas upp i lagen har dock valts ut av den anledningen att de har ansetts som särskilt allvarliga brott. Av den anledningen får tillstånd ges enligt lagen till hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning även när brottet annars inte är sådant att detta skulle vara möjligt (5 § första stycket). Enligt lagen har dessutom åklagare rätt att meddela interimistiska beslut om tillstånd till de tvångsmedlen. Det får ske om det kan befaras att inhämtande av domstolsbeslut skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. Ett sådant beslut skall ofördröjligen anmälas till rätten, som skyndsamt skall pröva ärendet (5 § andra stycket).

Även hemlig dataavläsning, som är avsett att användas vid de allvarligaste och farligaste brotten, måste kunna användas vid misstanke om de brott som 1952 års tvångsmedelslag omfattar och under de förutsättningar som gäller enligt den lagen. Den brottslighet som faller inom Säkerhetspolisens ansvarsområde är som framgått speciell till sin karaktär och utredningarna berör en begränsad krets människor. Detta innebär att användningen av hemlig dataavläsning, på samma sätt som de övriga tvångsmedlen, måste kunna accepteras vid utredning av dessa brott. Precis som för de andra tvångsmedlen finns det också ett så påtagligt behov av att i brådskande situationer kunna börja verkställa beslut om hemlig dataav-

läsning vid sådana brott, att åklagares interimistiska beslutanderätt bör gälla även för hemlig dataavläsning enligt lagen.

Lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Enligt 28 § lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. får åklagare interimistiskt fatta beslut om bl.a. hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Beslutet skall genast anmälas till rätten, som snabbt skall pröva ärendet.

Hemlig dataavläsning bör omfattas av de regler som anges i den nu aktuella lagen. Åklagare skall med andra ord ha interimistisk beslutanderätt även rörande detta tvångsmedel under de förutsättningar som gäller enligt lagen.

Lagen om särskild utlänningskontroll

Hemlig teleavlyssning och hemlig teleövervakning får i vissa fall äga rum även enligt lagen om särskild utlänningskontroll. Åtgärder enligt den lagen syftar framför allt till att förebygga terrordåd. Om det finns synnerliga skäl får rätten under vissa förutsättningar meddela Rikspolisstyrelsen eller polismyndighet tillstånd enligt 27 kap. RB till hemlig teleavlyssning och hemlig teleövervakning (20 § första stycket). Förutsättningen är att åtgärden är av betydelse för att utröna om utlänningen eller en organisation eller grupp som han tillhör eller verkar för planlägger eller förbereder terroristbrott (19 § första stycket).

Bestämmelserna i lagen om särskild utlänningskontroll skiljer sig principiellt från rättegångsbalkens bestämmelser om tvångsmedel. En avgörande skillnad är att lagen används i spaningssyfte eller i s.k. preventivt syfte och inte i syfte att erhålla bevisning om kända, begångna brott. Tvångsmedlen används med andra ord utanför en förundersökningssituation för att de brottsbekämpande myndigheterna skall ha möjlighet att få reda på om utlänningen eller om organisationen eller gruppen som utlänningen tillhör eller verkar för planlägger eller förbereder terroristbrott.

En parlamentarisk kontroll av reglerna sker årligen genom att regeringen lämnar en skrivelse till riksdagen. Den senaste redovis-

ningen gjordes i regeringens skrivelse 2004/05:44. Av redovisningen framgår att Säkerhetspolisen inte i något fall under tiden den 1 juli 2003 till den 30 juni 2004 ansökte hos regeringen om utvisning enligt lagen. Regeringen biföll under perioden en och avslog en ansökan om upphävande av tidigare meddelande utvisningsbeslut.

Den internationella terrorismen har under senare år allt mer kommit att dra fördel av öppnare gränser och avancerad informationsteknik. Det är numera snarare regel än undantag att terrornätverk sträcker sig över ett flertal länder samt att stämpling, förberedelse och försök till ett terroristbrott äger rum i ett eller flera andra länder än det land där terroristbrottet skall utföras. Att hindra och bekämpa internationell terrorism på ett effektivt sätt är en angelägenhet för alla stater, även om de planerade terroristbrotten sker utanför den egna statens territorium. Det internationella samarbetet på detta område har därför förstärkts och allt mer kommit att inriktas på att förebygga och förhindra terroristbrott oavsett var de befaras äga rum (prop. 2002/03:38 s. 82).

I Sverige finns medlemmar och sympatisörer till organisationer eller grupperingar som i sina respektive hemländer samt internationellt bedriver verksamhet som kan betecknas som terrorism. Som nämndes har det senaste decenniet inneburit en globalisering och internationalisering av sådana grupper, organisationer och strukturer. Det är givet att personerna som agerar i sådana sammanhang behöver ha kontakt med varandra för att utbyta information. Det är välkänt att exempelvis Internet används som ett effektivt redskap i den verksamheten. Informationen som utbyts är ofta krypterad. I terrorismbekämpningen finns det bl.a. mot den bakgrunden ett behov av att hemlig dataavläsning blir möjlig att använda även enligt lagen om särskild utlänningskontroll. Vi lägger därför fram ett sådant förslag. Det måste dock framhållas att användning av hemlig dataavläsning i det sammanhanget säkerligen kommer att bli sällsynt men ändå värdefull i de fall metoden används.

9.4.14 Parlamentarisk kontroll

Förslag: Regeringen skall årligen till riksdagen redovisa de brottsutredande myndigheternas tillämpning av bestämmelserna om hemlig dataavläsning.

Som nämndes i avsnitt 2.9 tillämpas sedan många år den ordningen att regeringen årligen i en skrivelse till riksdagen redovisar de

brottsutredande myndigheternas tillämpning av hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Den tvångsmedelsanvändning som regleras i 1952 års tvångsmedelslag redovisas dock inte i skrivelserna. Redovisningarna medger en parlamentarisk kontroll över hur de hemliga tvångsmedlen har använts. Den parlamentariska kontrollen kan också med dagens ordning fördjupas på så sätt som skett genom att Justitieutskottet har företagit granskningar i egen regi av användningen av tvångsmedlen (se bet. 1997/98:JuU10).

Det är naturligt att det på liknande sätt sker en redovisning till riksdagen årligen av de brottsutredande myndigheternas tillämpning av bestämmelserna om hemlig dataavläsning. Det bör dock inte gälla när beslutet har sin grund i 1952 års tvångsmedelslag (se avsnitt 9.4.13).

10 Konsekvenser och genomförande

10.1 Ekonomiska konsekvenser av förslagen

Bedömning: Förslaget om att de brottsutredande myndigheternas tillgång till uppgifter om meddelanden uteslutande skall regleras i 27 kap. RB kan komma att kräva ett resurstillskott på högst tre miljoner kronor vardera för åklagar- respektive domstolsväsendet. I övrigt innebär förslagen i betänkandet inte några sådana ekonomiska konsekvenser att det behövs resursförstärkningar till någon del av statens verksamhet.

Våra förslag i de delar som gäller operatörernas anpassningsskyldighet och medverkan vid verkställighet av tvångsmedelsbeslut innebär en viss skärpning av kraven på operatörerna. Det kommer att leda till en något större kostnad för dessa än de har i dag. Liksom är fallet med de nuvarande kostnaderna kommer de dock att kunna finansieras genom att operatörerna för dessa vidare på sina abonnenter. Den avgiftshöjning som på detta sätt kan komma att drabba respektive abonnent är försumbar.

Enligt 14 och 15 §§ kommittéförordningen (1998:1474) skall det i ett betänkande finnas redovisat vissa konsekvenser av de förslag som presenteras. Det gäller särskilt de ekonomiska konsekvenserna. Om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, skall sådana konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, skall också dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, skall kommittén föreslå en finansiering.

Våra förslag innebär bl.a. att de brottsutredande myndigheternas tillgång till uppgifter som angår särskilda elektroniska meddelanden blir exklusivt reglerad genom tvångsmedlet övervakning i 27 kap. 19 § RB. Den inhämtning av historiska uppgifter som sker i dag med stöd av lagen om elektronisk kommunikation kommer således att upphöra. Enligt beräkningar gjorda av Säkerhetspolisen rör det sig om drygt 4000 fall årligen. Mot bakgrund av det stora behov som finns i brottsutredningar av sådana uppgifter bedömer vi att minst det antalet ärenden i framtiden kommer att föras till domstol av åklagare för beslut om övervakning. Såsom vi har utformat förslaget är det dessutom möjligt att antalet fall ökar något. I beräkningarna av de ekonomiska konsekvenserna utgår vi därför från en ökning till drygt 5000 domstolsärenden årligen om övervakning.

Det är svårt att bedöma hur ärendena kommer att fördelas rent geografiskt. Vi har antagit att den största andelen, kanske 3000 ärenden, kommer att beröra de tre storstadsregionerna. Det är också svårt att bedöma den genomsnittliga tidsåtgången för varje ärende. Även om ärendena många gånger kräver snabba beslut och åklagare och domare behöver avbryta det han eller hon just då sysslar med, har vi beräknat 30 minuters arbete för båda yrkeskategorierna.

Mot den bakgrund som nu har angivits är det vår uppfattning dels att det framför allt i de tre storstadsregionerna kan komma att krävas ett resurstillskott i form av någon åklagar- och domartjänst i varje region, dels att tillströmningen av ärenden inte kommer att bli så stor i övriga delar av landet att ett resurstillskott är nödvändigt. Den totala kostnaden kan därför beräknas till högst tre miljoner kronor vardera för åklagar- respektive domstolsväsendet. Regeringen har i budgetpropositionen (prop. 2004/05:1) aviserat att rättsväsendet avses tillföras betydande anslagsökningar för åren 2006 och 2007. Inom den ramen bör det därför finnas möjlighet att finansiera de tillskott som vi nu bedömt nödvändiga.

Statens kostnader för att genomföra våra förslag i övrigt kan hållas relativt låga. Det rör sig framför allt om införskaffande av viss utrustning, informations- och utbildningsinsatser och verkställighetskostnader för att t.ex. identifiera tekniska hjälpmedel och genomföra hemlig dataavläsning. Det rör sig också om Rikspolisstyrelsens föreslagna prövningsrätt i frågor om anpassningsskyldighet. Vi bedömer att det inte finns något behov av resursförstärkningar för detta.

De förslag som rör den brottsutredande verksamheten kommer att öka effektiviteten i rättsväsendets arbete och leda till att fler

brott kan utredas och beivras. De vinster som rättsväsendet kan komma att göra genom förslagen kommer att uppstå på detta sätt. Några kostnadsbesparingar i egentlig mening kommer dock inte att uppstå. Tvärtom kan ett ökat antal fall som går till lagföring leda till att kostnaderna ökar inom vissa sektorer av rättsväsendet. Om t.ex. polisen blir effektivare kan det leda till en ökad arbetsbörda för åklagare och domstolar.

I betänkandet föreslår vi en utvidgning av anpassningsskyldigheten till att omfatta flera verksamheter och operatörer än i dagsläget. Regleringen innebär i sig att ansvaret blir tydligare i förhållande till nuvarande ordning, vilket bör leda till effektivitetsvinster för såväl operatörerna som de brottsutredande myndigheterna. Säkert kommer ett betydande antal av de operatörer som inte tidigare har omfattats av skyldigheten att bli undantagna från kravet på anpassning efter beslut av Rikspolisstyrelsen. Det stora flertalet behöver dock uppfylla kravet genom att vidta olika anpassningsåtgärder. Vi behandlar frågan om kostnader för åtgärderna i avsnitt 6.6.5. Där framgår bl.a. att den ordning som gäller i dag även skall gälla fortsättningsvis, dvs. operatörerna skall stå för de kostnader som uppkommer i det avseendet. Som vi också konstaterade i det avsnittet har vi utan framgång försökt att få detaljerade uppgifter från operatörerna i kostnadsfrågan men inte fått något tillräckligt underlag för beräkningar. Den kostnad som med vårt förslag skulle tillkomma och i första hand belasta operatörerna är därför svår för oss att uppskatta. Vi ser det dock som närmast självklart att operatörerna kommer att vältra över kostnaderna på sina abonnenter, dvs. såväl stat, kommuner och företag som privatpersoner. På så sätt sker det en ”pulvrisering”. Den avgiftshöjning som på detta sätt kan komma att drabba respektive abonnent är försumbar. Också när det gäller det krav vi föreslår i avsnitt 8 om medverkan från operatörernas sida vid verkställigheten av tvångsmedelsbesluten, är det självklart att det kommer att ske en övervältring av kostnaderna på abonnenterna

Även om regeringen i en lagrådsremiss den 3 mars 2005 (Kostnadsansvar för hemlig teleavlyssning m.m.) har föreslagit att den som lämnar ut uppgifter enligt 6 kap. 22 § första stycket 2 och 3 LEK inte har rätt till ersättning för det, skall, när det gäller operatörernas kostnader, också nämnas att förslaget i avsnitt 5.4 om en effektiv tillgång till uppgifter om abonnemang kommer att innebära en viss effektivisering även för operatörerna, som inte längre behöver hantera förfrågning från de brottsutredande myndigheterna om abonnemangsuppgifter.

I det sammanhanget kan nämnas att några ledamöter i den referensgrupp som är knuten till beredningen har framfört synpunkten att utnyttjandet av operatörernas tjänster inte bör vara helt kostnadsfritt för de brottsutredande myndigheterna.

Det skall också nämnas att PTS har fått regeringens uppdrag att beskriva konsekvenserna för operatörerna av anpassningsskyldigheten. Beskrivningen skall omfatta vad skyldigheten innebär i form av kostnader och administrativ börda och hur skyldigheten kan påverka marknaden för elektronisk kommunikation. Uppdraget till PTS innefattar också att utreda vilka konsekvenser som förslagen om att rätt till ersättning inte skall föreligga kan få för mindre operatörer i form av kostnader och administrativ börda. Uppdraget skall redovisas senast den 1 juli 2005.

Förslagens betydelse för brottslighet och brottsförebyggande arbete har redovisats på andra ställen i betänkandet.

10.2 Ikraftträdande och övergångsbestämmelser

Förslag: Förslagen i betänkandet skall träda i kraft den 1 januari 2007. Några övergångsbestämmelser skall inte finnas.

Förslagen i betänkandet bör kunna träda i kraft den 1 januari 2007.

Vi erinrar om förslaget i avsnitt 6.6.8 om att de operatörer vars verksamhet, till skillnad från i dag, kommer att omfattas av anpassningsskyldigheten skall få en viss tid för att vidta de åtgärder som krävs. Som vi kom fram till i det fallet bör dock tiden från det att den ändrade lagstiftningen utfärdas till dess att den träder kraft inte vara längre än ett år.

Några övergångsbestämmelser till de föreslagna författningsändringarna behövs inte. Vad gäller sådana bestämmelser måste dock följande nämnas.

När bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning ändrades den 1 oktober 2004 till att även avse telemeddelanden som redan hade befordrats, alltså historiska uppgifter, föreskrevs att tillstånd till tvångsmedlen för tiden före rättens beslut inte fick avse tiden före ikraftträdandet. Regeringen motiverade den begränsningen med att ange att möjligheten att inhämta sådana telemeddelanden inte borde ges retroaktiv effekt (prop. 2002/03:74 s. 46). I det sammanhanget måste det hållas i minnet att en ”parallell” möjlighet för de brottsutredande myndigheterna att få tillgång till historiska uppgifter hittills har funnits i 6 kap. 22 §

första stycket 3 LEK. Vi föreslår att den bestämmelsen i lagen om elektronisk kommunikation skall upphävas och att de brottsutredande myndigheternas tillgång till historiska uppgifter uteslutande skall regleras i 27 kap. RB enligt bestämmelserna om avlyssning och övervakning.

Vi har på flera ställen i betänkandet redogjort för den stora betydelse som uppgifterna har i brottsutredningsarbetet (se t.ex. avsnitt 7). I samband med att vårt förslag till ändring av övervakningsbestämmelsen i 27 kap. 19 § RB träder i kraft är det med hänsyn till effektiviteten i brottsutredningsarbetet inte nödvändigt eller ens acceptabelt att föreskriva några begränsande övergångsbestämmelser till den ändringen av den typ som fanns när paragrafen senast ändrades. Särskilt i de fall där det för dagen saknas en skäligen misstänkt person, skulle en sådan begränsning i praktiken innebära en slags ”amnesti” för en mycket stor mängd ännu outredd brottslighet. Historiska uppgifter om meddelanden skulle inte kunna inhämtas genom övervakning för tiden före det att ändringen träder i kraft och bestämmelsen i lagen om elektronisk kommunikation upphör att gälla. Om en begränsande övergångsbestämmelse införs i rättegångsbalken, kan en alternativ lösning vara att tillåta att bestämmelsen i lagen om elektronisk kommunikation får användas även efter ikraftträdandet, när uppgifterna angår ett meddelande som har befordrats före den tidpunkten.

Vi nämnde i avsnitt 9.4.8 att hemlig dataavläsning kan innebära att de brottsutredande myndigheterna får tillgång till sådan information i informationssystemet som så att säga redan fanns där när tillståndet gavs, alltså en slags historiska uppgifter. Det är inte lämpligt eller ens möjligt att begränsa tillgången till sådana uppgifter vid verkställigheten av tvångsmedlet till att enbart avse uppgifter som finns vid tiden för ikraftträdandet och som tillkommer därefter.

11 Författningskommentar

11.1 Förslaget till lag om ändring i brottsbalken

4 kap. 8 §

Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller som sådant meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.

Bestämmelsen reglerar brotten brytande av post- eller telehemlighet. I avsnitt 3.3 kom vi fram till att begreppet telemeddelande skulle mönstras ut ur rättegångsbalken och ersättas av begreppet meddelande. I enlighet med detta har även den nu aktuella bestämmelsen ändrats. Vi kom också fram till att de begrepp som innehöll uttrycket tele i tvångsmedelsbestämmelserna skulle ersättas med andra begrepp. Det finns en mängd författningar med ord där uttrycket tele ingår i någon form. Ett sådant ord är telebefordringsföretag. De begreppen ändrades inte i samband med att telelagen upphävdes och lagen om elektronisk kommunikation trädde i kraft. Det ankommer inte på oss att utreda om det behövs några förändringar av dessa begrepp i författningarna, såvida inte saken har en direkt koppling till vårt arbete. Vi har därför låtit begreppen telebefordringsföretag och telehemlighet vara kvar i den nu aktuella bestämmelsen.

11.2 Förslaget till lag om ändring i rättegångsbalken

27 kap. Om beslag, avlyssning m.m.

27 kap. 18 §

Ett meddelande som befordras eller har befordrats i ett elektroniskt kommunikationsnät får efter tillstånd i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.

Sådan avlyssning får användas vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,

2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff eller

3. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Ett tillstånd enligt denna paragraf omfattar även sådana åtgärder som avses i 19 §.

Med elektroniskt kommunikationsnät i detta kapitel avses detsamma som i lagen (2003:389) om elektronisk kommunikation med undantag för nät som enbart är avsett för utsändning av program i ljudradio eller television.

Bestämmelsen i 27 kap. 18 § RB innehåller de grundläggande bestämmelserna om hemlig teleavlyssning. I dagsläget anges i *första stycket* att hemlig teleavlyssning innebär att telemeddelanden som befordras eller har befordrats till eller från ett telefonnummer, kod eller annan teleadress i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.

Vi har i avsnitt 3 redovisat våra överväganden när det gäller rättegångsbalkens terminologi på det aktuella området och bl.a. kommit fram till att den behöver moderniseras och göras mer oberoende av den snabba tekniska utvecklingen. Särskilt mot bakgrund av att telelagen relativt nyligen ersattes av lagen om elektronisk kommunikation är det nödvändigt att flera av de begrepp som numera finns i bestämmelserna om hemlig teleavlyssning mönstras ut ur lagtexten och ersätts av andra. Som vi kom fram till i avsnitt 3 rör det exempelvis begreppen telemeddelande och teleadress. Den nu aktuella bestämmelsen har ändrats så att telemeddelande har ersatts av meddelande och så att bestämmelsen inte anknyter till begreppet teleadress. Det skall vara fråga om en överföring av in-

formation med exempelvis fast telefon, mobiltelefon, telefax, modem eller Internetterminal. Meddelandet skall befordras eller ha befordrats i ett elektroniskt kommunikationsnät.

Vad som avses med detta begrepp följer av förslaget till definition i fjärde stycket, där det sägs att med ett sådant nät avses detsamma som i lagen om elektronisk kommunikation med undantag för elektroniskt kommunikationsnät som enbart är avsett för utsändning av program i ljudradio eller television. Även begreppet hemlig teleavlyssning har mönstrats ut ur lagtexten. I enlighet med detta har kapitlets rubrik ändrats. Dessutom markeras numera i lagtexten att tvångsmedlet får användas bara efter tillstånd (se 27 kap. 21 § RB).

Genom ett nytt *tredje stycke* får övervakningsuppgifter enligt 27 kap. 19 § RB (uppgifter om meddelanden som befordras eller har befordrats och för lokalisering eller identifiering av ett tekniskt hjälpmedel) hämtas in även vid avlyssning. Dessutom får meddelanden hindras från att nå fram till eller lämna ett tekniskt hjälpmedel. Frågan har behandlats i avsnitt 4.6. Genom den föreslagna ändringen behöver åklagaren inte ansöka om tillstånd till både avlyssning och övervakning. Faller förutsättningarna för tillstånd till avlyssning så faller även rätten för de brottsutredande myndigheterna enligt tredje stycket. Om det kvarstår ett behov av att få ut sådana uppgifter eller att hindra meddelanden från att nå fram till eller lämna ett tekniskt hjälpmedel, får åklagaren ansöka om tillstånd till övervakning enligt 27 kap. 19 § RB.

I ett nytt *fjärde stycke* i bestämmelsen ges en definition av begreppet elektroniskt kommunikationsnät, som används i 27 kap. 18-21 §§ RB. Enligt 1 kap. 7 § LEK är ett elektroniskt kommunikationsnät system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs. Den definitionen skall gälla även i 27 kap. RB med undantag för nät som enbart är avsett för utsändning av program i ljudradio eller television. Frågan har behandlats i avsnitt 3.4.

27 kap. 19 §

Uppgifter får efter tillstånd i hemlighet hämtas in om meddelanden som befordras eller har befordrats med tekniskt hjälpmedel till eller från ett elektroniskt kommunikationsnät och för lokalisering eller

identifiering av ett sådant tekniskt hjälpmedel. Meddelanden får även hindras från att nå fram till eller lämna ett sådant tekniskt hjälpmedel.

Med uppgifter för lokalisering i första stycket avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits. Med uppgifter för identifiering i samma stycke avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden.

Åtgärder som avses i första stycket (övervakning) 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.

Bestämmelsen i 27 kap. 19 § RB innehåller de grundläggande bestämmelserna om hemlig teleövervakning. I dagsläget anges i *första stycket* att 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.

Vi har i avsnitt 3 redovisat våra överväganden när det gäller rättegångsbalkens terminologi på det aktuella området och bl.a. kommit fram till att den behöver moderniseras och göras mer oberoende av den snabba tekniska utvecklingen. Särskilt mot bakgrund av att telelagen relativt nyligen ersattes av lagen om elektronisk kommunikation är det nödvändigt att flera av de begrepp som numera finns i bestämmelserna om hemlig teleövervakning mönstras ut ur lagtexten och ersätts av andra. Som vi kom fram till i avsnitt 3 rör det exempelvis begreppen telemeddelande och teleadress. Den nu aktuella bestämmelsen har ändrats så att telemeddelande har ersatts av meddelande och så att bestämmelsen anknyter till begreppet tekniskt hjälpmedel. I detta ligger att det skall vara fråga om en överföring av information med exempelvis fast telefon, mobiltelefon, telefax, modem eller Internetterminal. Meddelandet skall enligt bestämmelsen befordras eller ha befordrats till eller från ett elektroniskt kommunikationsnät. I det ligger att uppgifterna kan avse överföringen i nätet, alltså t.ex. färdväg.

Vad som avses med elektroniskt kommunikationsnät följer av förslaget i 27 kap. 18 § fjärde stycket RB, där det sägs att med ett sådant nät avses detsamma som i lagen om elektronisk kommunikation med undantag för elektroniskt kommunikationsnät som enbart är avsett för utsändning av program i ljudradio eller television. Även begreppet hemlig teleövervakning har mönstrats ut ur lagtexten. Dessutom markeras numera i lagtexten att tvångsmedlet får användas bara efter tillstånd (se 27 kap. 21 § RB).

Som har redovisats i avsnitt 4.4 är det, när det gäller mobiltelefoner, möjligt att ta reda på från vilket geografiskt område ett samtal rings. När telefonen enbart är påslagen, utan att det samtidigt pågår ett samtal, är det också möjligt att lokalisera i vilket område telefonen finns. En ändring har skett i första stycket för att göra det tydligt att sådana lokaliseringsuppgifter, såväl historiska uppgifter som realtidsuppgifter, får inhämtas vid användning av det aktuella tvångsmedlet. Det har också skett ett förtydligande så att det framgår att möjligheten att hindra meddelanden avser såväl att meddelandet når fram till ett tekniskt hjälpmedel som att meddelanden lämnar hjälpmedlet.

I första stycket har dessutom lagts till att uppgifter för identifiering omfattas av tvångsmedlet. Bakgrunden till det tillägget, som har behandlats utförligt i avsnitt 4.5, är de problem som finns i brottsutredningar med att anonyma kontantkort i mycket stor utsträckning används i brottslig verksamhet. När uppgifter för identifiering kan inhämtas genom övervakning enligt paragrafen kommer det problemet att minska. Vad som avses med uppgifter för identifiering förklaras i andra stycket.

Andra stycket är nytt och ger en definition av två av de begrepp som används i första stycket. Med uppgifter för lokalisering avses uppgifter om var ett visst tekniskt hjälpmedel finns eller har funnits. Med uppgifter för identifiering avses uppgifter som inhämtas för att klargöra vilket visst tekniskt hjälpmedel som används för befordran av meddelanden.

Tredje stycket var tidigare andra stycke i paragrafen. Förutom att begreppet övervakning numera används i bestämmelsen har en hänvisning gjorts till första stycket. Det har framförts till oss att även hets mot folkgrupp enligt 16 kap. 8 § BrB borde tas med i bestämmelsen. Vi har dock inte behandlat den frågan.

27 kap. 20 §

Avlyssning och övervakning enligt 18 respektive 19 § får, utom i fall som avses i tredje stycket, bara ske om någon är skäligen misstänkt för brottet. Åtgärden skall vara av synnerlig vikt för utredningen och får, utom i fall som avser identifiering av tekniska hjälpmedel, bara avse

1. sådana tekniska hjälpmedel 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. sådana tekniska hjälpmedel som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Övervakning i syfte att identifiera tekniska hjälpmedel får avse sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte.

Vid förundersökning angående brott som anges i 18 § andra stycket får övervakning användas även om det inte finns någon som är skäligen misstänkt för brottet.

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

I paragrafen anges de närmare förutsättningar som måste vara uppfyllda för att hemlig teleavlyssning och hemlig teleövervakning skall få användas. I avsnitt 3.6 kom vi fram till att de begreppen skulle ersättas av avlyssning och övervakning. I avsnitt 3.3-3.5 behandlades andra begreppsfrågor. Vi kom då fram till att begreppen telemeddelande och telenät skulle mönstras ut ur lagtexten och ersättas av begreppen meddelande respektive elektroniskt kommunikationsnät. Dessutom skulle begreppet teleadress inte längre användas utan bestämmelserna skulle anknyta till begreppet tekniskt hjälpmedel. Ändringar har skett i paragrafen i enlighet med detta. En särskild definition av begreppet elektroniskt kommunikationsnät föreslås i 27 kap. 18 § fjärde stycket RB.

I *första stycket* har ett tillägg gjorts mot bakgrund av frågan om identifiering av tekniska hjälpmedel (se avsnitt 4.5). I stycket anges liksom tidigare att det krävs en skäligen misstänkt person för att avlyssning och övervakning skall få användas och att åtgärden skall vara av synnerlig vikt för utredningen. Dessutom finns angivet vilka tekniska hjälpmedel med anknytning till den skäligen misstänkte

som åtgärden får avse. I fall när identifiering av tekniskt hjälpmedel kommer i fråga rörande en misstänkt person är det oklart vilka tekniska hjälpmedel som den personen använder eller kan komma att kontakta etc. Kraven på anknytning som finns mellan den misstänkte och det tekniska hjälpmedlet kan därför inte gälla i sådana fall.

I ett nytt *andra stycke* klargörs vilka tekniska hjälpmedel som metoden att identifiera hjälpmedel får avse. Det skall röra sådana tekniska hjälpmedel som kan antas användas eller komma att användas för meddelanden till eller från den misstänkte. Enligt första stycket skall dock alltid en skäligen misstänkt person finnas och åtgärden vara av synnerlig vikt för utredningen. Det tidigare andra stycket är efter förändringarna *fjärde stycke* i bestämmelsen. En mindre språklig ändring har skett i det stycket.

I avsnitt 4.3 behandlade vi frågan om övervakning även utan misstänkt gärningsman. Som en följd av förslaget i den delen har ett nytt *tredje stycke* införts i paragrafen. Förslaget skall ses mot bakgrund av att 6 kap. 22 § första stycket 3 LEK föreslås bli upphävd. Innebörden av det nya tredje stycket är att övervakning får användas vid förundersökning rörande brott som kan bli föremål för avlyssning enligt 27 kap. 18 § RB, oavsett om det finns någon som är skäligen misstänkt för brottet eller inte. I avsnitt 4.3 finns närmare uppgifter om bakgrunden till bestämmelsen. Även i ett sådant fall krävs att det är av synnerlig vikt för utredningen att uppgifterna hämtas in (se första stycket i den nu aktuella paragrafen), att det elektroniska kommunikationsnätet har viss omfattning (se fjärde stycket i den nu aktuella paragrafen) och att domstolen, som huvudregel, beslutar om tillstånd (se 27 kap. 21 § första stycket RB).

27 kap. 21 §

Frågor om tillstånd till avlyssning och övervakning enligt 18 respektive 19 § prövas av rätten på ansökan av åklagaren. Åklagaren får dock i brådskande fall fatta beslut om övervakning enligt 19 §. Ett sådant beslut skall genast skriftligen anmälas hos rätten, som skyndsamt skall pröva frågan.

I ett beslut att tillåta avlyssning eller övervakning skall 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. Rätten får också i övrigt föreskri-

va villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.

I tillstånd till avlyssning eller övervakning skall det särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga elektroniska kommunikationsnät.

Den aktuella paragrafen behandlar domstolens beslut om hemlig teleavlyssning och hemlig teleövervakning. I avsnitt 3.6 kom vi fram till att de begreppen skulle ersättas av avlyssning och övervakning. Bestämmelsens tre stycken har ändrats i enlighet med detta.

I bestämmelsens *första stycke* framgår att det är domstolen som fattar beslut om tillstånd till avlyssning respektive övervakning. I stycket har ett tillägg gjorts genom att åklagare ges rätt att i brådskande fall fatta interimistiska beslut om övervakning. Frågan har behandlats i avsnitt 4.3. Bedömningen av om rekvisitet ”i brådskande fall” är uppfyllt måste ske utifrån en helhetsbedömning av omständigheterna i det enskilda fallet. Det skall då vara så bråttom att ändamålet med en åtgärd kan antas gå förlorat om man väntar med att företa den.

Det anges också i första stycket att åklagaren är skyldig att genast anmäla beslutet till rätten, dvs. till den behöriga domstolen, som skyndsamt skall pröva frågan. Med rekvisitet ”genast” avses att anmälan skall göras så snart det kan ske med hänsyn till den ordinarie tjänstetiden vid domstolen. Bestämmelsen innebär således inte någon skyldighet för åklagaren att anmäla beslutet till rätten utom ordinarie tjänstetid. En anmälan skall göras skriftligen. Av rättssäkerhets- och kontrollskäl skall domstolsprövning ske också i de fall det interimistiska beslutet redan har verkställts, och även om åtgärden redan har upphört. Prövningen skall i dessa fall gå ut på att kontrollera om det fanns laga grund för åklagarens interimistiska beslut. Om rätten kommer fram till att tvångsmedlet skall bestå, kan domstolen besluta om villkor eller ytterligare villkor för användningen av tvångsmedlet eller ändra av åklagaren meddelade villkor.

Vi behandlade frågan om teleadress i avsnitt 3.5 och föreslog då att det begreppet skulle mönstras ut ur lagtexten. I stället skulle bestämmelserna anknytas till begreppet tekniskt hjälpmedel. Paragrafens *andra stycke* har utformats så att det i beslutet att tillåta avlyssning eller övervakning inte behöver anges vilket tekniskt hjälpmedel som avses. Det skall bl.a. ses mot bakgrund av förslaget i avsnitt 4.3 och 4.5 om övervakning utan misstänkt gärningsman, där det särskilda tekniska hjälpmedlet är okänt för de brottsutre-

dande myndigheterna, och problemen med anonyma kontantkort och svårigheten att identifiera tekniska hjälpmedel, vilket skapar stora effektivitetsförluster i det brottsutredande arbetet (jfr även avsnitt 5.6). Det är i stället tillräckligt att bestämmelsen föreskriver att tillståndstiden skall anges i beslutet.

Som ett förtydligande av att det står domstolens fritt att i övrigt föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när, har ett tillägg gjorts i andra stycket med det innehållet. Någon ändring i förhållande till nuvarande ordning är inte avsedd. Villkoren kan gälla exempelvis särskilda tekniska hjälpmedel, vissa geografiska områden eller vissa basstationer.

I paragrafens *tredje stycke* har begreppet allmänt tillgängligt telenät ersatts av allmänt tillgängligt elektroniskt kommunikationsnät. Frågan om att ersätta begreppet telenät med elektroniskt kommunikationsnät behandlas i avsnitt 3.4. En särskild definition av begreppet elektroniskt kommunikationsnät finns i 27 kap. 18 § fjärde stycket RB.

27 kap. 22 §

Avlyssning enligt 18 § får inte ske av meddelanden mellan den misstänkte och hans försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant meddelande, skall avlyssningen avbrytas.

Upptagningar och uppteckningar skall, i den mån de omfattas av förbudet, omedelbart förstöras.

I 27 kap. 22 § RB finns i dag ett förbud mot hemlig teleavlyssning vad avser telefonsamtal eller andra telemeddelanden mellan den misstänkte och hans försvarare. Som en följd av att vi i avsnitt 3.3 och 3.6 kom fram till att begreppen telefonsamtal, telemeddelande och hemlig teleavlyssning skulle mönstras ut ur rättegångsbalken och ersättas av meddelande och avlyssning, har *första stycket* i den aktuella paragrafen ändrats i enlighet med detta.

27 kap. 23 §

Om det inte längre finns skäl för ett beslut om avlyssning eller övervakning enligt 18 respektive 19 §, skall åklagaren eller rätten omedelbart häva beslutet.

27 kap. 23 a §

Om det vid avlyssning eller övervakning enligt 18 respektive 19 § har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avlyssning eller övervakning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller

2. det finns särskilda skäl.

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

Enligt 27 kap. 23 § RB skall åklagaren eller rätten omedelbart häva beslutet om hemlig teleavlyssning eller hemlig teleövervakning när det inte längre finns skäl för åtgärden.

Bestämmelsen i 27 kap. 23 a § RB, som föreslås i prop. 2004/05:143, reglerar användningen av överskottsinformation som framkommer vid verkställigheten av aktuella tvångsmedel.

Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har de aktuella paragraferna ändrats så att de begreppen har ersatts av avlyssning och övervakning.

27 kap. 24 §

En upptagning eller uppteckning som gjorts vid avlyssning enligt 18 § skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.

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

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

De upptagningar eller uppteckningar som görs vid hemlig teleavlyssning skall enligt 27 kap. 24 § första stycket RB granskas snarast

möjligt. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppet hemlig teleavlyssning skulle mönstras ut ur rättegångsbalken, har den nu aktuella paragrafens *första stycke* ändrats så att det begreppet har ersatts av avlyssning. Lydelserna av *andra* och *tredje styckena* är hämtade från förslagen i prop. 2004/05:143 om överskottsinformation vid användning av hemliga tvångsmedel.

27 kap. 25 §

Har rätten lämnat tillstånd till avlyssning eller övervakning enligt 18 respektive 19 §, får de tekniska hjälpmedel som behövs för åtgärden användas.

En enskild är skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av avlyssning eller övervakning.

I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om avlyssning och övervakning som gäller för den som driver verksamhet som avses i 6 kap. 19 § den lagen.

Enligt paragrafens *första stycke* får de tekniska hjälpmedel som behövs användas för att verkställa beslut om hemlig teleavlyssning eller hemlig teleövervakning. Av detta följer även att de tekniska hjälpmedlen får anslutas, underhållas och återtas, dvs. enskilda, (operatörerna) har bl.a. en skyldighet att biträda och lämna tillträde för polisen. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har det aktuella stycket ändrats så att de begreppen har ersatts av avlyssning och övervakning.

I avsnitt 8 behandlade vi frågan om skyldighet för enskilda att medverka i högre grad vid verkställighet av tvångsmedelsbesluten än vad som följer av första stycket i paragrafen. Vi kom där fram till att det bör finnas en sådan lagreglerad skyldighet vid sidan om anpassningsskyldigheten. I ett nytt *andra stycke* i bestämmelsen föreskrivs numera att enskilda är skyldiga att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning och övervakning. Det är givetvis bara den vars medverkan behövs som kan bli aktuell för en sådan begäran. Den krets som kan träffas av skyldigheten är vidare än den som omfattas av anpassningsskyldigheten. Det är mycket svårt att avgränsa den kretsen i lagtext. Särskilt som någon sanktion inte föreskrivs, är det möjligt att använda begreppet enskild i bestämmelsen.

Medverkan kan bestå i allt från att lämna information om funktioner och andra tekniska förutsättningar som är nödvändiga för att kunna verkställa tvångsmedelsbesluten till att tillhandahålla teknisk utrustning. Som exempel kan nämnas att operatören lämnar uppgift om vilka tjänster som tillhandahålls, nätets uppbyggnad och konstruktion, logiska och fysiska punkter för inkoppling och om avgränsningar som säkerställer att inte större ingrepp än nödvändigt sker. I skyldigheten ligger också att snabbt vidta åtgärder från det att verkställigheten har beställts av polisen. Begreppet ”genast” i bestämmelsen markerar att det inte skall röra sig om mer än någon timmes väntetid för de brottsutredande myndigheterna under kontorstid. Den tidsgränsen bör gälla även i övrigt för de operatörer som på annan tid har personella resurser avdelade för drift- och nätövervakning.

Det tidigare andra stycket har placerats som *tredje stycke* i paragrafen. Det innehåller en hänvisning till bestämmelserna om anpassningsskyldighet i lagen om elektronisk kommunikation (se nedan 6 kap. 19 § LEK).

27 kap. 26 §

Offentliga ombud skall bevaka enskildas integritetsintressen i ärenden hos domstol om avlyssning enligt 18 §.

Ett offentligt ombud har rätt att ta del av vad som förekommer i ärendet, att yttra sig i ärendet och att överklaga rättens beslut.

27 kap. 28 §

När en ansökan om avlyssning enligt 18 § har kommit in till rätten, skall rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet skall åklagaren och det offentliga ombudet närvara.

Om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med tvångsmedlet, får sammanträde hållas och beslut fattas utan att ett offentligt ombud har varit närvarande eller annars fått tillfälle att yttra sig.

Ett uppdrag som offentligt ombud gäller även i högre rätt.

Bestämmelserna i 27 kap. 26-30 §§ RB rör offentliga ombud som skall bevaka enskildas integritetsintressen i ärenden om hemlig teleavlyssning. Reglerna trädde i kraft den 1 oktober 2004. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppet hemlig teleav-

lyssning skulle mönstras ut ur rättegångsbalken, har 27 kap. 26 och 28 §§ RB ändrats så att det begreppet har ersatts av avlyssning.

11.3 Förslaget till lag om hemlig dataavläsning

Definition

1 § Med hemlig dataavläsning avses i denna lag att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål.

Paragrafen innehåller en definition av tvångsmedlet hemlig dataavläsning. Bakgrunden till förslaget behandlas i avsnitt 9.4.1. Hemlig dataavläsning är ett tvångsmedel som får användas endast av brottsutredande myndigheter. Att tvångsmedlet får användas endast vid förundersökning i brottmål framgår av bestämmelsen. Lydelsen i den delen ansluter till det uttryck som används i 1 § lagen om hemlig kameraövervakning, där det också framgår att tvångsmedlet används vid förundersökning i brottmål. Av den föreslagna bestämmelsen följer också att hemlig dataavläsning, liksom hemlig teleavlyssning (avlyssning enligt 27 kap. 18 § RB), hemlig teleövervakning (övervakning enligt 27 kap. 19 § RB) och hemlig kameraövervakning (enligt lagen om hemlig kameraövervakning), är tvångsmedel som verkställs i hemlighet, dvs. utan att den som åtgärden riktar sig mot har kännedom om den under verkställigheten.

Hemlig dataavläsning innebär att information som redan finns i informationssystem när tvångsmedlet börjar verkställas eller som därefter genereras avläses med hjälp av program eller annat tekniskt hjälpmedel.

Begreppet informationssystem används i många författningar och i andra sammanhang utan att det kan sägas finnas någon vedertagen definition. Det finns heller ingen anledning att definiera begreppet i detta sammanhang. Det är helt nödvändigt att använda ett teknikneutralt begrepp i lagtexten som täcker in de informationsmöjligheter och informationsvägar som finns nu och som kommer att finnas i framtiden. Begreppet skall med andra ord också kunna stå sig över tiden. En avgränsning av det informationssystem som tvångsmedlet rör skall göras i domstolens tillstånd (se 11 § nedan).

Som har framgått tidigare (avsnitt 3.5) används begreppet tekniskt hjälpmedel redan i dag i 27 kap. 25 § första stycket RB och innefattar såväl den hårdvara som den mjukvara som behövs för att

genomföra hemlig teleavlyssning och hemlig teleövervakning. Enligt vårt förslag till ändring av bl.a. 27 kap. 18-20 §§ RB kommer begreppet att användas i den betydelsen också i de paragraferna. Även i den nu aktuella bestämmelsen används begreppet tekniskt hjälpmedel i samma vida betydelse. För att få bestämmelsen något mera upplysande används även begreppet program som en exemplifiering av ett tekniskt hjälpmedel. Vilken information som programmet kommer att ge de brottsutredande myndigheterna i det enskilda fallet bestäms i samband med att programmet skapas. Givetvis måste då hänsyn tas bl.a. till det integritetsintrång som kan uppkomma.

När hemlig dataavläsning får äga rum

2 § Hemlig dataavläsning får äga rum bara efter tillstånd enligt denna lag.

Paragrafen klargör att hemlig dataavläsning bara får äga rum efter tillstånd enligt den nu aktuella lagen.

3 § Hemlig dataavläsning får äga rum vid förundersökning angående

1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,

2. försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff,

3. brott enligt 4 kap. 9 c § brottsbalken, brott enligt 16 kap. 8 § brottsbalken som inte är att anse som ringa, brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, eller

4. annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år.

I paragrafen, som behandlas i avsnitt 9.4.4, ges grundläggande förutsättningar för att hemlig dataavläsning skall kunna komma i fråga. För det första måste förundersökning om brott vara inledd och för det andra får endast misstanke om vissa allvarliga brott läggas till grund för åtgärden.

Att hemlig dataavläsning får äga rum endast om det har inletts en förundersökning förutsätter bl.a. att det finns anledning att anta att det har begåtts ett brott (se 23 kap. 1 § RB). Hemlig dataavläsning får alltså inte äga rum endast i förebyggande syfte eller som en allmän spaningsåtgärd.

Tillämpningsområdet när det gäller de brott vid vilka hemlig dataavläsning skall kunna komma ifråga är, med undantag för dataintrång, hets mot folkgrupp och barnpornografibrott enligt nedan, utformat på samma sätt som för avlyssning enligt 27 kap. 18 § RB och för hemlig kameraövervakning enligt 2 § lagen om hemlig kameraövervakning. Avgränsningen sker i den första punkten utifrån brottets minimistraff och i den sista punkten utifrån brottets straffvärde i det enskilda fallet.

Första punkten innebär att hemlig dataavläsning får äga rum vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Därmed omfattas exempelvis mord, grovt rån, grovt narkotikabrott och grov narkotikasmuggling. I *andra punkten* anges att hemlig dataavläsning får äga rum även vid straffbara fall av försök, förberedelse och stämpling till dessa brott. *Tredje punkten* anger särskilt att hemlig dataavläsning får äga rum vid dataintrång, hets mot folkgrupp som inte är att anse som ringa och vid barnpornografibrott som inte är att anse som ringa. Det är en angelägen uppgift att bekämpa den typen av brottslighet och i det arbetet kan hemlig dataavläsning bli ett effektivt hjälpmedel (jfr de brott som ger möjlighet att använda övervakning enligt 27 kap. 19 § RB). *Fjärde punkten* innehåller en straffvärdeventil och innebär att hemlig dataavläsning kan äga rum även vid andra brott om det kan antas att brottets straffvärde överstiger fängelse i två år. När straffvärdeventil infördes för hemlig teleavlyssning och hemlig kameraövervakning uttalade regeringen bl.a. följande om tillämpningen (prop. 2002/03:74 s. 34 f. och 48). Uttalandena har giltighet även när det gäller hemlig dataavläsning.

> Konstruktionen på ventilen bör vara sådan att rätten skall göra i princip samma typ av bedömning som den gör när den prövar om de omständigheter som åklagaren åberopar till stöd för att brottet faller under en viss brottsrubricering är tillräckliga för en sådan rubricering. Vid en tillämpning av ventilen skall dock rätten i stället utifrån omständigheterna värdera brottets straffvärde. Bedömningen utgår i första hand från omständigheterna kring gärningen som sådan. Också omständigheter kring gärningsmannens person skall vägas in om de är relevanta för själva gärningen, även om utrymmet för detta normalt är begränsat på det tidiga stadium i utredningen som det vanligtvis är fråga om.

Straffvärdehöjande eller straffvärdelindrande omständigheter enligt 29 kap. brottsbalken kring brottet skall beaktas vid denna bedömning i den mån de är kända.

Att en straffvärdeventil av det slag regeringen nu föreslår skall användas restriktivt följer av att det är fråga om hemlig tvångsmedelsanvändning mot enskild.

4 § Hemlig dataavläsning får äga rum, om

1. någon är skäligen misstänkt för brottet,

2. åtgärden är av synnerlig vikt för utredningen, och

3. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.

Hemlig dataavläsning får också äga rum när det inte finns någon som är skäligen misstänkt för brottet, om åtgärden syftar till att fastställa vem som skäligen kan misstänkas för brottet.

Paragrafen innehåller ytterligare förutsättningar för att hemlig dataavläsning skall få äga rum. Frågorna har behandlats i avsnitt 9.4.5 och 9.4.6.

Enligt *första stycket första punkten* krävs att det finns en skäligen misstänkt person för ett brott som får föranleda hemlig dataavläsning. Begreppet skäligen misstänkt har samma innebörd som enligt bestämmelserna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning (27 kap. 20 § RB och 3 § lagen om hemlig kameraövervakning). Skälig misstanke är en lägre misstankegrad än sannolika skäl, vilket som huvudregel krävs för häktning, men högre än ”kan misstänkas” (se 23 kap. 9 § RB). För att tvångsmedlen skall få användas krävs alltså som huvudregel att den person åtgärden avser är skäligen misstänkt för ett konkret brott. Enligt Ekelöf är begreppet skälig misstanke jämförbart med uttrycket ”antagligt” (se Rättegång V, sjunde upplagan, 1998 s. 113). Det är inte möjligt att med någon större precision ange det beviskrav som ligger i att någon är skäligen misstänkt utan frågan om brottsmisstankens styrka måste bedömas efter omständigheterna i det enskilda fallet. Prövningen av styrkan i misstankarna måste grunda sig på en objektiv och allsidig bedömning av utredningsmaterialet. JO har vid ett flertal tillfällen uttryckt saken så att det krävs att det finns konkreta omständigheter av viss styrka som pekar på att den misstänkte har begått brottet (se t.ex. JO 1993/94 s. 103 och 1992/93 s. 152 och 206). Detta innebär att brottsmisstan-

ken måste vara konkret grundad och att ett beslut om tvångsmedel aldrig kan grunda sig enbart på allmänna kunskaper om en persons livsföring eller hans tidigare brottslighet. Det skall också sägas att skälig misstanke om brott kan föreligga redan innan det har fastslagits att den gärning som har begåtts utgör brott. Detta medför att en person kan vara skäligen misstänkt redan innan det föreligger full klarhet om de objektiva brottsrekvisiten är uppfyllda, t.ex. så att skälig misstanke om mord föreligger mot en person redan innan det har med säkerhet slagits fast att ett mord har begåtts och i så fall vem som har mördats (SOU 1998:46 s. 486). I vissa fall (se andra stycket) skall dock hemlig dataavläsning kunna användas utan att det finns en skäligen misstänkt person.

I *första stycket andra punkten* i paragrafen anges att hemlig dataavläsning får användas endast om det är av synnerlig vikt för utredningen att åtgärden vidtas. Bestämmelsen innebär ett kvalitetskrav avseende de upplysningar som avläsningen kan ge. Utredningsläget skall göra hemlig dataavläsning nödvändig.

Enligt *första stycket tredje punkten* får beslut om hemlig dataavläsning fattas enbart om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Den proportionalitetsprincip som kommer till uttryck i bestämmelsen tar sikte på de negativa verkningar som en tvångsåtgärd kan ha på ett motstående intresse. Det brukar beskrivas så att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet skall stå i rimlig proportion till vad som står att vinna med åtgärden. Bestämmelsen innebär en skyldighet för rätten att såsom vid andra tvångsmedel alltid beakta principen när en begäran om hemlig dataavläsning skall prövas. Proportionalitetsprincipen får betydelse vid prövningen inte enbart för frågan om tillstånd skall ges eller inte, utan också för hur tillståndet skall utformas och vilka villkor som skall föreskrivas, t.ex. om vilka tvångsmedel som får verkställas samtidigt mot en misstänkt person, vilka delar av ett informationssystem som verkställigheten får avse och om vilket intrång som får ske för att genomföra åtgärden (se 11 §). Principen måste beaktas av de brottsutredande myndigheterna under hela verkställigheten.

Hemlig dataavläsning skall av effektivitetsskäl kunna användas även om det saknas en skäligen misstänkt person. Frågan har behandlats i avsnitt 9.4.6. Enligt *andra stycket* skall syftet med åtgärden i ett sådant fall vara att fastställa vem som skäligen kan misstänkas för brottet. Som följer av första stycket krävs det även i dessa fall att åtgärden är av synnerlig vikt för utredningen och att skä-

len för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för ett motstående intresse. När de brottsutredande myndigheterna med hjälp av tvångsmedlet har identifierat en skäligen misstänkt person, får domstolen på ansökan av åklagaren göra en ny prövning utifrån de omständigheter som föreligger vid det tillfället och utan de begränsningar som följer av den aktuella paragrafen vad gäller syftet med åtgärden och av 6 § vad gäller informationssystemet.

Vad som får avläsas

5 § Hemlig dataavläsning i fall som avses i 4 § första stycket får endast avse informationssystem som det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av. Avser åtgärden informationssystem i någon annans stadigvarande bostad, får hemlig dataavläsning äga rum endast om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av detta.

I paragrafen anges kraven på sambandet, eller kopplingen, mellan den misstänkte och det eller de informationssystem som hemlig dataavläsning får avse. Det rör alltså fall där det finns en skäligen misstänkt person. Frågan har behandlats i avsnitt 9.4.7. Av *första meningen* framgår att det skall finnas särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av informationssystemet. Det skall inte bara vara fråga om ett antagande om att den användningen har skett eller kommer att ske utan det skall finnas någon faktisk omständighet som tyder på detta.

I *andra meningen* uppställs ett högre krav på sambandet mellan den misstänkte och informationssystemet för det fall åtgärden avser informationssystem i någon annans stadigvarande bostad. Det skall då finnas synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av informationssystemet. Uttrycket kan sammanfattningsvis sägas innebära att det skall vara i det närmaste klart att den kopplingen finns.

6 § Hemlig dataavläsning i fall som avses i 4 § andra stycket får endast avse informationssystem som har använts eller används vid brottet.

När det saknas en skäligen misstänkt person krävs enligt paragrafen att åtgärden avser informationssystem som har använts eller an-

vänds vid brottet. Frågan har behandlats i avsnitt 9.4.6. Detta begränsar typiskt sett inte i sig vilken information som får avläsas eller hur den informationen senare får användas. Frågan om möjligheten att utnyttja överskottsinformation regleras i 8 §.

Genomförande av hemlig dataavläsning

7 § Vid genomförande av hemlig dataavläsning får olägenhet eller skada inte förorsakas utöver vad som är oundgängligen nödvändigt.

Hemlig dataavläsning får inte ske av sådana meddelanden mellan den misstänkte och hans försvarare som avses i 27 kap. 22 § rättegångsbalken. Om det framkommer under avläsningen att det är fråga om ett sådant meddelande, skall avläsningen omedelbart avbrytas. En upptagning skall omedelbart förstöras i den del där meddelandet förekommer.

Vid hemlig dataavläsning får med särskilt tillstånd de tekniska hjälpmedlen i hemlighet installeras på en plats som annars särskilt skyddas mot intrång.

Paragrafen reglerar vissa frågor vid genomförandet av hemlig dataavläsning. Frågorna har behandlats i avsnitt 9.4.9 och 9.4.10.

Den föreslagna bestämmelsens *första stycke* motsvarar vad som i dag gäller vid husrannsakan (28 kap. 6 § första stycket RB) och skall beaktas av såväl rätten som den verkställande myndigheten. Den kan få betydelse t.ex. i fråga om hur intrånget skall ske i någons bostad, vid vilken tidpunkt det tekniska hjälpmedlet skall placeras ut och hur hjälpmedlet skall gömmas. Det skall sägas att i likhet med vad som gäller enligt bestämmelserna om husrannsakan får polisen ta sig in i det skyddade utrymmet med hjälp av våld. Polisen får alltså, om det anses lämpligt eller nödvändigt, bryta sig in i t.ex. en bostad eller ett annat utrymme som tillståndet gäller för att placera ut utrustningen (se dock tredje stycket).

I *andra stycket* anges att hemlig dataavläsning inte får ske av sådana meddelanden mellan den misstänkte och hans försvarare som avses i 27 kap. 22 § RB, alltså det som tidigare benämndes telemeddelanden (se avsnitt 3.3). I praktiken innebär det att den verkställande myndigheten omedelbart skall avbryta avläsningen så snart det kan konstateras att det är fråga om ett sådant meddelande. I detta ligger inget krav på att myndigheten alltid behöver ha direktavläsning, alltså en avläsning i realtid. Upptagningen behöver alltså inte ske samtidigt med direktavläsning. Det kan inte undvikas att meddelanden kommer att avläsas till korta delar trots att det inte

får ske. Bestämmelsen innebär dock en skyldighet för myndigheten att se till att de meddelanden som har tagits upp inte avläses eller granskas vidare utan i stället förstörs och inte längre blir tillgängliga för utredningen.

För att hemlig dataavläsning skall kunna användas effektivt måste, som framgår av avsnitt 9.4.9, de tekniska hjälpmedel som behövs för verkställigheten ibland installeras i det aktuella informationssystemet genom ett fysiskt ingrepp. Av paragrafens *tredje stycke* framgår att hemlig dataavläsning får förenas med en rätt att i hemlighet göra intrång på platser som annars särskilt skyddas mot intrång, t.ex. bostäder och arbetsplatser. Syftet skall vara att installera tekniska hjälpmedel, alltså den hård- eller mjukvara som behövs för att tvångsmedlet skall kunna verkställas. Någon möjlighet till sådant tillträde ges inte av bestämmelserna om husrannsakan eller beslag. Det är självklart att intrång bör ske bara i den mån det är absolut nödvändigt. Vad som avses med plats som särskilt skyddas mot intrång följer av det som skyddas genom bestämmelserna i 4 kap. 6 § BrB (hemfridsbrott och olaga intrång). Enligt 13 § nedan finns en skyldighet att återta eller göra ett installerat tekniskt hjälpmedel obrukbart. I tillståndet att installera ett hjälpmedel får därför anses ingå en rätt att även återta hjälpmedlet. Någon särskild bestämmelse om detta behövs inte. Med stöd av den föreslagna bestämmelsen skall de brottsutredande myndigheterna också ha rätt att ta sig in i utrymmet för att utföra underhåll och reparera ett tekniskt hjälpmedel som har gått sönder. Det skall då inte krävas något ytterligare beslut av rätten (jfr JO 1997/98 s. 165 ff. beträffande husrannsakan). Behovet av intrång för att genomföra hemlig dataavläsning är en omständighet som domstolen givetvis måste ta hänsyn till när rätten enligt proportionalitetsprincipen skall avgöra om tvångsmedlet skall tillåtas i det enskilda fallet. Principen behandlas i avsnitt 9.4.5 (se också 4 §).

8 § Om det vid hemlig dataavläsning har kommit fram uppgifter om ett annat brott än det som har legat till grund för beslutet om avläsning, får uppgifterna användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller

2. det finns särskilda skäl.

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

Paragrafen reglerar de brottsbekämpande myndigheternas användning av s.k. överskottsinformation för brottsutredande och brottsförebyggande ändamål. Regeringen har nyligen lagt fram ett motsvarande förslag avseende hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning (prop. 2004/05:143, se särskilt s. 50 f.).

Enligt *första stycket* får uppgifter som framkommit vid hemlig dataavläsning och som rör ett annat brott än det som legat till grund för beslutet om avläsning användas för att utreda brottet. Pågår det, när uppgifterna kommer fram vid avläsningen, redan en förundersökning beträffande det andra brottet, får således uppgifterna användas i den undersökningen, t.ex. som grund för husrannsakan eller annan brottsutredningsåtgärd.

Om det inte pågår förundersökning om det andra brottet, får som huvudregel sådan undersökning inledas på grund av uppgifter som framkommit vid hemlig dataavläsning. Det gäller dock inte beträffande mindre allvarliga brott; förundersökning eller motsvarande utredning får normalt inledas på grund av uppgifter som framkommit vid avläsningen endast om det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter. Förundersökning eller motsvarande utredning får normalt inte inledas beträffande exempelvis misshandel som är ringa, snatteri, och narkotikabrott som är ringa, när brottsmisstanken grundar sig enbart på sådana uppgifter. Med motsvarande utredning avses sådana förenklade utredningar som genomförs med stöd av 23 kap. 22 § RB. Det kan dock finnas fall där brottsmisstanken grundar sig också på andra uppgifter än de som framkommit vid avläsningen. Om dessa uppgifter är sådana att de endast tillsammans med den framkomna överskottsinformationen ger tillräckligt underlag för ett beslut om inledande av förundersökning, får förundersökning inte inledas. Men om uppgifterna är av sådant slag att de i sig är tillräckliga för att en förundersökning skall få inledas, får förundersökning inledas med stöd av dessa uppgifter. När förundersökning får inledas, får de uppgifter som erhållits genom tvångsmedelsanvändningen användas i förundersökningen.

En förundersökning får alltid bedrivas vidare, även om det under förundersökningens gång framkommer att gärningen är mindre allvarlig än vad som först misstänktes.

Förundersökning får alltid inledas på grund av överskottsinformation som kommit fram vid hemlig dataavläsning, om det finns

särskilda skäl för det. Sådana särskilda skäl får anses föreligga i de fall när ett väsentligt allmänt intresse talar för att brottet bör utredas och åtal komma till stånd. Som exempel på det kan nämnas fall av övergrepp i rättssak, falsk angivelse och förgripelse mot tjänsteman. I vissa fall kan polisen få information om ett brott vars svårhetsgrad kan variera avsevärt på grund av omständigheterna i det enskilda fallet men som i det konkreta fallet bedöms som ringa brott. Som exempel kan nämnas att polisen får uppgift om att någon innehar ett fåtal barnpornografiska bilder, varför brottet skulle rubriceras som ringa. I ett sådant fall kan det undantagsvis finnas särskilda skäl att inleda en förundersökning, när polisen utifrån sin erfarenhet på goda grunder misstänker att det har begåtts ett betydligt allvarligare brott är det som de initiala uppgifterna ger misstanke om.

En s.k. förutredning syftar till att berika beslutsunderslaget i fråga om en förundersökning skall inledas. Förbudet mot att inleda förundersökning eller motsvarande utredning får givetvis inte kringgås genom att överskottsinformation läggs till grund för en förutredning i syfte att får fram nya uppgifter som kan läggas till grund för ett beslut om inledande av förundersökning.

Enligt *andra stycket* får uppgifter som framkommit vid hemlig dataavläsning om ett förestående brott användas för att förhindra brott. Med uppgifter om förestående brott avses uppgifter om planerade brott. Det kan också vara fråga om uppgifter om ännu ej genomförda straffbara eftergärningar till den som avses med tvångsmedelsbeslutet, t.ex. uppgifter om ett förestående häleri som framkommer i en förundersökning om grovt rån.

Om det förestående brottet inte kan förhindras utan genomförs, får uppgifterna, med de begränsningar som följer av första stycket, användas för att utreda brottet.

9 § En upptagning som har gjorts vid hemlig dataavläsning skall granskas snarast möjligt. I fråga om sådan granskning tillämpas 27 kap. 12 § första stycket rättegångsbalken.

De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt skall bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott skall de bevaras så länge det behövs för att förhindra brott. De skall därefter förstöras.

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

Paragrafen reglerar vad som skall gälla i fråga om upptagningar som har gjorts vid hemlig dataavläsning och överensstämmer i huvudsak med vad som gäller enligt 27 kap. 24 § andra och tredje styckena RB och 7 § andra och tredje styckena lagen om hemlig kameraövervakning (enligt förslaget i prop. 2004/05:143, se särskilt s. 52). Frågan har behandlats i avsnitt 9.4.12.

I *första stycket* anges att en upptagning skall granskas snarast möjligt och att 27 kap. 12 § första stycket RB skall tillämpas vid granskningen. Det främsta syftet med granskningen är att pröva i vilken utsträckning upptagningen är av betydelse från utredningssynpunkt. Hänvisningen till bestämmelsen i rättegångsbalken innebär att endast vissa befattningshavare i normala fall är behöriga att närmare ta del av upptagningen.

Inte bara de delar av upptagningarna som är av betydelse för utredningen av det brott som legat till grund för beslutet om avläsning skall bevaras, utan även, i förekommande fall, de delar som är av betydelse för att utreda andra brott. Av *andra stycket* följer att upptagningarna skall bevaras till dess förundersökningen avseende ett sådant brott har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. Om det kommer fram uppgifter om ett annat brott som redan är föremål för en förundersökning, skall således uppgifterna bevaras på samma sätt som gäller för uppgifter i den förundersökning som föranledde tvångsmedelsanvändningen. Om brottet inte är föremål för en förundersökning förutsätts för bevarande av uppgifterna att en sådan undersökning faktiskt inleds. När upptagningarna inte längre skall bevaras, skall de förstöras.

Enligt andra meningen får även uppgifter i upptagningar som är av betydelse för att förhindra förestående brott bevaras så länge det behövs för att förhindra brott. Om brottet inte kan förhindras utan genomförs, skall uppgifterna i stället bevaras i enlighet med de förutsättningar som ställs upp i första meningen.

Tredje stycket innehåller ett undantag från vad som föreskrivs om förstörande av upptagningar i andra stycket. Enligt undantagsregeln får de brottsutredande myndigheterna behandla uppgifter från upptagningar i enlighet med vad som är särskilt föreskrivet i lag. Det kan vara exempelvis polisdatalagen (1998:622) och lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

Prövning av frågor om hemlig dataavläsning

10 § Frågor om tillstånd till hemlig dataavläsning prövas av tingsrätten på ansökan av åklagaren. Därvid gäller i fråga om behörig domstol 19 kap. 12 § rättegångsbalken. Vid prövningen gäller vad som föreskrivs om offentligt ombud i 27 kap. 26-30 §§ samma balk.

Av paragrafen, som reglerar prövningen av frågor om hemlig dataavläsning, framgår att det är tingsrätten som först skall pröva frågor om tillstånd till tvångsmedlet efter att åklagaren har ansökt om tillstånd till åtgärden. Bestämmelsen överensstämmer med vad som gäller för hemlig teleavlyssning och hemlig teleövervakning enligt 27 kap. 21 § första stycket RB samt för hemlig kameraövervakning enligt 4 § första stycket lagen om hemlig kameraövervakning. De allmänna bestämmelserna om laga domstol i brottmål skall tillämpas (19 kap. 12 § RB). Det innebär enligt huvudregeln att frågan om hemlig dataavläsning skall prövas av den domstol där förundersökningen bedrivs. Av 1 kap. 3 § RB följer att tingsrätten skall bestå av en lagfaren domare. Hänvisningen till 27 kap. 26-30 §§ RB innebär bl.a. att åklagarens begäran skall prövas vid sammanträde inför rätten och att ett offentligt ombud skall närvara vid det tillfället för att bevaka enskildas integritetsintressen. Frågorna har behandlats i avsnitt 9.4.3. Av 12 och 14 §§ nedan framgår att domstolens beslut får verkställas omedelbart och kan överklagas. För tydlighetens skull skall nämnas att ett tillstånd till hemlig dataavläsning givetvis utesluter att den som verkställer tvångsmedlet i enlighet med beslutet gör sig skyldig till exempelvis dataintrång enligt 4 kap. 9 c § BrB.

Vad ett beslut om tillstånd skall innehålla

11 § Ett beslut att tillåta hemlig dataavläsning skall innehålla uppgifter om det informationssystem tillståndet gäller och, när någon är misstänkt för brottet, vem som är misstänkt.

Om tillståndet är förenat med en rätt att installera tekniska hjälpmedel enligt 7 §, skall det särskilt anges i beslutet.

I beslutet skall det också anges under vilken tid tillståndet gäller. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Rätten får också i övrigt föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när.

Paragrafen reglerar innehållet i beslut om hemlig dataavläsning.

Enligt *första stycket* skall ett beslut om tillstånd till hemlig dataavläsning innehålla uppgift om vilket eller vilka informationssystem tillståndet gäller samt, när någon är misstänkt för brottet, vem som är misstänkt. Det förstnämnda kan bl.a. anges som ”de persondatorer NN utnyttjar hemma” eller som en viss statisk IP-adress. Som har framgått tidigare finns det givetvis inget hinder mot att beslutet ger tillstånd till hemlig dataavläsning i flera informationssystem samtidigt. Om det efter beslutet uppstår behov av att verkställa tvångsmedlet i ett annat informationssystem än som omfattas av beslutet får en ny begäran ges in till domstolen. Som framgår av 4 § första stycket är det som huvudregel en förutsättning för att kunna använda hemlig dataavläsning att det finns någon som är skäligen misstänkt för brottet. Enligt den nu aktuella paragrafen skall den misstänkte då också anges i beslutet. Detta gäller naturligt nog inte de fall där hemlig dataavläsning får ske även om det saknas en skäligen misstänkt person (se 4 § andra stycket).

Enligt *andra stycket* skall det anges i beslutet om de brottsutredande myndigheterna får tillträde till en plats som annars skyddas mot intrång för att installera tekniska hjälpmedel. Något krav på att det även i andra fall skall behöva anges en plats för verkställigheten är inte lämpligt att föreskriva. Tvångsmedlet kan t.ex. avse en bärbar dator.

Av *tredje stycket* framgår att tillstånd till hemlig dataavläsning får gälla som längst en månad från dagen för beslutet. Frågan har behandlats i avsnitt 9.4.8. Tillståndstiden överensstämmer därmed med vad som gäller för hemlig teleavlyssning och hemlig teleövervakning enligt 27 kap. 21 § andra stycket RB och 4 § andra stycket lagen om hemlig kameraövervakning. När rätten bestämmer tiden får hänsyn tas till den tid som kan behövas för att få det tekniska hjälpmedlet installerat och alltså användbart. Rätten får dock inte bestämma tiden för tillståndet längre än nödvändigt. Det finns inget som hindrar att rätten beviljar förlängning om det är nödvändigt och skälen för tillstånd i övrigt är uppfyllda. I tredje stycket föreskrivs dessutom att det står domstolens fritt att i övrigt föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan träds för när (jfr förslaget till 27 kap. 21 § andra stycket RB).

Verkställighet och upphävande av beslut

12 § Rättens beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, skall åklagaren eller rätten omedelbart häva beslutet.

Paragrafen reglerar verkställighet och upphävande av beslut.

Av paragrafens *första stycke* framgår att rättens beslut om hemlig dataavläsning får verkställas omedelbart. Om det offentliga ombudet överklagar ett tillståndsbeslut gäller således rättens beslut till dess att högre rätt förordnar annat. Enligt 52 kap. 7 § tredje stycket RB får hovrätten förordna om inhibition (jfr t.ex. vad som gäller enligt 6 § första stycket lagen om hemlig kameraövervakning och som anges i prop. 2002/03:74 s. 54).

Andra stycket reglerar de fall då det inte längre finns skäl för hemlig dataavläsning och överensstämmer med vad som gäller för hemlig teleavlyssning och hemlig teleövervakning enligt 27 kap. 23 § RB samt för hemlig kameraövervakning enligt 5 § lagen om hemlig kameraövervakning. Av bestämmelsen följer att beslutet då skall hävas i förtid. Om det under den tid som tillståndet gäller kommer fram att förutsättningar för tillståndet har fallit bort, skall åklagaren eller domstolen agera. Det finns alltså ett kontinuerligt ansvar för tvångsmedelsanvändningen. Polisen är skyldig att omedelbart underrätta åklagaren om omständigheter som har betydelse för att beslutet skall hävas (jfr prop. 1995/96:85 s. 40). Om åklagaren eller rätten häver beslutet, bör rätten respektive åklagaren givetvis underrättas om det.

Förfarandet med tekniska hjälpmedel

13 § Ett tekniskt hjälpmedel som har installerats skall återtas eller göras obrukbart så snart det kan ske efter det att tiden för tillståndet gått ut eller tillståndet hävts. När hjälpmedlet har återtagits eller gjorts obrukbart, skall rätten underrättas om det.

I paragrafen, som reglerar förfarandet med tekniska hjälpmedel, föreskrivs att ett tekniskt hjälpmedel som har installerats skall återtas eller göras obrukbart så snart det kan ske efter det att tiden för tillståndet har gått ut eller tillståndet har hävts. Frågan har behandlats i avsnitt 9.4.9. Det är av utredningsmässiga och praktiska skäl inte möjligt att ange en bestämd tid inom vilken detta skall ha skett

annat än att det skall genomföras så snart som möjligt. I sista meningen anges att rätten skall underrättas om att hjälpmedlet har återtagits eller gjorts obrukbart. På så sätt uppstår en kontrollmöjlighet i efterhand, bl.a. genom det offentliga ombudet, av att verkställigheten inte fortsätter sedan tillståndet upphört. Underrättelsen bör lämpligen lämnas av åklagaren. Skulle åtgärden bli omöjlig att genomföra för de brottsutredande myndigheterna, bör domstolen underrättas även om det.

Överklagande

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

Den föreslagna bestämmelsen, som reglerar överklagande av rättens beslut, överensstämmer med lydelsen i 6 § andra stycket lagen om hemlig kameraövervakning. Beslut om hemlig dataavläsning får överklagas på samma sätt som gäller för övriga tvångsmedel enligt 25-28 kap. RB. Det innebär att rättens beslut om tillstånd överklagas särskilt (49 kap. 5 § 6 RB). Om rätten under förundersökningen avslår en begäran om tillstånd anses beslutet vara slutligt och kan då överklagas enligt 49 kap. 3 § första stycket RB. Ett beslut om tillstånd till hemlig dataavläsning kan, som framgått, i likhet med vad som gäller vid t.ex. hemlig teleavlyssning enligt 27 kap. 18 § RB, förenas med föreskrifter av inskränkande slag, t.ex. rörande informationen och informationssystemet. Även sådana inskränkande föreskrifter kan överklagas. På samma sätt kan det offentliga ombudet överklaga ett tillståndsbeslut på den grunden att det inte är förenat med erforderliga föreskrifter i syfte att förhindra onödigt intrång i enskildas integritet. I praktiken är det endast åklagaren och det offentliga ombudet som kan överklaga rättens beslut i frågor om hemlig dataavläsning. Har den misstänkte fått kännedom om beslutet och överklagar detta, kan det, på samma sätt som vid andra hemliga tvångsmedel, ifrågasättas om förutsättningar för hemlig dataavläsning fortfarande är uppfyllda.

11.4 Förslaget till lag om ändring i lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål

5 §

Tillstånd till avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken får meddelas, även om brottet inte omfattas av de angivna bestämmelserna. Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § i den lagen. Tillstånd till hemlig dataavläsning får meddelas enligt lagen (0000:00) om hemlig dataavläsning, även om brottet inte omfattas av 3 § i den lagen.

Kan det befaras att inhämtande av rättens tillstånd till avlyssning, övervakning, hemlig kameraövervakning eller hemlig dataavläsning skulle medföra sådan fördröjning eller annan olägenhet, som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.

Vid de brott som omfattas av 1952 års tvångsmedelslag kan tillstånd i dag ges till hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning även om brottet inte är av så allvarligt slag att tvångsmedlen normalt får användas. Dessutom kan åklagaren fatta interimistiska beslut om tillstånd. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har den aktuella paragrafen ändrats så att de begreppen har ersatts av avlyssning respektive övervakning. Dessutom har bestämmelsen kompletterats med det föreslagna tvångsmedlet hemlig dataavläsning. Den frågan har behandlats i avsnitt 9.4.13.

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

5 kap. 1 §

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,

2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,

4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

5. Finansinspektionens verksamhet som rör övervakning enligt insiderstrafflagen (2000:1086), eller

6. prövning av frågor enligt 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott gäller sekretess, 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 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 underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndighet i konkurs och inom exekutionsväsendet för uppgift som angår misstanke om brott.

Utan hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av

1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,

2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid rikspolisstyrelsens säkerhetsavdelning, eller

3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

Sekretess med hänsyn främst till intresset att förebygga och beivra brott regleras i 5 kap. sekretesslagen. I 5 kap. 1 § den lagen finns regler till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Uppgifter som hänför sig till den verksamheten kan också skyddas genom bestämmelserna i 2 kap. sekretesslagen om sekretess med hänsyn till bl.a. rikets säkerhet.

I den nu aktuella paragrafens *första stycke* har den sjätte punkten lagts till. Frågan behandlas i avsnitt 6.6.7. Sekretess gäller därmed för uppgift som hänför sig till prövning av frågor enligt 6 kap. 19 § LEK, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. I den nämnda bestämmelsen tas frågor om anpassningsskyldigheten för operatörer upp. Enligt förslaget till ändring av 36 § förordningen om elektronisk kommunikation skall Rikspolisstyrelsen ha möjlighet att meddela undantag från skyldigheten och de föreläggande som behövs för att skyldigheten skall efterlevas. I sådana ärenden hos Rikspolisstyrelsen kan det förekomma uppgifter som avslöjar t.ex. begränsningar i möjligheterna att verkställa beslut enligt 27 kap. RB om avlyssning och övervakning. Om sådana uppgifter blir offentliga kan det få allvarliga konsekvenser för de brottsbekämpande myndigheternas arbete, eftersom det kan resultera i att kriminella personer väljer operatörer och kommunikationsformer där tvångsmedlen inte kan verkställas. Bestämmelsen i 5 kap. 1 § sekretesslagen kommer att gälla även hos förvaltningsdomstolarna efter exempelvis ett överklagande av Rikspolisstyrelsens beslut. Enligt 12 kap. 4 § sekretesslagen kan domstolen förordna att sekretessen skall bestå även om uppgifterna har tagits in i domstolens beslut.

9 kap. 8 §

Sekretess gäller hos tillståndsmyndigheten på postområdet och hos myndighet som bedriver postverksamhet för uppgift som angår särskild postförsändelse. Om sekretess inte följer av annan bestämmelse, får dock sådan uppgift lämnas till den som är försändelsens avsändare eller mottagare.

Sekretess gäller hos myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande. Om sekretess inte följer av någon annan bestämmelse, får dock sådan uppgift lämnas till den som har

tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller, beträffande något annat än innehållet i meddelandet, innehavaren av ett abonnemang som använts för ett elektroniskt meddelande.

Sekretess gäller hos myndighet som handhar allmän samfärdsel för uppgift som angår enskilds förbindelse med samfärdselverksamheten och som inte avses i första eller andra stycket, om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Sekretess gäller för uppgift vid särskild sambandstjänst inom totalförsvaret, om uppgiften avser elektroniskt meddelande som utomstående utväxlar på elektroniskt kommunikationsnät.

Sekretess gäller i ärenden som avser TV-avgifter för uppgift om enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon honom närstående lider skada eller men om uppgiften röjs.

I fråga om uppgift i allmän handling gäller sekretessen enligt tredje och femte styckena i högst tjugo år.

I 9 kap. sekretesslagen finns regler om sekretess med hänsyn till skyddet för enskilds förhållanden av såväl personlig som ekonomisk natur. Den aktuella bestämmelsens *andra stycke* stadgar i dag sekretess hos myndighet som driver televerksamhet för uppgift som angår särskilt telefonsamtal eller annat telemeddelande. Om sekretess inte följer av annan bestämmelse, får dock enligt paragrafen sådan uppgift lämnas till den som tagit del i telefonsamtalet eller annars är telemeddelandets avsändare eller mottagare eller som annars innehar apparat som har använts för telemeddelandet.

Vi har i avsnitt 3 kommit fram till att flera av de begrepp som finns i den aktuella bestämmelsen skall mönstras ut ur rättegångsbalken. Det gäller t.ex. begreppen telefonsamtal och telemeddelande. Även begreppet televerksamhet är förlegat sedan telelagen upphävdes. Paragrafens andra och *fjärde stycke* har ändrats för att nå överensstämmelse i det avseendet med reglerna om tystnadsplikt i 6 kap. 20 § LEK.

14 kap. 2 §

Sekretess hindrar inte att uppgift i annat fall än som avses i 1 § lämnas till myndighet, om uppgiften behövs där för

1. förundersökning, rättegång, ärende om disciplinansvar eller skiljande från anställning eller annat jämförbart rättsligt förfarande vid

myndigheten mot någon rörande hans deltagande i verksamheten vid den myndighet där uppgiften förekommer,

2. omprövning av beslut eller åtgärd av den myndighet där uppgiften förekommer, eller

3. tillsyn över eller revision hos den myndighet där uppgiften förekommer.

Sekretess hindrar inte att uppgift lämnas i muntligt eller skriftligt yttrande av sakkunnig till domstol eller myndighet som bedriver förundersökning i brottmål.

Sekretess hindrar inte att uppgift om enskilds adress, telefonnummer och arbetsplats eller uppgift i form av fotografisk bild av enskild lämnas till en myndighet, om uppgiften behövs där för delgivning enligt delgivningslagen (1970:428). Uppgift hos myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst om enskilds telefonnummer får dock, om den enskilde hos myndigheten begärt att abonnemanget skall hållas hemligt och uppgiften omfattas av sekretess enligt 9 kap. 8 § tredje stycket, lämnas ut endast om den myndighet som begär uppgiften finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl.

Sekretess hindrar inte att uppgift som angår misstanke om brott lämnas till åklagarmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet, om fängelse är föreskrivet för brottet och detta kan antas föranleda annan påföljd än böter. Detta gäller dock inte uppgift som omfattas av sekretess enligt 9 kap. 8 § andra stycket.

För uppgift som omfattas av sekretess enligt 7 kap. 1-6 och 34 §§, 8 kap. 8 § första stycket, 9 eller 15 § eller 9 kap. 4 eller 7 §, 8 § första stycket eller 9 § gäller vad som föreskrivs i fjärde stycket endast såvitt angår misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Dock hindrar sekretess enligt 7 kap. 1, 4 eller 34 § inte att uppgift som angår misstanke om brott enligt 3, 4 eller 6 kap. brottsbalken mot någon som inte har fyllt arton år lämnas till åklagarmyndighet eller polismyndighet. Inte heller hindrar sekretess enligt 7 kap. 1 eller 4 § att uppgift som gäller misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i ett år och som avser överföring eller försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168) lämnas till åklagarmyndighet eller polismyndighet.

Sekretess enligt 7 kap. 1 § och 4 § första och tredje styckena hindrar inte att uppgift om enskild, som inte fyllt arton år eller som fortgående missbrukar alkohol, narkotika eller flyktiga lösningsmedel, eller när-

stående till denne lämnas från myndighet inom hälso- och sjukvården och socialtjänsten till annan sådan myndighet, om det behövs för att den enskilde skall få nödvändig vård, behandling eller annat stöd. Detsamma gäller i fråga om lämnande av uppgift om gravid kvinna eller närstående till henne, om det behövs för en nödvändig insats till skydd för det väntade barnet.

I 14 kap. sekretesslagen finns bestämmelser om begränsningar i sekretessen och om förbehåll. I den nu aktuella paragrafen finns sekretessbrytande regler. Paragrafens *fjärde stycke* anger att sekretess inte hindrar att uppgift som angår misstanke om brott lämnas till bl.a. åklagarmyndighet eller polismyndighet om fängelse är föreskrivet för brottet och detta kan antas föranleda annan påföljd än böter. Enligt paragrafens *femte stycke* gäller vissa undantag från detta, på så sätt att för uppgifter som omfattas av vissa angivna sekretessbestämmelser gäller att misstanken skall röra brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Hittills har det gällt bl.a. uppgifter som omfattas av sekretess enligt exempelvis 9 kap. 8 § andra stycket sekretesslagen, alltså uppgifter som angår särskilt telefonsamtal eller annat telemeddelande (jfr 6 kap. 20 och 22 §§ LEK).

Vi har i avsnitt 4.2 kommit fram till att de brottsutredande myndigheternas tillgång till uppgifter som angår vad som i 9 kap. 8 § andra stycket sekretesslagen anges som särskilt telemeddelande uteslutande bör regleras i rättegångsbalken. I den nu aktuella paragrafen har ett tillägg gjorts i *fjärde stycket* som innebär att det inte är tillåtet att lämna uppgifter som omfattas av sekretess enligt 9 kap. 8 § andra stycket sekretesslagen till bl.a. åklagarmyndighet eller polismyndighet. Hänvisningen i *femte stycket* till 9 kap. 8 § andra stycket sekretesslagen har utgått. Dessutom har en språklig justering skett i paragrafens *tredje stycke* vad gäller begreppet televerksamhet för att nå överensstämmelse med uttryckssättet i 9 kap. 8 § andra stycket sekretesslagen och 6 kap. 20 § LEK.

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, avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, hemlig kameraövervakning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare*
5 kap. 7 §	*såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag, avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, hemlig kameraövervakning eller hemlig dataavläsning på grund av beslut av domstol 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 avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken på grund av beslut av domstol, undersökningsledare eller åklagare*

I paragrafen anges i vilka fall tystnadsplikt har företräde framför meddelarfriheten. I avsnitt 3.6 kom vi fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken. Som en följd av detta har de begreppen ersatts i den nu aktuella bestämmelsen av avlyssning och övervakning.

Dessutom har paragrafen kompletterats med beslut om hemlig dataavläsning såvitt avser 5 kap. 1 och 7 §§ sekretesslagen.

11.6 Förslaget till lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

28 §

Kan det befaras att inhämtande av rättens tillstånd till avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, hemlig kameraövervakning enligt lagen (1995:1506) om hemlig kameraövervakning eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får åtgärden beslutas av åklagaren. I fråga om kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken får åtgärden även beslutas av undersökningsledaren. Anmälan som avses i tredje stycket i nämnda paragraf skall göras hos den som har fattat beslutet. Denne skall pröva beslagsfrågan.

Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, skall det genast anmälas hos rätten. Anmälan skall vara skriftlig och innehålla skälen för beslutet. Rätten skall pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, skall det upphävas.

Bestämmelsen i 28 § lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. om åklagares behörighet att fatta interimistiskt beslut om bl.a. hemlig teleavlyssning och hemlig teleövervakning får tillämpas framför allt om riket är i krig. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har den aktuella paragrafens *första stycke* ändrats så att de begreppen har ersatts av avlyssning respektive övervakning. Dessutom har bestämmelsen kompletterats med det föreslagna tvångsmedlet hemlig dataavläsning. Den frågan har behandlats i avsnitt 9.4.13.

11.7 Förslaget till lag om ändring i lagen (1991:572) om särskild utlänningskontroll

20 §

För ett sådant ändamål som avses i 19 § första stycket kan rätten, om det finns synnerliga skäl, meddela Rikspolisstyrelsen eller en polismyndighet tillstånd till avlyssning eller, om det är tillräckligt, övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning..

Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Rikspolisstyrelsen eller en polismyndighet tillstånd att närmare undersöka, öppna eller granska post- eller telegrafförsändelser, brev, andra slutna handlingar eller paket som har ställts till utlänningen eller som avsänts från honom och som påträffas vid husrannsakan, kroppsvisitation eller kroppsbesiktning eller som finns hos ett befordringsföretag.

I det tillstånd som avses i andra stycket kan rätten förordna att en försändelse som avses i tillståndet och som ankommer till ett befordringsföretag, skall hållas kvar till dess den närmare undersökts, öppnats eller granskats. Förordnandet skall innehålla underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den som har begärt åtgärden.

21 §

Det tillstånd som avses i 20 § skall meddelas att gälla för en viss tid som inte överstiger en månad.

Frågan om tillstånd prövas av Stockholms tingsrätt på yrkande av Rikspolisstyrelsen eller en polismyndighet. Rättens beslut om tillstånd gäller omedelbart. I fråga om förfarandet tillämpas i övrigt 27 kap. rättegångsbalken respektive lagen (0000:00) om hemlig dataavläsning på motsvarande sätt.

21 a §

Om det vid avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning har kommit fram uppgifter om ett brott som inte är av betydelse för det ändamål som har föranlett avlyssningen, övervakningen eller avläsningen, får uppgifterna användas

för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får dock inledas på grund av dessa uppgifter endast om

1. det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller

2. det finns särskilda skäl.

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

22 §

En upptagning eller uppteckning som har gjorts vid avlyssning enligt 27 kap. 18 § rättegångsbalken eller hemlig dataavläsning enligt lagen (0000:00) om hemlig dataavläsning skall granskas snarast möjligt. Granskningen får utföras endast av rätten, Rikspolisstyrelsen, en polismyndighet eller en åklagare.

Om upptagningen eller uppteckningen innehåller något som inte är av betydelse för det ändamål som har föranlett avlyssningen eller avläsningen, skall den i denna del omedelbart förstöras efter granskningen. I fråga om brott eller förestående brott som inte är av betydelse för det ändamål som har föranlett avlyssningen eller avläsningen skall dock 27 kap. 24 § andra och tredje styckena rättegångsbalken respektive 9 § andra och tredje styckena lagen (0000:00) om hemlig dataavläsning tillämpas.

En försändelse eller någon annan handling som omfattas av tillstånd enligt 20 § får inte närmare undersökas, öppnas eller granskas av någon annan än rätten, Rikspolisstyrelsen, en polismyndighet eller en åklagare. En sådan handling skall undersökas snarast möjligt. När undersökningen har slutförts, skall en försändelse som finns hos ett befordringsföretag tillställas den till vilken försändelsen är ställd och en annan handling återlämnas till den hos vilken handlingen påträffats, om den inte tas i beslag.

Med stöd av lagen om särskild utlänningskontroll får en utlänning underkastas vissa tvångsmedel, om det är av betydelse för att utröna om utlänningen eller en organisation eller grupp som han tillhör eller verkar för planlägger eller förbereder terroristbrott. För ett sådant ändamål får tillstånd i vissa fall ges till bl.a. hemlig teleavlyssning och hemlig teleövervakning. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har bestämmelserna i 20, 21 a och 22 §§ den aktuella lagen ändrats på det sättet att de begreppen har ersatts av avlyssning respektive över-

vakning. Dessutom har bestämmelserna i 20-22 §§ kompletterats med det föreslagna tvångsmedlet hemlig dataavläsning. Den frågan har behandlats i avsnitt 9.4.13. I prop. 2004/05:143 behandlar regeringen frågan om överskottsinformation vid användning av hemliga tvångsmedel. Utformningen av 21 a och 22 §§ utgår från förslaget i den propositionen.

11.8 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

1 kap. 2 §

Rättslig hjälp enligt denna lag omfattar följande åtgärder:

1. förhör i samband med förundersökning i brottmål,

2. bevisupptagning vid domstol,

3. telefonförhör,

4. förhör genom videokonferens,

5. kvarstad, beslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,

6. avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken,

7. tekniskt bistånd med avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken,

8. tillstånd till gränsöverskridande avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken,

9. hemlig kameraövervakning och hemlig dataavläsning,

10. överförande av frihetsberövade för förhör m.m., och

11. rättsmedicinsk undersökning av en avliden person.

Lagen hindrar inte att hjälp lämnas med annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

Rättslig hjälp och tekniskt bistånd med avlyssning och övervakning

Rättslig hjälp i Sverige med avlyssning och övervakning

4 kap. 25 §

En ansökan om avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden.

Upptagningar och uppteckningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken.

Omedelbar överföring av meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken eller uppgifter om sådant meddelande från Sverige till den ansökande staten

4 kap. 25 a §

Rättens beslut enligt 25 § att tillåta avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken får verkställas genom omedelbar överföring av meddelandena eller uppgifter om dessa till den ansökande staten, om det kan ske under betryggande former. Verkställighet genom omedelbar överföring får endast ske i förhållande till en stat som är medlem i Europeiska unionen eller till Island eller Norge. Åklagaren prövar om förutsättningar för omedelbar överföring finns. Om omedelbar överföring av meddelanden sker, får upptagning eller uppteckning inte göras i Sverige.

Tekniskt bistånd i Sverige med avlyssning och övervakning

4 kap. 25 b §

Tekniskt bistånd med avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken i form av omedelbar överföring av

meddelande som avses i de bestämmelserna eller uppgifter om sådant meddelande får lämnas i Sverige enligt denna paragraf.

Tekniskt bistånd lämnas på ansökan av en annan stat som är medlem i Europeiska unionen eller av Island eller Norge, om

1. avlyssningen eller övervakningen avser någon som befinner sig i en av dessa stater,

2. ansökan innehåller en bekräftelse på att ett beslut om avlyssning eller övervakning i en brottsutredning har meddelats i den ansökande staten, och

3. omedelbar överföring av meddelanden eller uppgifter om meddelanden kan ske under betryggande former till den ansökande staten.

Av ansökan skall det framgå under vilken tid åtgärden önskas. Ansökan skall vidare innehålla sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Om den person som ansökan avser inte befinner sig i den ansökande staten, skall det också framgå av ansökan att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Ansökan skall prövas av åklagare. För beslutet om tekniskt bistånd tillämpas bestämmelserna i 27 kap. 18 § första stycket, 19 § första stycket, 20 § fjärde stycket, 21 § andra och tredje styckena samt 23 § rättegångsbalken.

Om omedelbar överföring av meddelanden sker, får upptagning eller uppteckning inte göras i Sverige.

4 kap. 25 c §

Om en stat har begärt tekniskt bistånd enligt 25 b § men omedelbar överföring inte kan ske, skall åklagaren ge den ansökande staten tillfälle att få ansökan behandlad som en ansökan enligt 25 §. Prövningen av rättslig hjälp med avlyssning eller övervakning avser dock i detta fall någon som befinner sig i en annan stat. Om den person som åtgärden avser inte befinner sig i den ansökande staten, skall det av ansökan framgå att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Rättslig hjälp och tekniskt bistånd i utlandet med avlyssning och övervakning

4 kap. 26 §

Åklagare får ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med avlyssning eller övervakning enligt 27 kap. 18

respektive 19 § rättegångsbalken av någon som befinner sig i en annan stat eller i Sverige.

Om den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får rätten på begäran av svensk åklagare pröva frågan om att tillåta den avlyssning eller övervakning som ansökan enligt första stycket avser.

Av ansökan enligt första stycket skall det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden skall kunna genomföras. Om den andra staten kräver ett tillstånd enligt andra stycket, skall ansökan innehålla en bekräftelse på att ett sådant tillstånd har meddelats. Befinner sig den person som åtgärden avser inte i den stat där rättslig hjälp eller tekniskt bistånd söks, skall det av ansökan framgå att ett sådant tillstånd som avses i 26 c § har lämnats av den stat där personen finns.

Tillstånd till gränsöverskridande avlyssning och övervakning

Tillstånd i Sverige till gränsöverskridande avlyssning och övervakning

4 kap. 26 a §

En stat som är medlem i Europeiska unionen eller Island eller Norge får ansöka om tillstånd till att, utan svenskt biträde, i en brottsutredning genomföra avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken av någon som befinner sig i Sverige. Ansökan handläggs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett beslut om avlyssning eller övervakning har meddelats i den ansökande staten.

Åklagaren skall genast pröva om det finns förutsättningar för avlyssning eller övervakning och, om så är fallet, ansöka om rättens tillstånd till åtgärden.

De förutsättningar som gäller enligt 27 kap. 18-22 §§ rättegångsbalken skall tillämpas vid tillståndsprövningen. Rätten skall även tillämpa motsvarande förfarande som anges i 27 kap. 26 och 28-30 §§ samma balk. Tingsrättens beslut får inte överklagas.

4 kap. 26 b §

Ett beslut enligt 26 a § skall meddelas inom 96 timmar från det att ansökan inkom eller, om det finns särskilda skäl, inom högst tolv dagar från ansökan.

Åklagaren skall genast underrätta den ansökande staten när ett beslut enligt 26 a § har meddelats. Om tillstånd vägras, skall underrättelsen ange att avlyssningen eller övervakningen inte får ske eller omedelbart skall upphöra. I sådant fall skall underrättelsen även ange att det material som tagits upp eller hämtats in inte får användas eller att det endast får användas på de villkor som åklagaren ställer upp.

Tillstånd från en annan stat till gränsöverskridande avlyssning och övervakning

4 kap. 26 c §

Har beslut om avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken i en brottsutredning meddelats i Sverige och befinner sig den person som beslutet avser i en annan stat som är medlem i Europeiska unionen eller i Island eller Norge, får meddelanden enligt de bestämmelserna avlyssnas eller övervakas i den andra staten, utan hjälp från denna stat, om

1. åtgärden får ske enligt en internationell överenskommelse som är bindande mellan Sverige och den andra staten, och

2. den andra staten lämnar tillstånd till åtgärden.

Ansökan om tillstånd görs av åklagare. Av ansökan skall det framgå under vilken tid åtgärden beräknas pågå. Ansökan skall också innehålla en bekräftelse på att ett svenskt beslut om avlyssning eller övervakning har meddelats.

Om beslut om avlyssning eller övervakning har meddelats i Sverige men avlyssningen eller övervakningen inte har påbörjats när det blir känt att den person som åtgärden avser befinner sig i en sådan främmande stat som anges i första stycket, skall tillstånd från den andra staten sökas innan avlyssningen eller övervakningen påbörjas. Har avlyssningen eller övervakningen redan påbörjats i Sverige och vill åklagaren att avlyssningen eller övervakningen skall fortsätta i den andra staten, skall han eller hon omedelbart ansöka om tillstånd hos den andra staten. Avlyssningen eller övervakningen får i ett sådant fall fortsätta där under den tid frågan om tillstånd prövas.

Vad som sägs i tredje stycket andra och tredje meningarna tillämpas på motsvarande sätt, om avlyssningen eller övervakningen genomförts

med stöd av tillstånd i en främmande stat och det kommer fram att den person som åtgärden avser befinner sig i en annan stat än den som har meddelat tillståndet.

Hemlig kameraövervakning och hemlig dataavläsning

Hemlig kameraövervakning och hemlig dataavläsning rörande någon i Sverige

4 kap. 27 §

En ansökan om hemlig kameraövervakning eller hemlig dataavläsning rörande någon som befinner sig i Sverige handläggs av åklagare. Åklagaren skall genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd.

Hemlig kameraövervakning och hemlig dataavläsning rörande någon i utlandet

4 kap. 28 §

Om hemlig kameraövervakning eller hemlig dataavläsning skall äga rum rörande någon som befinner sig i en annan stat och den andra staten kräver att ansökan först skall prövas av domstol i Sverige, får tingsrätten på begäran av svensk åklagare besluta att tillåta kameraövervakningen eller dataavläsningen.

I lagen om internationell rättslig hjälp i brottmål finns bestämmelser som rättslig hjälp i brottmål i Sverige och utomlands. Rättslig hjälp enligt lagen omfattar enligt 1 kap. 2 § bl.a. hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. I 4 kap. 25-28 §§ finns särskilda bestämmelser om de tvångsmedlen. Vi har utgått från den lydelse paragraferna har enligt regeringens prop. 2004/05:144. Som en följd av att vi i avsnitt 3.3 och 3.6 kom fram till att begreppen hemlig teleavlyssning, hemlig teleövervakning och telemeddelande skulle mönstras ut ur rättegångsbalken, har de aktuella paragraferna ändrats så att de begreppen har ersatts av avlyssning, övervakning och meddelande. Dessutom har ett flertal rubriker före de angivna bestämmelserna ändrats i enlighet med detta. Som en följd av förslaget till ändring i rättegångsbalken har en tidigare hänvisning i 4 kap. 25 b § tredje stycket till 27 kap. 20 §

andra stycket RB ändrats till att avse fjärde stycket i samma paragraf.

I propositionen Internationell rättslig hjälp i brottmål (prop. 1999/2000:61 s. 79 f. och 83) anges bl.a. att målsättningen bör vara att svenska domstolar och åklagare skall kunna ge rättslig hjälp till utländska myndigheter med alla de åtgärder som kan vidtas vid en svensk förundersökning eller rättegång. Enligt regeringen föreligger det ingen anledning att utesluta vissa tvångsmedel eller att generellt begränsa de svenska åklagarnas möjlighet att begära rättslig hjälp utomlands.

Även hemlig dataavläsning bör vara en åtgärd som omfattas av rättslig hjälp enligt den aktuella lagen. Ändringar har skett i 1 kap. 2 § och 4 kap. 27-28 §§ i enlighet med detta. Regleringen rörande hemlig dataavläsning överensstämmer med regleringen rörande hemlig kameraövervakning.

11.9 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 omfattas av beslut om avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, tekniskt bistånd med avlyssning eller med övervakning, 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 den aktuella paragrafen görs undantag från de regler om behandling av trafikuppgifter som finns i 6 kap. 5-7 §§ LEK. De sistnämnda bestämmelserna reglerar särskilt operatörernas skyldighet att utplåna och avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande. Undantaget i andra punkten i den nu aktuella bestämmelsen rör elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om bl.a. hemlig teleavlyssning eller hemlig teleövervakning. Som en följd av att vi i avsnitt 3.6 kom fram till att de be-

greppen skulle mönstras ut ur rättegångsbalken, har den nu aktuella paragrafen ändrats så att begreppen har ersatts av avlyssning respektive övervakning. Vi har utgått från den lydelse paragrafen har enligt regeringens prop. 2004/05:144.

6 kap. 19 §

En verksamhet som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. rättegångsbalken eller tjänster inom ett sådant nät skall bedrivas så att beslut om avlyssning och övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken kan verkställas och så att verkställandet inte röjs.

Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand.

Regeringen eller den myndighet som regeringen bestämmer får i enskilda fall medge undantag från skyldigheten enligt första stycket och får meddela de föreläggande som behövs för efterlevnaden av skyldigheterna enligt första och andra styckena. Föreläggandena får förenas med vite.

Paragrafen reglerar anpassningsskyldigheten för operatörer. Frågan behandlas i avsnitt 6.

I *första stycket* anges *för det första* vilka verksamheter som skall omfattas av anpassningsskyldigheten. Verksamheten skall avse ett allmänt tillhandahållande av elektroniskt kommunikationsnät eller tjänster inom ett sådant nät. Vad som avses med sådana nät i detta fall framgår av den föreslagna definitionen i 27 kap. 18 § fjärde stycket RB. Från de verksamheter som omfattas av anpassningskravet utesluts verksamheter där meddelandena över huvud taget inte kan bli föremål för beslut om avlyssning eller övervakning (se 27 kap. 20 § fjärde stycket RB), alltså vid nät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt. Med det valda uttryckssättet att tillhandahållandet skall vara allmänt utesluts även verksamheter som avser tillhandahållande av sådana nät eller tjänster som inte står till förfogande för användning av allmänheten och som samtidigt inte heller effektivt konkurrerar med sådan verksamhet. Företag, bostadsrättsföreningar eller andra sammanslutningar som internt tillhandahåller vissa tjänster kommer generellt sett inte att vara anpassningsskyldiga, även om beslut om tvångsmedel kan omfatta meddelanden som

befordras i deras nät. I den mån dessa erbjuder sina tjänster till en vid krets, t.ex. i en stadsdel eller ett motsvarande större geografiskt område, och därigenom kan sägas effektivt konkurrera med operatörer på marknaden, kommer de dock att omfattas av anpassningsskyldigheten. Liksom tidigare skall operatörerna stå för de kostnader anpassningsåtgärderna kräver.

I *första stycket* anges *för det andra* vad som innefattas i anpassningsskyldigheten. Verksamheten skall bedrivas så att beslut om avlyssning och övervakning enligt 27 kap. 18 respektive 19 § RB kan verkställas och så att verkställandet inte röjs.

I bestämmelsens *andra stycke* regleras liksom i dag en annan del av anpassningsskyldigheten, nämligen att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand. Samma uttryckssätt används i paragrafens gällande lydelse.

Den föreslagna bestämmelsens *tredje stycke* reglerar *för det första* möjligheten att i enskilda fall besluta om undantag från skyldigheten att bedriva verksamheten så att tvångsmedlen kan verkställas och så att verkställandet inte röjs (jfr fjärde stycket i gällande lydelse). Som framgår av förslaget till ändring av 36 § förordningen om elektronisk kommunikation skall undantagen meddelas av Rikspolisstyrelsen. När frågan om undantag skall avgöras får det främst ske en avvägning mellan nyttan eller effektiviteten och kostnaderna för den enskilde operatören. Frågor om nytta eller effektivitet i den brottsbekämpande verksamheten kan knappast mätas i ett visst antal verkställigheter hos en enskild operatör. I stället är en viktig del i sammanhanget det samhällsintresse som ligger i att kunna upprätthålla en beredskap för att snabbt ha möjlighet att verkställa beslut om tvångsmedlen. Beslut om undantag kan tidsbegränsas med hänsyn till faktorer som teknikutveckling och kostnader och villkoras med avseende på exempelvis viss teknik samt verksamhetens omfattning, art och kundkrets.

Andra stycket ger *för det andra* Rikspolisstyrelsen (se förslaget till ändring av 36 § förordningen om elektronisk kommunikation) ett påtryckningsmedel på en operatör för det fall anpassningsskyldigheten inte efterlevs i något avseende. Rikspolisstyrelsen, som därmed i praktiken får en tillsynsuppgift, skall då få meddela de förelägganden som behövs i det avseendet och förena dessa med vite. PTS har redan i dag en liknande möjlighet enligt 7 kap. LEK. Frågor om utdömande av vite prövas enligt 6 § viteslagen av länsrätt på ansökan av Rikspolisstyrelsen.

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, och

2. angelägenhet som avser användning av avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken eller tekniskt bistånd med avlyssning eller med övervakning enligt 4 kap. 25 a § lagen (2000:562) om internationell rättslig hjälp i brottmål.

Bestämmelser om tystnadsplikt för operatörer finns i 6 kap. 20 och 21 §§ LEK. Enligt *andra punkten* i den sistnämnda paragrafen, som utgår från förslaget till lydelse i prop. 2004/05:144, finns tystnadsplikt för angelägenhet som avser användning av bl.a. hemlig teleavlyssning eller hemlig teleövervakning. Som en följd av att vi i avsnitt 3.6 kom fram till att de begreppen skulle mönstras ut ur rättegångsbalken, har bestämmelsen ändrats så att begreppen har ersatts av avlyssning respektive övervakning.

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 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 myndighet som skall ingripa mot brottet och även i andra fall till polismyndighet eller åklagarmyndighet,

3. uppgift som avses i 20 § första stycket 3 samt sådana uppgifter för lokalisering av ett tekniskt hjälpmedel som avses i 27 kap. 19 § rättegångsbalken till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa,

4. uppgift som avses i 20 § första stycket 1 till en kronofogdemyndighet som behöver uppgiften i exekutiv verksamhet, om 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), och

6. 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 6 skall vara skälig med hänsyn till kostnaderna för utlämnandet.

Bestämmelsen reglerar skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst att utan hinder av den tystnadsplikt som finns i 6 kap. 20 § LEK lämna ut uppgifter i vissa fall.

I *första stycket andra, sjätte och sjunde punkterna* föreskrevs tidigare att operatören skulle lämna uppgifter om abonnemang enligt 6 kap. 20 § första stycket 1 LEK till brottsutredande myndigheter i vissa fall under förundersökning samt till polismyndighet i vissa situationer i främst den hjälpande verksamheten och till polismyndighet eller åklagarmyndighet vid viss underrättelseskyldighet enligt lagen med särskilda bestämmelser om unga lagöverträdare. Andra punkten har ändrats så att det numera finns en generell skyldighet för operatören att lämna uppgifter om abonnemang till brottsutredande myndigheter och till polismyndighet eller åklagarmyndighet även i andra fall. Frågan har behandlats i avsnitt 5.4. Som en följd av den ändringen har sjätte och sjunde punkterna upphävts och den tidigare åttonde punkten numrerats som sjätte punkt i stycket.

I *första stycket tredje punkten* föreskrevs tidigare att operatören skulle lämna ut uppgifter som angår särskilda elektroniska meddelanden till åklagarmyndighet, polismyndighet eller annan myndighet som skall ingripa mot brottet. I avsnitt 4.2 kom vi fram till att den regleringen skulle upphävas. Det innebär att ett utlämnande i liknande fall får ske endast efter beslut enligt 27 kap. RB.

I den nämnda punkten föreskrivs numera i stället att uppgifter som angår särskilda elektroniska meddelanden skall lämnas till polismyndighet, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa. I punkten tydliggörs

också att operatören skall lämna lokaliseringsuppgifter bl.a. rörande en mobiltelefon som är påslagen utan att det samtidigt pågår ett samtal (jfr 27 kap. 19 § RB).

Frågan behandlas i avsnitt 5.5. Bestämmelsen är avsedd att tillämpas utanför en förundersökningssituation i syfte att effektivisera efterforskning av försvunna personer. Genom tillgång till de aktuella uppgifterna kan personen påträffas snabbare och stora resurser sparas i polisarbetet. Förslaget i 27 kap. 25 § andra stycket RB om att en operatör skall vara skyldig att genast på begäran medverka vid verkställighet av avlyssning eller övervakning kommer att leda till att uppgifterna enligt den nu aktuella paragrafen kan lämnas ut mycket snabbt.

Som framgår skall en bedömning göras av om försvinnandet har skett under sådana omständigheter att det kan befaras att det föreligger fara för personens liv eller allvarlig risk för dennes hälsa. Det får då bedömas om det finns omständigheter som tyder på att försvinnandet är frivilligt. Vid exempelvis underårigas försvinnanden eller när personer som kan ha en nedsatt mental förmåga har försvunnit, kan man dock alltid utgå från att sådan fara eller risk föreligger, även om försvinnandet kan framstå som ”frivilligt”.

Som en följd av ändringarna i första stycket har hänvisningen i *andra stycket* ändrats.

6 kap. 23 §

Den som i annat fall än som avses i 20 § första stycket och 21 § i radiomottagare har avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett radiobefordrat meddelande som avses i 27 kap. 18 respektive 19 § rättegångsbalken och som inte är avsett för honom eller henne själv eller för allmänheten får inte obehörigen föra det vidare.

Tystnadsplikt för operatörer finns föreskriven i 6 kap. 20 och 21 §§ LEK. Därutöver stadgas i den nu aktuella bestämmelsen tystnadsplikt för den som i annat fall har avlyssnat eller på annat sätt med användande av radiomottagare har fått tillgång till ett radiobefordrat telemeddelande som inte är avsett för den personen eller för allmänheten. Som en följd av att vi i avsnitt 3.3 kom fram till att begreppet telemeddelande skulle mönstras ut ur rättegångsbalken och ersättas av begreppet meddelande, har bestämmelsen ändrats i enlighet med detta.

6 kap. 23 a §

Den som i verksamhet som anges i 19 § första stycket lämnar ut innehållet i och uppgifter om avlyssnade eller övervakade meddelanden har inte rätt till ersättning.

Den som lämnar ut uppgifter enligt 22 § första stycket 2 och 3 har inte rätt till ersättning.

Regeringen får meddela föreskrifter om undantag från första och andra styckena.

I lagrådsremiss den 3 mars 2005 (Kostnadsansvar för hemlig teleavlyssning m.m.) föreslår regeringen att den aktuella paragrafen, som behandlar kostnadsansvaret vid enskilda verkställigheter av bl.a. beslut om hemlig teleavlyssning och hemlig teleövervakning, skall införas i lagen om elektronisk kommunikation.

Som en följd av att vi i avsnitt 3.3 kom fram till att begreppet telemeddelande skulle mönstras ut ur rättegångsbalken och ersättas av begreppet meddelande, har bestämmelsens *första stycke* ändrats i enlighet med detta.

Någon ändring i övrigt av bestämmelsen har inte skett. *Andra stycket* anger att operatörer som på begäran lämnar ut uppgifter enligt 6 kap. 22 § första stycket 2 och 3 LEK inte har rätt till ersättning för detta. Som följd av vårt förslag till ändring de bestämmelserna kommer detta i fortsättningen att gälla även i vissa andra fall som inte behandlas i den nämnda propositionen, t.ex. uppgifter som efterfrågas när personer har försvunnit.

11.10 Förslaget till förordning om ändring i sekretessförordningen (1980:657)

6 §

Följande myndigheter skall i den utsträckning som framgår nedan inte tillämpa föreskriften i 15 kap. 2 § andra stycket sekretesslagen (1980:100).

Myndigheter	*Register*
allmänna domstolarna	*diarier över ärenden om kvarhållande av försändelser på befordringsföretag och om avlyssning eller övervakning*

	enligt 27 kap. 18 respektive 19 § rättegångsbalken, hemlig kameraövervakning och hemlig dataavläsning
---	---
polismyndigheterna	*diarier över ärenden om kvarhållande av försändelse på befordringsföretag och om avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, hemlig kameraövervakning och hemlig dataavläsning*
---	---
åklagarmyndigheterna	*diarier över ärenden om kvarhållande av försändelse på befordringsföretag och om avlyssning eller övervakning enligt 27 kap. 18 respektive 19 § rättegångsbalken, hemlig kameraövervakning och hemlig dataavläsning samt diarier över förundersökningar som rör brott mot rikets säkerhet*

När en allmän handling har kommit in till eller upprättats hos en myndighet skall handlingen som huvudregel registreras utan dröjsmål. I 15 kap. 2 § sekretesslagen anges att det av registret skall framgå bl.a. datum, diarienummer, från vem handlingen har kommit in eller till vem den har expedierats och vad handlingen rör. Regeringen får enligt samma bestämmelse föreskriva att detta inte skall tillämpas för vissa register. Sådana föreskrifter har regeringen meddelat i 6 § sekretessförordningen. Av bestämmelsen framgår att undantag gäller för diarier över ärenden hos allmänna domstolar, polismyndigheter och åklagarmyndigheter om bl.a. hemlig teleavlyssning och hemlig teleövervakning. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppen hemlig teleavlyssning och hemlig teleövervakning skulle mönstras ut ur rättegångsbalken, har den nu aktuella paragrafen ändrats så att de begreppen har ersatts av avlyssning respektive övervakning. Ändring har också skett på så sätt att begreppet befordringsföretag har ersatt begreppet befordringsanstalt för att nå överensstämmelse med lydelsen av bestämmelsen i 27 kap. 9 § RB. Dessutom har paragrafen kompletterats med ärenden om hemlig dataavläsning.

Bilaga

Verksamheten består i	*Särskilda begränsningar i sekretessen*

134. Rikspolisstyrelsens prövning av frågor enligt 36 § förordningen (2003:396) om elektronisk kommunikation

Sekretess med hänsyn främst till skyddet för enskilds ekonomiska förhållanden regleras i 8 kap. sekretesslagen. I 8 kap. 6 § den lagen finns huvudregeln om sekretess i statlig tillsynsverksamhet m.m. Sekretess gäller, i den utsträckning regeringen föreskriver det, i statlig myndighets verksamhet som består i bl.a. tillståndsgivning och tillsyn för uppgift om enskilds affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs. Paragrafen ger med andra ord inte själv upphov till någon sekretess utan den förutsätter att regeringen föreskriver om det. Med stöd av paragrafen har regeringen meddelat föreskrifter om sekretess i 2 § sekretessförordningen. Där anges att sekretess gäller i den utsträckning som anges i bilagan till förordningen. I den bilagan har punkten 134 lagts till. Där anges Rikspolisstyrelsens prövning av frågor enligt 36 § förordningen om elektronisk kommunikation som den verksamhet i vilken sekretess gäller. I 6 kap. 19 § LEK tas frågor om anpassningsskyldigheten för operatörer upp och 36 § förordningen om elektronisk kommunikation ger i vissa fall Rikspolisstyrelsen möjlighet att meddela undantag från skyldigheten och de föreläggande som behövs för att skyldigheten skall efterlevas. I sådana ärenden hos Rikspolisstyrelsen kan det förekomma uppgifter som avslöjar t.ex. operatörernas tekniska system och liknande. Sådana uppgifter kan vara mycket avslöjande för den operatören i förhållande till framför allt konkurrenter på marknaden och skall därför kunna omfattas av sekretess hos Rikspolisstyrelsen.

11.11 Förslaget till förordning om ändring i polisförordningen (1998:1558)

3 kap. 8 §

Länspolismästare, biträdande länspolismästare, polismästare, polisöverintendenter, polisintendenter eller polissekreterare får fatta beslut

---

20. om att göra en anmälan som rör utvisning enligt 2 § lagen (1991:572) om särskild utlänningskontroll, om förvar enligt 8 § första stycket samma lag, om husrannsakan, kroppsvisitation m.m. enligt 19 § samma lag eller om att framställa yrkande om tillstånd till avlyssning m.m. enligt 21 § andra stycket samma lag,

---

Polismyndigheten får uppdra åt en annan anställd än som anges i första stycket att fatta beslut i ärenden som anges där, om den anställde har den kompetens, utbildning och erfarenhet som behövs.

I 3 kap. 8 § polisförordningen finns vissa frågor angivna som det i första hand ankommer på polischefer att fatta beslut om. Dit hör exempelvis att framställa yrkande om tillstånd till bl.a. hemlig teleavlyssning enligt lagen om särskilt utlänningskontroll. Som en följd av att vi i avsnitt 3.6 kom fram till att begreppet hemlig teleavlyssning skulle mönstras ut ur rättegångsbalken, har den nu aktuella paragrafens *första stycke* ändrats så att det begreppet har ersatts av avlyssning.

11.12 Förslaget till förordning om ändring i förordningen (2000:704) om internationell rättslig hjälp i brottmål

7 §

Följande kostnader skall återkrävas av den ansökande staten:

---

4. avlyssning enligt 27 kap. 18 § rättegångsbalken: myndighets utlägg för operatörs kostnader för verkställandet av avlyssning.

Den aktuella förordningen innehåller bestämmelser om tillämpningen av lagen om internationell rättslig hjälp i brottmål. I 7 § re-

gleras vilka kostnader som skall återkrävas av den ansökande staten, bl.a. myndighets utlägg för teleoperatörs kostnader för verkställandet av hemlig teleavlyssning. Som en följd av att vi i avsnitt 3.6 kom fram till att bl.a. begreppet hemlig teleavlyssning skulle mönstras ut ur rättegångsbalken, har den nu aktuella paragrafen ändrats så att det begreppet har ersatts av avlyssning. Dessutom har teleoperatör ändrats till operatör.

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

36 §

Rikspolisstyrelsen får medge undantag och meddela förelägganden enligt 6 kap. 19 § tredje stycket lagen (2003:389) om elektronisk kommunikation.

I 22 a § förvaltningslagen (1986:223) finns bestämmelser om överklagande hos allmän förvaltningsdomstol.

I 6 kap. 19 § LEK finns bestämmelser om anpassningsskyldighet. Där föreskrivs att regeringen eller den myndighet som regeringen bestämmer i enskilda fall får meddela undantag från den skyldigheten och även meddela de förelägganden som behövs för efterlevnaden av skyldigheten. Förelägganden får förenas med vite. I avsnitt 6.6.4 och 6.6.6 behandlas frågan om vilken myndighet som skall få meddela sådana undantag och förelägganden. Slutsatsen blev att det är Rikspolisstyrelsen som skall ha den rollen. Detta föreskrivs i *första stycket* i den nu aktuella bestämmelsen i förordningen om elektronisk kommunikation.

I *andra stycket* erinras om att det i 22 a § förvaltningslagen finns en bestämmelse som medför att Rikspolisstyrelsens beslut i fråga om undantag och förelägganden överklagas hos allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten (jfr prop. 1997/98:101 s. 62 f.). Frågor om utdömande av vite regleras i 6 § viteslagen.

Särskilt yttrande

Särskilt yttrande av *Lars Trägård*

Anpassnings- och medverkandeskyldigheterna

I betänkandet (avsnitt 6 och 8) föreslås bl.a. att två typer av skyldigheter skall åvila operatörerna av allmänna elektroniska kommunikationsnät eller dem som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst (fortsättningsvis kallade operatörerna). Den ena är en i princip obegränsad skyldighet att anpassa sin verksamhet så, att beslut om avlyssning och övervakning kan verkställas omgående (anpassningsskyldigheten). Den andra är en skyldighet att, likaså i obegränsad omfattning, medverka till att ett sådant beslut kan verkställas i det enskilda fallet, i regel inom en timme från begäran därom (medverkandeskyldigheten). Medverkandeskyldigheten föreslås gälla även andra enskilda än operatörer. Den avses inte vara sanktionerad och efterlevnaden föreslås inte heller bli föremål för statlig tillsyn. I betänkandet förutsätts att bestämmelserna likväl kommer att efterlevas. Det framhålls också att sanktionsmöjligheter annars måste övervägas. Anpassningsskyldigheten skall enligt förslaget kunna begränsas genom undantag för en viss operatör efter beslut av Rikspolisstyrelsen (RPS), som också föreslås få uppgiften att utöva tillsyn över operatörerna med avseende på denna skyldighet. Skyldigheten föreslås bli sanktionerad genom vitesbestämmelser.

Jag instämmer, utifrån det faktamaterial som presenterats för oss, i allt väsentligt i de överväganden som betänkandet ger uttryck för i dessa avseenden. Jag har emellertid följande att anföra beträf-

fande betänkandets förslag om att operatörerna skall ha hela kostnadsansvaret för åtgärderna.

Kostnadsansvaret

Tidigare ställningstaganden

Anpassnings- och medverkandeskyldigheterna skall alltså enligt förslaget vara i princip obegränsade och åtgärderna inte grunda ersättningsrätt för operatörerna. I beredningens tidigare avgivna betänkande (SOU 2003:74) Ökad effektivitet och rättssäkerhet i brottsbekämpningen föreslogs att innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden som omfattades av beslut om hemlig teleavlyssning eller hemlig teleövervakning skulle göras tillgängliga utan kostnad för de brottsutredande myndigheterna. Även utlämnande från operatörer av uppgifter enligt lagen om elektronisk kommunikation skulle enligt förslaget ske kostnadsfritt. Vid remissbehandlingen anförde ett antal remissinstanser, däribland PTS i ett yttrande vari jag deltog, kritik mot förslaget och förordade bl.a. en ersättning som skulle begränsas till att täcka operatörernas kostnader. Remisskritiken avsåg såvitt nu är av intresse i huvudsak följande punkter.

1. Tveksamhet kunde råda om förslagets överensstämmelse med 2 kap. 18 § regeringsformen eller bestämmelser om mänskliga rättigheter i Europakonventionen.
2. Den brottsutredande verksamheten ansågs vara en statlig angelägenhet som borde finansieras med skattemedel och inte av enskilda.
3. Kostnadsfria tjänster kunde leda till överkonsumtion och därmed onödiga utgifter totalt.
4. Reglerna skulle snedvrida konkurrensen och innebära etableringshinder.

Regeringen beslöt emellertid den 3 mars 2005 att inhämta Lagrådets yttrande över ett förslag i som i dessa delar i huvudsak överensstämde med förslaget i betänkandet SOU 2003:74. Lagrådet anförde i sitt svar att förslaget innebar en helt motsatt syn på ersättningsansvaret än som redovisades i propositionen 2003/04:74, där regeringens ståndpunkt, som godtogs av riksdagen, var att de ökade

kostnader som förutsågs för polisväsendets del i samband med ökad användning av hemlig teleavlyssning och hemlig teleövervakning skulle belasta statsbudgeten. Lagrådet anförde bl.a. att remissinstansernas synpunkter inte hade närmare bemötts i lagrådsremissen och att det över huvud taget saknades en närmare redogörelse och diskussion beträffande de motstående intressen som gjorde sig gällande. Lagrådet föreslog mot bakgrund av sitt yttrande att förslaget borde bli föremål för ytterligare överväganden.

Utredningen om kostnaderna

Enligt min uppfattning är inte heller beträffande det nya förslaget kostnader och konsekvenser i övrigt för operatörerna tillräckligt utredda för att man utan vidare skall kunna ålägga dessa hela kostnadsbördan under de antaganden som görs i betänkandet, nämligen att kostnaderna är försumbara beträffande anpassningsskyldigheten eller att det inte blir fråga om några stora tillkommande kostnader beträffande medverkandeskyldigheten.

Att utredningen på denna punkt är i det närmaste obefintlig betingas visserligen nästan helt av brist på konkreta uppgifter från operatörerna. Jag anser dock inte att lagstiftaren bör ta detta till intäkt för att förbigå frågan. Det är tvärtom angeläget att utreda denna ytterligare. Såvitt jag har inhämtat är frågan om kostnadsansvar alltjämt föremål för beredning av regeringen och konsekvenserna för operatörerna av tidigare förslag utreds på uppdrag av regeringen av PTS. Ett grundligare material för bedömning av konsekvenserna bör tas fram i det fortsatta lagstiftningsarbetet.

Överensstämmelse med regeringsformen och Europakonventionen

Den bedömning av förslagets överensstämmelse med regeringsformen och europakonventionen som gjordes i lagrådsremissen – mot vilken Lagrådet inte uttalade någon erinran – hade till utgångspunkt betydligt mindre omfattande skyldigheter än de nu föreslagna. Vilka anpassningsåtgärder som skulle vidtas avsågs dessutom bli prövat i förväg av en myndighet med avseende på proportionalitet, behov och rimlighet i övrigt.

Det nu avgivna betänkandets förslag innebär i princip obegränsade förpliktelser som huvudregel med möjlighet för en myndighet

att medge undantag från anpassningsskyldigheten. Några preciserade anvisningar i författningsform för prövningen är inte avsedda. Av motiven till förslaget framgår emellertid enligt min mening att denna möjlighet är avsedd att vara relativt begränsad.

Medverkandeskyldigheten är inte begränsad i lagförslaget och kan enligt de föreslagna motiven till förslaget omfatta allt. Som exempel nämns bl.a. att tillhandahålla teknisk utrustning samt att vidta de personella och organisatoriska dispositioner som är nödvändiga för verkställighet inom kort tid av ett tvångsmedelsbeslut. Medverkandeskyldigheten är inte direkt sanktionerad i lag men det förutsätts att sådan kommer att övervägas om operatörerna inte ställer sig till efterrättelse vad denna skyldighet kan medföra.

Det bör i det fortsatta lagstiftningsarbetet övervägas om även det nya förslaget överensstämmer med bestämmelserna i regeringsformen och Europakonventionen om ingen ersättningsregel införs.

Risk för överkonsumtion

Det hävdades också i det ovan nämnda remissförfarandet att en risk för överkonsumtion skulle föreligga. Därmed torde förstås att för utredaren kostnadsfria tjänster som ingår i en utredningsmetod kan föranleda att denna metod väljs framför andra, totalt sett billigare metoder som leder till samma resultat. Mot detta resonemang anförs i betänkandet bl.a. att det hittills inte kunnat noteras något sådant överdrivet bruk.

Som återges i betänkandet, har regeringen under förarbetena med tidigare lagstiftning mot argumentet anfört att risken för överkonsumtion var liten, eftersom anpassningen skulle bestämmas genom en balans mellan telepolitiska och kriminalpolitiska intressen som skulle eliminera sådan överdriven användning. Den föreslagna ordningen innebär emellertid vida större möjligheter att genomdriva anpassningsåtgärder och i praktiken, genom bl. a. den roll RPS föreslås få, bestämmanderätt för de brottsbekämpande myndigheterna i fråga om omfattning och utförande av anpassning i det enskilda fallet. Förslaget har i detta hänseende vissa drag av förfogandelagstiftning. Detsamma torde gälla den föreslagna medverkandeskyldigheten, även om denna – såvitt kan utläsas av förslaget dock närmast på försök – är osanktionerad och operatörerna i detta hänseende inte föreslås stå under statlig tillsyn. Jag anser med hänsyn till att de föreslagna skyldigheternas omfattning och karaktär är så olika dem i den nuvarande ordningen, att tillämpningen av

denna knappast kan tillmätas betydelse vid bedömningen vad avser förslaget.

Domstolsprövningen vid allmän domstol av tvångsåtgärderna i det enskilda fallet i förslaget avser inte anpassningsskyldigheten och tar närmast sikte på integritetsfrågor och de begränsningar dessa bör medföra. Att avgöra om en utredningsmetod som innebär en sökt tvångsåtgärd är ekonomiskt motiverad vid en jämförelse med andra sådana metoder torde inte vara möjligt och heller inte avsedd. Inte heller domstolsprövningen är därför enligt min mening någon garanti mot en omotiverat omfattande användning av tvångsmedlen. Det är inte heller inte troligt att sådana överväganden är åtkomliga för bedömning vid RPS eller förvaltningsdomstols undantagsprövning.

Jag kan sålunda inte se att det finns något som direkt hindrar en mer generell övergång från andra spaningsåtgärder till avlyssning och övervakning. En sådan övergång är också i viss mån avsikten med förslaget och förväntas effektivisera brottsutredningarna. Den omständigheten, att förslaget i praktiken öppnar möjlighet till ett mer extensivt bruk av de föreslagna tvångsmedlen bör inte avfärdas. Från ekonomisk teori är det välkänt att priset generellt påverkar efterfrågan. Den påtalade konsumtionsökningen bör enligt min mening beaktas vid en avvägning av hur kostnadsansvaret skall fördelas.

Finansieringsprinciperna

Den uppfattning som PTS och andra remissinstanser uttryckt under remissen av beredningens betänkande SOU 2003:74, nämligen att verksamheten bör finansieras med statliga medel snarare är privata, vidhåller jag alltjämt. Det gäller i synnerhet som kostnaderna med det nya betänkandets förslag framstår än mer osäkra och inte osannolikt högre än vad som är fallet med nuvarande ordning. Jag delar uppfattningen i betänkandet, att en ny och annan avvägning av berörda samhällsintressen bör göras. Intresset av funktionella och billiga elektroniska kommunikationer och av en växande marknad på området bör dock inte helt förbises vid denna avvägning. Ställningstagandet behöver inte innebära att samhället ålägger operatörerna – och samtidigt konsumenterna av sådana kommunikationer – bördor, vars omfattning är okända och därmed ställer upp hinder för nyetablering och utveckling. Intresset av att bekämpa

brott är snarare så centralt att det måhända bör avvägas mot även andra samhällsintressen.

Ersättningsbestämmelser

Bestämmelser om ersättning i någon form skulle lösa flertalet av tveksamheterna kring förslaget i dessa hänseenden. Jag kan inte se att de nackdelar som framförts i betänkandet mot ett sådant system överväger fördelarna. Liksom tidigare ansluter jag mig således till dem som under remissen av beredningens betänkande SOU 2003:74 förordade bestämmelser om ersättning som inskränks till att täcka operatörernas kostnader. Bevisbördan bör, som föreslagits av beredningen, ligga hos operatörerna. För att undvika dröjsmål skulle ersättningsfrågan kunna avgöras i efterhand om överenskommelse inte kan nås.

Övriga frågor

I betänkandet framförs på enstaka ställen påståenden och slutsatser i detaljfrågor som jag inte helt kan dela. Dessa saknar dock betydelse för helhetsbedömningen och jag instämmer i övrigt väsentligen betänkandets förslag. På en punkt vill jag dock uttrycka en avvikande mening.

Det anges på ett par ställen i betänkandet att någon operatör skulle ha framfört att det inte läggs resurser på åtgärder som denne inte får betalt för, något som beredningen betraktar som anmärkningsvärt eftersom det rör sig om en skyldighet som framgår av lag. Jag kan inte se operatörens ståndpunkt som ett uttryck för att operatörer skulle avsiktligt bryta mot någon författning eller annat myndighetsbeslut. Yttrandet avspeglar enligt min mening den fullt legitima inställningen att operatörerna känner sig oförhindrade att, där utrymme finns, tolka bestämmelserna restriktivt i avvaktan på vägledande domstolsavgöranden men att tillåtna åtgärder som inte innebär en ekonomisk belastning vidtas, även om författningsstödet är osäkert eller saknas.

Bilaga 1, Dir. 2000:90

Sammanfattning av uppdraget

En beredning tillkallas med uppgift att verka för rättsväsendets utveckling. En huvuduppgift för beredningen blir att undersöka möjligheterna att med bibehållen rättssäkerhet öka effektiviteten och kvaliteten i rättsväsendets arbete. När det gäller lagföringen av brott skall beredningen särskilt undersöka möjligheterna att förkorta den genomsnittliga genomströmningstiden från brottsanmälan till dom och straffverkställighet. Beredningen skall också särskilt överväga på vilket sätt brottsutredningsverksamheten kan förbättras. Beredningen skall vidare uppmärksamma frågor om myndigheters lokalisering. I beredningens uppgift skall även ingå att överväga frågor om utbildning, kompetensutveckling och personalrörlighet inom rättsväsendet. Beredningens överväganden bör kunna leda till förslag som kan komma att innefatta allt från författningsändringar till ändringar av såväl administrativ som organisatorisk karaktär.

Beredningens arbete skall ske i nära samverkan med berörda myndigheter inom rättsväsendet och därvid ta hänsyn till det utvecklingsarbete som pågår. Detta utgör en fortsättning på och ett komplement till det arbete som redan inletts mellan företrädare för myndigheterna inom rättsväsendet och Regeringskansliet.

Delbetänkanden skall presenteras av beredningen efter hand som olika frågor behandlas.

Beredningen skall senast före utgången av år 2003 redovisa det vid detta tillfälle aktuella läget inom rättsväsendet för de frågor som ankommer på beredningen samt en plan för det fortsatta arbetet.

Bakgrund

Målet för rättsväsendet är den enskildes rättstrygghet och rättssäkerhet (prop. 2000/2001:1, utgiftsområde 4, avsnitt 4.3.1, bet. 2000/01:JuU1). Häri ligger bl.a. krav på att brott skall klaras upp samt leda till lagföring så snabbt och effektivt som möjligt utan att rättssäkerhetskraven åsidosätts. I syfte att uppnå detta har ett omfattande utvecklingsarbete bedrivits inom rättsväsendet under senare år. Sverige har vid en internationell jämförelse kommit långt i arbetet med att skapa ett rättsväsende som svarar mot högt ställda krav på snabbhet, effektivitet och rättssäkerhet. Samarbetet mellan rättsväsendets olika myndigheter utvecklas positivt. Samverkan är etablerad i många olika former och på flera nivåer.

Denna positiva utveckling till trots har ibland frågor av t.ex. administrativ, organisatorisk och författningsmässig karaktär betraktats utan tillräcklig samordning. Processer som hänför sig till gränssnitten mellan myndigheterna förtjänar således att ägnas ytterligare uppmärksamhet. En utvecklad och djupgående myndighetssamverkan som ett sätt att uppnå bl.a. en ökad snabbhet och effektivitet bör ha förutsättningar att få större genomslag. Samverkan skall ske med respekt för den grundläggande rollfördelningen mellan rättsväsendets myndigheter. Denna rollfördelning utgör ytterst en garanti för den demokratiska rättsstaten. I detta sammanhang måste främst domstolarnas och domarnas oberoende och särskilda roll framhållas.

En utgångspunkt bör kunna vara att en ökad samverkan myndigheter emellan samt en helhetssyn på rättsväsendet och ett flödesorienterat tänkesätt kan bidra till ökad effektivitet, snabbhet och rättssäkerhet. Det bör också bidra till att allmänheten uppfattar myndigheterna som mera tillgängliga och att stärka uppfattningen om en bra information och ett positivt bemötande.

Behov av en reformering

Allmänna utgångspunkter

Det fortsatta reformarbetet bör liksom hittills utgå från ett medborgarperspektiv och en helhetssyn på verksamheten inom rättsväsendet (jfr prop. 2000/2001:1, utgiftsområde 4, avsnitt 4.4.1). Medborgarperspektivet innebär att det alltid är nyttan för den enskilde medborgaren av tilltänkta förändringar och reformer som

skall stå i fokus. Helhetssynen innebär bl.a. att konsekvenserna för samtliga myndigheter av tilltänkta reformer och förändringar måste beaktas. Hinder av administrativ, organisatorisk och författningsmässig art som motverkar en snabb, effektiv och rättssäker hantering inom rättsväsendet bör identifieras och – i den mån det är möjligt och önskvärt – undanröjas. En långtgående myndighetssamverkan – med fortsatt bibehållen respekt för den grundläggande rollfördelningen – skall eftersträvas. Rättskedjeperspektivet, där samverkan och sambanden mellan myndigheterna poängteras, tillsammans med medborgarperspektivet skall således utgöra ledstjärnor i arbetet.

När det gäller innebörden av uttrycket rättsväsendet skall framhållas att i detta sammanhang avses – om inte annat uttryckligen anges - myndigheter som omfattas av politikområdet rättsväsendet.

I det följande redovisas ett antal områden där det bör finnas utrymme för förändringar av olika slag. För närvarande intar därvid frågor om minskade genomströmningstider i brottmål, den brottsutredande verksamheten, myndigheters lokalisering, utbildning, kompetensutveckling och personalrörlighet en central plats. I ett senare skede kan det också bli aktuellt att mera direkt inrikta sig mot andra frågor, t.ex. sådana som rör tvistemål och förvaltningsmål. Regeringen återkommer i så fall till dessa frågor. Här skall framhållas att det arbete med att utveckla och reformera rättsväsendet som nu och i framtiden bedrivs av rättsväsendets myndigheter och av regering och riksdag inte får hämmas av den tillkallade beredningens uppdrag. Det är tvärtom viktigt att detta reformarbete fortsätter med oförminskad kraft. Ett exempel på vad som pågår inom detta område är reformeringen av tingsrättsorganisationen.

De frågor som behandlas i det följande hör nära samman med och går delvis in i varandra. Så torde t.ex. en väl fungerande brottsutredningsverksamhet vara en förutsättning för ett snabbare flöde genom brottmålskedjan. Myndigheters lokalisering bör även ha betydelse för en effektiv och snabb hantering etc.

Minskade genomströmningstider i brottmål

En huvuduppgift i ett framtida reformarbete är att se över rättsväsendets hantering av brottmål för att undersöka möjligheterna att med bibehållen rättssäkerhet förkorta de totala genomströmningstiderna.

Det kan här vara relevant att återge viss statistik som rör genomströmningstider i brottmål.

Antalet till polisen inkomna ärenden utgjorde ca 1 160 000 år 1997, 1 170 000 år 1998 och 1 164 000 år 1999. De balanserade ärendena minskade med drygt 23 000 ärenden eller med 12 procent mellan 1997 och 1998 samt med 2 procent mellan 1998 och 1999 (se prop. 2000/2001:1, utgiftsområde 4, avsnitt 4.6.1 samt prop. 1999/2000:1, utgiftsområde 4, avsnitt 4.3.4). Trots de minskade balanserna ökade andelen balanserade ärenden som var äldre än tolv månader från 22 procent vid utgången av år 1997 till 24 procent vid utgången av år 1998. Vid utgången av år 1999 hade denna andel dock minskat till 19 procent. Genomströmningstiderna blev under perioden 1997–1999 längre inom nästan samtliga områden. Inom närpolisen har dock den genomsnittliga handläggningstiden inte ökat nämnvärt. Vid utgången av år 1999 var den 67 dagar. Antalet ärenden som redovisats till åklagare minskade från 192 482 ärenden år 1997 till 185 430 ärenden år 1998. År 1999 minskade antalet ytterligare till 168 228 ärenden.

Ur polisens årsredovisning för 1999 framgår att den genomsnittliga genomströmningstiden nu är för t.ex. våldsbrottsärenden 143 dagar, narkotikabrottsärenden 81 dagar och tillgrepps- och skadegörelsebrott 24 dagar.

Det finns naturligtvis flera förklaringar till de ökande genomströmningstiderna. Så förlänger, statistiskt sett, t.ex. avarbetningar av balanser av äldre mål den genomsnittliga genomströmningstiden för nya mål/ärenden.

Runt om i landet pågår nu en rad försöksprojekt som syftar till att, inom ramen för gällande regelverk, förkorta de totala genomströmningstiderna från brottsanmälan till dom. De första projekten startade för ca ett och ett halvt år sedan i Handen och i Jönköping. Ett av flera medel som man i projekten har använt för att minska genomströmningstiderna har varit att öka parallelliteten i handläggningen. Det innebär att nästa led i kedjan påbörjar handläggningen innan det tidigare ledet är helt klart med sin del. Man har också – i detaljerna – sett över rollfördelningen mellan framför allt polis och åklagare men även mellan åklagare och tingsrätt. En positiv effekt – vid sidan av minskade genomströmningstider – av det utökade samarbetet på dessa orter uppges för t.ex. domstolarnas del ha varit att antalet inställda huvudförhandlingar har minskat.

Det finns inte några givna svar på frågan hur brottmålsprocessen kan effektiviseras och förbättras. En författningsöversyn i syfte att skapa ett permanent snabbt förfarande i brottmål bör dock kunna övervägas. För att nämna några exempel skulle det inom ramen för en sådan översyn kunna vara aktuellt att t.ex. se över rollfördel-

ningen inom brottmålskedjan men också att överväga att införa särskilda tidsfrister för olika led i brottmålsprocessen. Frågan om tidsfrister är emellertid komplicerad, bl.a. eftersom detta skulle komma att innebära en ytterligare prioritering av vissa brottmål vid sidan av de prioriteringar som redan finns. Samtidigt måste också beaktas att ett snabbförfarande inte får leda till sämre rättssäkerhet för den som är berörd av brottsutredningen.

Det kan också finnas anledning att överväga vilken omfattning som brottsutredningarna måste ha i olika situationer. Det är möjligt att förenklingar kan genomföras i detta avseende som i kombination med andra åtgärder kan leda till en snabbare genomströmning. Även frågor om dokumentationskraven under en förundersökning kan vara aktuella att överväga i detta sammanhang.

Det finns naturligtvis även andra åtgärder än en författningsöversyn som kan vara aktuella. Det kan t.ex. gälla allt från att se över administrativa rutiner till frågan om harmonisering av organisationer.

En särskild fråga när det gäller att förkorta genomströmningstiderna är möjligheterna att utnyttja modern teknik. Den moderna tekniken bör i långt större utsträckning än i dag kunna bidra till att stödja brottmålsprocessen och därigenom också medverka till att förkorta genomströmningstiderna i rättsväsendet. Inom detta område bör det således finnas utrymme för förändringar av olika slag.

Den brottsutredande verksamheten m.m.

Hanteringen av brottmål intar en central plats inom rättsväsendet. I brottmålskedjan intar brottsutredningarna hos polisen en särställning. Frågan om hur denna utredningsverksamhet skall kunna ytterligare förbättras bör också hamna i fokus i det fortsatta reformarbetet.

Brottsutredningar bedrivs i dag inom polisen på olika nivåer, nämligen hos närpolisen samt vid kriminal- och länskriminalavdelningar. Viss brottsutredande verksamhet bedrivs centralt vid Rikspolisstyrelsen hos Rikskriminalpolisen och Säkerhetspolisen. Även i den lokala polisens utryckningsverksamhet bedrivs brottsutredning i form av s.k. förstahandsåtgärder.

För närvarande arbetar cirka 30 procent av landets 16 200 poliser med brottsutredningar. Av dessa beräknas ca 1 200 vara närpoliser medan 3 700 arbetar vid kriminal- och länskriminalavdelningarna (Polisväsendets budgetunderlag för åren 2001–2003, avsnitt 7.3).

En stor del av landets brottsutredningar avseende ekonomisk brottslighet bedrivs av poliser som är inkommenderade att tjänstgöra vid Ekobrottsmyndigheten. Ekobrottsmyndigheten – som är en åklagarmyndighet – inrättades den 1 januari 1998. Inrättandet av Ekobrottsmyndigheten har inneburit att två av länkarna i den s.k. brottmålskedjan i viktiga avseenden har kommit närmare varandra med betydande effektivitetsvinster som följd. Vid myndigheten arbetar åklagare, poliser och även andra specialister i nära samverkan med varandra. Under år 1999 tjänstgjorde i genomsnitt 387 personer vid Ekobrottsmyndigheten. Av dessa var 194 anställda vid myndigheten. Övriga 193 var poliser.

Även vid skattemyndigheterna bedrivs idag brottsutredande verksamhet. Denna verksamhet utförs vid skattebrottsenheterna, som inrättades under år 1998. Enheterna har bedrivit operativ verksamhet med inriktning på skatte- och bokföringsbrott sedan våren 1999. Under år 2000 tjänstgjorde ca 100 personer vid skattebrottsenheterna och en ytterligare utbyggnad planeras. Enheterna har inneburit ett resurstillskott för utredning av ekonomisk brottslighet.

Tullverket har ansvaret för utredning av alla smugglingsbrott. Brottsutredningarna verkställs av särskilda tullkriminalenheter inom verket. Enheterna är organisatoriskt åtskilda från den fiskala verksamheten. Personalen vid tullkriminalenheterna är tulltjänstemän som har fått kompletterande utbildning för handläggning av brottsutredningar. Under år 2000 tjänstgjorde ca 94 personer vid enheterna.

Uppklaringsprocenten för samtliga brott år 1998 var 27 procent. Samma år uppgick uppklaringsprocenten för brott mot brottsbalken till 20 procent Andelen uppklarade brott har minskat successivt, främst sedan början av 1980-talet. Det har dock skett en tydlig förbättring under de senaste två åren (uppgifterna är hämtade ur Brottsförebyggande rådets kriminalstatistik och Brottsförebyggande rådets tidskrift, APROPÅ nr 2/2000 s. 30 f).

Det totala antalet ärenden som redovisades från polisen till åklagare minskade med 9 procent mellan åren 1998 och 1999. Betydande minskningar i denna del gällde för tillgrepps- och skadegörelsebrott, våldsbrott, övriga brott och ekobrott (uppgifterna är hämtade ur Polisens årsredovisning för 1999). Endast 14 procent av polisens ärenden överlämnas nu till åklagare mot 26 procent vid mitten av 1990-talet. Drygt en miljon ärenden lades ned eller skrevs av under år 1998 på grund av att spaningsuppslag saknades eller spaning-

arna inte gett något resultat (uppgifterna är hämtade ur den s.k. SAMRED-rapporten 991011 från Justitiedepartementet).

Under senare tid har det, från olika håll, framförts vissa synpunkter när det gäller den brottsutredande verksamheten.

Riksåklagaren har konstaterat att möjligheten att klara upp ett brott väsentligt har minskat under hela 1990-talet. Riksåklagaren framhåller att det inom hela åklagarorganisationen finns en oro för att polisens resurser för den brottsutredande verksamheten inte tillgodoser de krav som måste ställas på en av de kanske viktigaste funktionerna i ett rättssamhälle, nämligen att de brott som har begåtts skall klaras upp och leda till lagföring. Det gäller en oro för såväl kvalitet som kvantitet. Riksåklagaren har från åklagarväsendet inhämtat att kvalitén på polisutredningarna ofta inte uppnår en godtagbar nivå och att det i mycket stor utsträckning krävs kompletteringar av utredningarna såväl vad gäller rena formella krav som mer materiellt inriktade uppgifter. Riksåklagaren uppger också att många åklagare upplever att de får ”kämpa om utredningsmän” och att det blir allt svårare att driva utredningar med de krav som nu gäller i fråga om förbättrad lagföring och kortare handläggningstider (uppgifterna är hämtade ur Riksåklagarens budgetunderlag för år 2001).

Granskningskommissionen i anledning av brottsutredningen efter mordet på Olof Palme har i sitt betänkande pekat på brister och oklarheter i brottsutredningssystemet (SOU 1999:88). I betänkandet behandlas således frågor om bl.a. ansvars- eller rollfördelningen mellan polis och åklagare samt förundersökningsledarskapets innebörd.

När det gäller frågan hur utredningsverksamheten hos polisen bör vara organiserad har riksdagen i ett tillkännagivande till regeringen uttalat att regeringen bör se över denna fråga och vidta de åtgärder som behövs för att åstadkomma en specialisering av utredningsverksamheten inom närpolisen (bet. 1999/2000:JuU11, rskr. 1999/2000:211).

Rikspolisstyrelsen har uppgett att den brottsutredande verksamheten, till följd av resursläget, inte är helt tillfredsställande (Polisväsendets budgetunderlag för åren 2001–2003, avsnitt 6.4). Rikspolisstyrelsen har dock framhållit att en av orsakerna till att antalet ärenden som redovisats till åklagare har minskat är de nya reglerna om ledningen av förundersökningen i brottmål, det s.k. fördelningscirkuläret. Dessa har inneburit att polisen har fått större möjligheter att på egen hand slutföra handläggningen av vissa ärenden. Även förändringar i antalet till polisen inkomna ärenden har lyfts

fram när det gäller antalet ärenden som redovisas till åklagare (uppgifterna är hämtade ur Polisens årsredovisning för år 1999).

Det pågår arbete inom såväl polis- som åklagarväsendena för att förbättra den brottsutredande verksamheten. Samtidigt finns det skäl att i det fortsatta utvecklingsarbetet fokusera än mer på denna verksamhet. Det finns naturligtvis inget enkelt svar på frågan hur det går att uppnå en bättre fungerande sådan verksamhet. Ett brett angreppssätt bör därför anläggas där såväl ny lagstiftning som administrativa och organisatoriska förändringar övervägs. Även frågor om rollfördelning, utveckling av arbetsmetoder, möjlighet att utnyttja modern teknik, utbildning och kompetensutveckling samt rekrytering bör kunna övervägas i detta sammanhang. Samarbete och samverkan inom rättsväsendet bör utgöra ledstjärnor i arbetet.

Vad gäller rättsväsendets och särskilt polisens arbetsmetoder finns det anledning att överväga om det behövs författningsändringar som kan förbättra möjligheterna att förhindra, avslöja, utreda eller lagföra brott. Inte minst gäller det brott av organiserad eller annan allvarlig karaktär. I det sammanhanget kan det t.ex. finnas anledning att överväga frågor om tvångsmedel.

Utbildning, kompetensutveckling och personalrörlighet

Vid sidan av de reformer som rör redovisade områden kan sägas ligga frågor om utbildning, kompetensutveckling och personalrörlighet inom rättsväsendet. När det gäller den framtida utvecklingen bör dock på nytt framhållas att frågorna hör ihop på ett eller annat sätt. Frågor som rör utbildning, kompetensutveckling och personalrörlighet bör således kunna vara aktuella även vid överväganden som gäller t.ex. minskade genomströmningstider i brottmål och den brottsutredande verksamheten.

Brottsutvecklingen har inneburit att det ställs allt större krav när det gäller kompetens, skicklighet och effektivitet. Rättsväsendets myndigheter utvecklar också fortlöpande sin verksamhet för att kunna möta dessa krav. Här redovisas i korthet vad som pågår på detta område inom polis-, åklagar- och domstolsväsendena.

Polisutbildningen har genomgått stora förändringar under de senaste åren. Den nya grundutbildningen startade i januari 1998 vid Polishögskolan i Solna. Ett nytt antagningssystem tillämpas och utbildningen bygger på en ny metodik. Umeå universitet har fått ansvaret att vid sidan av Polishögskolan bedriva grundutbildning för poliser. Inom Rikspolisstyrelsen övervägs nu om utbildningen

också skall förläggas till ytterligare någon eller några orter i de södra delarna av landet.

Polismyndigheterna har utarbetat chefsförsörjningsprogram och planer för kompetensförsörjning. Flera myndigheter har ett samarbete i dessa frågor med universitet och högskolor. Ledarskapscentrum vid Polishögskolan har tillkommit för att stödja polismyndigheterna i deras arbete med chefsförsörjning och chefsutveckling. Polishögskolan erbjuder vidareutbildning till samtliga polismyndigheter och flera av utbildningarna är öppna för civilanställd personal och deltagare från övriga rättsväsendet.

Även åklagarväsendet utvecklar fortlöpande sin verksamhet för att kunna möta de krav som ställs på en modern organisation inom rättsväsendet. Inom åklagarväsendet genomförs därför betydande utbildningssatsningar för åklagarna. Det finns numera ett stort antal åklagare med specialistkompetens på de kriminalpolitiskt prioriterade områdena. Under år 2000 har alla specialiståklagare påbörjat en 3-årig högre åklagarutbildning som bl.a. tar sikte på olika brottstyper, t.ex. gränsöverskridande grov brottslighet, grova vålds- och narkotikabrott samt grova sexualbrott mot barn. Dessutom får samtliga åklagare som genomgått grundkursen för åklagare fortlöpande vidareutbildning varje år. Under 1999 ökade antalet utbildningsdagar från 4 till 17. Utvecklingen inom åklagarväsendet har fört med sig att det numera finns goda möjligheter till individuell utveckling och verksamhetsanpassad kompetens för åklagarna.

Inom domstolsväsendet genomförs nu utbildningsåtgärder i enlighet med en av Domstolsverket tillsammans med domstolarna utarbetad plan för domstolsanställda. Genom denna nya utbildningsplan kommer antalet kurser att utökas för samtliga personalkategorier. Utbildningsinsatser för icke ordinarie domare kommer sannolikt att utökas ytterligare till följd av det uppdrag som regeringen lämnade till Domstolsverket i regleringsbrevet för år 2000 avseende utformningen av domarutbildningen. Ordinarie domare kommer under de första anställningsåren att kallas till sammanlagt fem veckors obligatorisk utbildning. Samtliga domare kommer fortsättningsvis att kallas till en veckas återkommande utbildning vart tredje år. I övrigt erbjuds ett omfattande utbud av fördjupningskurser och specialkurser i olika ämnen. Samarbetet med universitet och högskolor kommer att utökas. Enligt utbildningsplanen kommer även övrig personal att kallas till baskurser, grundkurser, påbyggnadskurser och återkommande utbildning.

När det gäller domarutbildningen har regeringen fattat beslut om att den praktiska tjänstgöringen i underrätt skall förlängas från

ett till två år. Regeringen har dessutom för avsikt att i särskild ordning se över domarutbildningen i ett bredare perspektiv (se regeringens skrivelse [1999/2000:106] Reformeringen av domstolsväsendet – en handlingsplan).

Här kan också nämnas den högre utbildning i tillämpad kriminologi som Brottsförebyggande rådet bedriver tillsammans med kriminologiska institutionen vid Stockholms universitet. Utbildningen, som startade vårterminen 1999, ger 40 universitetspoäng och vänder sig till all personal inom rättsväsendet. Hittills har 110 personer antagits till utbildningen.

Det finns även i fortsättningen skäl att följa det arbete som pågår – i detta sammanhang – för att förvissa sig om att utvecklingen sker samordnat och med en helhetssyn för ögonen. Ett reformbehov inom nu aktuellt område kan handla om allt från gemensam utbildning och utbytestjänstgöring till behörighetskrav för de olika yrkesbanorna och arbetsuppgifter inom ramen för dem.

Lokaliseringsfrågor

En annan fråga gäller myndigheters lokalisering. Vid överväganden om myndigheters lokalisering innebär det anlagda helhetsperspektivet att myndigheternas planering av var viss verksamhet skall lokaliseras måste samordnas. Om t.ex. kriminalvården planerar var häkten skall lokaliseras får detta konsekvenser även för polisen när det gäller t.ex. lokalisering av arrester. Å andra sidan är kriminalvårdens transportorganisation beroende av var tingsrätterna är lokaliserade. Även åklagarna är beroende av och tjänar på korta avstånd till tingsrätterna etc.

Medborgarperspektivet innebär i detta sammanhang att det inte skall vara orimliga geografiska avstånd mellan medborgarna och rättsväsendets myndigheter. Å andra sidan bör man beakta att myndigheternas verksamhet ställer olika krav på närhet. Detta förhållande leder till att vissa av rättsväsendets myndigheter bör finnas lokaliserade till många orter över hela landet.

De omorganisationer av framför allt polis- och åklagarväsendena som ägt rum under senare år har på många orter fått till följd att de geografiska avstånden mellan utredningspersonalen och åklagarna har ökat. Det har framförts att det i sin tur har inneburit försämringar när det gäller det faktiska utredningsarbetet och samarbetet mellan polis och åklagare. Det finns nu skäl att överväga vilka åtgärder som skulle kunna vidtas för att i möjligaste mån överbrygga de hinder som uppstått genom organisationsförändringarna.

Här kan nämnas att i det arbete som nu pågår i särskild ordning med att reformera tingsrättsorganisationen utgör bl.a. den geografiska samordningen med rättsväsendets övriga myndigheter en viktig komponent.

Även för övriga delar av rättsväsendet och alldeles oavsett om organisationsförändringar har ägt rum finns det skäl att ägna lokaliseringsfrågor särskild uppmärksamhet. En fråga som bör vara aktuell att överväga i detta sammanhang är om det finns behov av ett särskilt ”samordningsforum” för lokaliseringsfrågor inom hela rättsväsendet. Vid ett sådant forum skulle myndigheterna ha att t.ex. presentera sina såväl kortsiktiga som långsiktiga planer i lokaliseringsfrågor. Även andra frågor som hör samman med var viss verksamhet skall vara lokaliserad bör kunna diskuteras och samordnas inom ramen för ett sådant forum.

Uppdraget

En särskild beredning tillkallas med uppgift att verka för rättsväsendets utveckling. En huvuduppgift för beredningen blir att undersöka möjligheterna att med bibehållen rättssäkerhet öka effektiviteten och kvaliteten i rättsväsendets arbete.

En viktig uppgift för beredningen är att bidra till att utvecklingsarbetet inom rättsväsendet sker samlat och utifrån ett helhetsperspektiv.

Målet för beredningen skall vara att bidra till att uppnå en ökad kvalitet i vid bemärkelse inom hela rättsväsendet. Beredningen skall därvid särskilt uppmärksamma frågor om en effektivare lagföring för brott och kortare genomströmningstid för mål och ärenden. I det sammanhanget skall beredningen överväga om det behövs förändringar i de regelsystem som styr främst polisens spanings- och utredningsverksamhet, åklagarnas verksamhet samt rättegångsförfarandet. Beredningen bör även överväga om det behövs några organisatoriska åtgärder på detta område.

Beredningen skall kontinuerligt kartlägga och följa det utvecklingsarbete som äger rum inom rättsväsendet. Resultaten av de granskningar av rättsväsendets myndigheter som har gjorts i olika sammanhang bör analyseras och beaktas. Beredningen skall fortlöpande identifiera organisatoriska, administrativa och författningsmässiga hinder för en rationell och effektiv verksamhet. Beredningen skall vidare bedöma och utveckla andras och egna förslag och idéer och därefter initiera det arbete som krävs. Här skall framhål-

las att den formella kompetensen att genomföra förändringar i vissa fall ligger hos myndigheterna och i andra fall hos regering och riksdag. Beredningens uppdrag innebär i detta hänseende självfallet ingen förändring. I många fall kan beredningen fullgöra sitt uppdrag genom att ta initiativ till att myndigheterna uppmärksammas på att det finns ett behov av förändring och sedan överlämna åt myndigheterna att själva besluta om åtgärder eller om att lägga fram förslag. I andra fall krävs att beredningen själv lägger fram förslag. Det får bli en uppgift för beredningen att från fall till fall ta ställning till vilken väg som bör väljas.

En del frågor som ligger inom ramen för beredningens uppdrag kan vara föremål för redan pågående arbete inom Regeringskansliet eller hos någon myndighet. Det är inte avsikten att sådant arbete skall avstanna eller försenas genom tillsättandet av beredningen. I sådana fall förutsätts i stället att beredningen och berörda parter kommer överens om hur arbetet i fortsättningen skall bedrivas. Under den tid som beredningen arbetar kan det också framträda nya områden där ett reformbehov föreligger. Även i sådana fall får det förutsättas att beredningen och berörda parter kommer överens om hur arbetet skall bedrivas.

En aktiv medverkan från rättsväsendets myndigheter är en nödvändig förutsättning för att utvecklingsarbetet skall kunna bli framgångsrikt. Hinder för ett snabbt och effektivt flöde genom rättskedjan identifieras bäst med hjälp av dem som rent faktiskt arbetar inom rättsväsendet. Beredningens arbete skall således ske i nära samverkan med berörda myndigheter inom rättsväsendet. För detta ändamål skall inrättas särskilda referens- och arbetsgrupper.

Inom de områden som här redovisas bör det finnas utrymme för förändringar av olika slag. Beredningen är oförhindrad att ta upp även andra frågor som arbetet ger anledning till och som gäller utvecklingen av rättsväsendet. För domstolarnas del kan det t.ex. gälla handläggningen av tvistemål och övriga domstolsuppgifter.

Beredningens arbete skall dock, åtminstone tills vidare, såvitt gäller domstolsväsendet endast omfatta verksamheten vid de allmänna domstolarna. Detta hindrar emellertid inte att beredningen när den lägger fram sina förslag kan ta hänsyn till att de lösningar som tas fram kan komma till användning också inom domstolsväsendet i övrigt.

I det följande redovisas några frågor som beredningen särskilt bör uppmärksamma inom ramen för sitt arbete.

Minskade genomströmningstider i brottmål

En huvuduppgift för beredningen är att se över rättsväsendets hantering av brottmål i syfte att undersöka möjligheterna att med bibehållen rättssäkerhet förkorta den totala genomströmningstiden från brottsanmälan till dom och straffverkställighet. Beredningen bör här kunna lämna förslag till åtgärder av olika slag. Dessa förslag kan komma att innefatta allt från att identifiera behov av författningsändringar till att ta fram färdiga förslag till sådana. Även förslag till förändringar av såväl administrativ som organisatorisk karaktär bör kunna ingå i beredningens överväganden. Frågor om utbildning och kompetensutveckling skulle också kunna bli aktuella att överväga i detta sammanhang.

Det är också en uppgift för beredningen att överväga på vilket sätt den moderna tekniken på ett bättre sätt än i dag kan stödja brottmålsprocessen och därigenom också bidra till bl.a. kortare genomströmningstider. Uppdraget i denna del innefattar även att undersöka om det i lagstiftningen finns hinder mot ett effektivt utnyttjande av IT-stödet i rättsväsendets verksamhet.

Den brottsutredande verksamheten m.m.

En annan huvuduppgift för beredningen, som hör nära samman med den föregående, är den brottsutredande verksamheten. En väl fungerande brottsutredningsverksamhet torde vara en grundförutsättning för en hög uppklaringsprocent samt ett snabbare flöde genom brottmålskedjan.

Beredningen skall överväga på vilket sätt denna verksamhet kan förbättras. Frågan bör närmas utifrån ett brett angreppssätt och kan komma att innefatta överväganden som innebär förslag till förändringar av såväl författningsmässig som administrativ och organisatorisk karaktär. Även frågor om rollfördelning, utveckling av arbetsmetoder, möjligheter att utnyttja modern teknik, utbildning och kompetensutveckling samt rekrytering bör kunna ingå i överväganden. För att nå målen när det gäller kriminalpolisverksamheten är det nödvändigt att beredningen också i viss utsträckning behandlar frågor om ordningspolisverksamheten. Det är emellertid inte avsikten att beredningen mera allmänt skall göra någon översyn av arbetsmetoderna inom ordningspolisverksamheten.

Beredningens överväganden när det gäller frågor av författningsmässig karaktär kan innebära allt ifrån att identifiera behov av författningsändringar till att presentera färdiga förslag till sådana.

Såvitt avser beredningens överväganden av författningsmässig karaktär och frågor om arbetsmetoder är det motiverat att även inbegripa Tullverkets och skattemyndigheternas brottsutredande verksamhet i beredningens uppdrag.

När det gäller frågor av organisatorisk karaktär skall det i beredningens uppdrag även ingå att se över frågan om en specialisering av utredningsverksamheten inom närpolisen och jämföra detta med andra alternativ.

Beredningen skall vidare beakta de synpunkter som framförs i Granskningskommissionens betänkande (SOU 1999:88) såvitt gäller den brottsutredande verksamheten. Det innebär att beredningen skall ha till uppgift att bl.a. se över frågan om ansvarsfördelningen mellan polis och åklagare.

Utbildning, kompetensutveckling och personalrörlighet

Beredningen skall följa det arbete som pågår inom rättsväsendet när det gäller utbildning, kompetensutveckling och personalrörlighet. Beroende på resultatet av denna kartläggning bör beredningen kunna lämna förslag som syftar till att uppnå största möjliga samordning även inom detta område. Beredningens överväganden kan komma att handla om gemensam utbildning och gemensamma utbildningsinstitutioner samt olika former av utbytestjänstgöring inom rättsväsendet. Även frågor om behörighetskrav för yrkesbanorna inom rättsväsendet eller för fullgörandet av särskilda uppgifter där kan ingå i övervägandena.

Lokaliseringsfrågor

Beredningen skall överväga om det finns anledning att ta några initiativ när det gäller att få till stånd en ökad samordning mellan rättsväsendets myndigheter i lokaliseringsfrågor. Det kan t.ex. ifrågasättas om det finns behov av ett särskilt ”samordningsforum” där myndigheterna hade att presentera såväl sina kortsiktiga som långsiktiga planer i lokaliseringsfrågor. Om beredningen kommer fram till att så är fallet bör man också kunna redovisa på vilket sätt och i vilka former ett sådant forum skulle kunna verka.

Övrigt

Förutom att beredningen skall arbeta med referens- och arbetsgrupper bör beredningen särskilt uppmärksamma behovet av samråd med dels berörda myndigheter inom rättsväsendet, dels sådana utredningar som initieras under beredningens arbete och som kan ha samband dess uppdrag.

Beredningen bör samråda med

- 1999 års rättegångsutredning (Ju 1999:11),
- utredningen om genomförandet av polisregisterlagstiftningen (Ju 2000:01) samt
- Rådet för rättsväsendets informationsförsörjning (dnr Ju96/3163).

Beredningen bör dessutom hålla kontakt med den arbetsgrupp inom domstolsväsendet som arbetar med processrättsliga frågor.

Beredningen bör hålla sig informerad om den fortsatta beredningen med anledning av betänkandena Den centrala polisen (SOU 2000:25) och Organiserad brottslighet, hets mot folkgrupp, hets mot homosexuella, m.m. – straffansvarets räckvidd – (SOU 2000:88).

Förslag skall presenteras i delbetänkanden av beredningen efter hand som olika frågor behandlas.

Beredningen skall senast före utgången av år 2003 redovisa det vid detta tillfälle aktuella läget inom rättsväsendet för de frågor som ankommer på beredningen samt en plan för det fortsatta arbetet.

(Justitiedepartementet)

Bilaga 2, Dir. 2003:145

Sammanfattning av uppdraget

Beredningen för rättsväsendets utveckling (dir. 2000:90) ges i uppdrag att göra en översyn av uppgifts- och ansvarfördelningen mellan polis och åklagare. Vidare skall beredningen göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation.

Beredningen skall lämna de förslag till författningsändringar och andra åtgärder som uppdraget kan ge anledning till.

Beredningens nuvarande uppdrag

Den 7 december 2000 beslutade regeringen att tillkalla en beredning med uppgift att verka för rättsväsendets utveckling. En huvuduppgift för beredningen är att undersöka möjligheterna att med bibehållen rättssäkerhet öka effektiviteten och kvaliteten i rättsväsendets arbete. När det gäller lagföringen av brott skall beredningen särskilt undersöka möjligheterna att förkorta den genomsnittliga genomströmningstiden från brottsanmälan till dom och straffverkställighet. Beredningen skall också särskilt överväga på vilket sätt brottsutredningsverksamheten kan förbättras. I beredningens uppgift ingår även att överväga frågor om utbildning, kompetensutveckling och personalrörlighet inom rättsväsendet.

Beredningens överväganden bör kunna leda till förslag som kan komma att omfatta allt från författningsändringar till ändringar av såväl administrativ som organisatorisk karaktär.

Beredningens arbete skall ske i nära samverkan med berörda myndigheter inom rättsväsendet och ta hänsyn till det utvecklingsarbete som pågår där.

Delbetänkanden skall presenteras av beredningen efter hand som olika frågor behandlas.

Beredningen skall senast den 31 december 2003 redovisa det aktuella läget inom rättsväsendet för de frågor som ankommer på beredningen och presentera en plan för det fortsatta arbetet.

Beredningens hittillsvarande arbete

Beredningen har hittills lagt fram fem delbetänkanden. I det första, Snabbare lagföring 1 – Några förslag till förenklingar (SOU 2001:59) föreslogs vissa åtgärder för att förkorta genomströmningstiden i brottmål samt för att underlätta att förhör under förundersökning kan komma till stånd. Förslagen är genomförda. I det andra, Snabbare lagföring 2 – Förenklad brottsutredning (SOU 2001:93), föreslogs att förenklad brottsutredning skulle kunna användas i stället för förundersökning i större utsträckning än hittills. I det tredje, Snabbare lagföring 3 – Snatteribrott (SOU 2002:44) föreslogs framför allt förenklingar i brottsutredningsförfarandet vad gäller snatteribrott. I det fjärde, Snabbare lagföring 4 – Ett snabbförfarande för brottmål (SOU 2002:45) föreslogs en försöksverksamhet med snabbare brottmålsförfarande i Stockholmsområdet. I det femte, Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74), lämnades förslag om framför allt nya regler för vissa av de brottsbekämpande myndigheternas arbetsmetoder samt en utvidgning av möjligheterna att använda strafföreläggande. Förslagen i betänkandena två till fyra har remissbehandlats och övervägs nu i Regeringskansliet. Det femte betänkandet har sänts ut på remiss.

Behovet av tilläggsdirektiv

Uppgifts- och ansvarsfördelning mellan polis och åklagare

Allmänna utgångspunkter

Regeringen bedömer liksom polisen och åklagarväsendet att det är nödvändigt att vidta ytterligare åtgärder för att höja kvaliteten och effektiviteten i brottsutredningsverksamheten. Frågan om uppgifts- och ansvarsfördelningen mellan polis och åklagare har en framträdande plats i det arbetet. I flera budgetpropositioner har

regeringen uttalat att det är angeläget att polisens och åklagarnas roller i brottsutredningssystemet vidareutvecklas. Regeringen har i det sammanhanget understrukit vikten av att polisen betydligt oftare än i dag är förundersökningsledare i brottmålsärenden av enkel och medelsvår karaktär (se prop. 2002/03:1 s. 28 f. och prop. 2003/04:1 s. 28 f.).

Mot denna bakgrund har myndigheterna under flera år eftersträvat att generellt införa en sådan ordning som skulle bidra till att åklagarna i större utsträckning skulle kunna koncentrera sina insatser på komplicerade brottmålsärenden och utöva aktiv förundersökningsledning i dessa. Myndigheternas insatser har dock hittills inte lett till några större förändringar i uppgifts- och ansvarsfördelningen mellan dem.

När det gäller förhållandet mellan polismyndighet och åklagare under genomförandet av en förundersökning i brottmål finns det grundläggande bestämmelser i 23 kap. 3 § rättegångsbalken. Därutöver har Riksåklagaren efter samråd med Rikspolisstyrelsen utfärdat allmänna råd och föreskrifter om ledningen av förundersökning m.m. (RÅFS 1997:12).

Granskning och utvecklingsarbete

Granskningskommissionen i anledning av brottsutredningen efter mordet på statsminister Olof Palme har pekat på oklarheter i roll- och ansvarsfördelningen mellan polis och åklagare. Kommissionen understryker att såväl det reella som det formella ansvaret för en förundersökning alltid ligger på förundersökningsledaren (SOU 1999:88 s. 990 f.).

Rikspolisstyrelsen och Riksåklagaren har i sina remissyttranden över betänkandet angett att det är nödvändigt att bl.a. vidareutveckla polisens och åklagarnas roller i brottsutredningsarbetet (dnr Ju1999/3196/PÅ).

Därutöver har Riksrevisionsverket i en rapport till regeringen velat fästa regeringens uppmärksamhet på att det kan finnas anledning att överväga vilka åtgärder som bör vidtas för att klargöra ansvarsförhållandet mellan åklagare i egenskap av förundersökningsledare och polisen som utredare. Enligt Riksrevisionsverket ligger det ett dilemma inbyggt i det faktum att åklagaren kan ge direktiv om vad som skall utföras, men inte disponera över polisens resurser (Rapport 2003:15 s. 23).

Flera åtgärder i syfte att stärka förundersökningsledningen har redan genomförts. Inom polisen har särskild utbildning av förun-

dersökningsledare anordnats. Uppgiften att vara polisiär förundersökningsledare har renodlats. Åtgärderna har medfört att det har skapats bättre förutsättningar för en kvalificerad förundersökningsledning hos polisen. Inom åklagarväsendet har man genomfört en satsning på specialiståklagare för förundersökningsledning inom svårutredda brottsområden samt ett utökat deltagande av åklagare i polisens brottsutredande verksamhet, både i form av handledning och som förundersökningsledare.

Genom inrättandet av Ekobrottsmyndigheten finns goda förutsättningar för en vidareutveckling av arbetsmetoderna inom ekobrottsbekämpningen. Myndigheten har ett nationellt samordningsansvar för bekämpningen av ekonomisk brottslighet. Vid myndigheten genomförs förundersökningar regelmässigt av arbetsgrupper som består av åklagare, polismän, ekonomer och andra specialister. Arbetet i grupperna sker under ledning av åklagare.

Dessutom bedriver både polisen och åklagarväsendet ett omfattande arbete för att förstärka och vidareutveckla det internationella samarbetet inom brottsbekämpningen. Det ställs krav på att polis och åklagare skall ha en god förmåga att effektivt och rättssäkert kunna lämna bistånd till utländska brottsbekämpande myndigheter.

Mot bakgrund av denna verksamhetsutveckling anser Rikspolisstyrelsen och Riksåklagaren att det nu finns ett behov av att utreda hur den framtida uppgifts- och ansvarsfördelningen bör vara mellan polis och åklagare när det gäller att utreda och lagföra brott. Frågan om polisen i större utsträckning än i dag skall kunna vara förundersökningsledare när det gäller s.k. mängdbrottslighet har en framträdande plats i myndigheternas utvecklingsarbete.

Enligt de ursprungliga direktiven kan beredningen vid övervägandena som rör förbättringar i verksamheten med att uppdaga, utreda och lagföra brott också överväga bl.a. frågor om rollfördelning. Det finns dock behov av att ge beredningen vissa ytterligare riktlinjer för det arbetet.

Elektronisk kommunikation

Nuvarande regelverk

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns i 27 kap. rättegångsbalken. Ett beslut om hemlig teleavlyssning eller hemlig teleövervakning innebär att de brottsutredande myndigheterna får rätt att avlyssna eller med tekniskt hjälpme-

del ta upp telemeddelanden eller uppgifter om sådana meddelanden.

Den 25 juli 2003 trädde lagen (2003:389) om elektronisk kommunikation i kraft och ersatte då telelagen (1993:597) och lagen (1993:599) om radiokommunikation.

I 17 § telelagen fanns en bestämmelse om skyldighet för den som hade tillstånd enligt telelagen att bedriva televerksamhet så att hemlig teleavlyssning och hemlig teleövervakning kunde verkställas och så att verkställandet inte röjdes. Innehållet i och uppgifter om de avlyssnade eller övervakade telemeddelandena skulle göras tillgängliga så att informationen enkelt kunde tas om hand (anpassningsskyldighet). Dessutom innehöll telelagen bestämmelser som under vissa förutsättningar gav de brottsbekämpande myndigheterna rätt att, utan domstolsprövning, få ut vissa uppgifter om telemeddelanden från teleoperatörerna.

Lagen om elektronisk kommunikation har en annan terminologi och delvis andra utgångspunkter än telelagen. Lagen om elektronisk kommunikation innehåller emellertid bestämmelser om hemlig teleavlyssning m.m. samt utlämnande av uppgifter till brottsbekämpande myndigheter som är avsedda att så långt som möjligt motsvara det regelverk som gällde enligt telelagen.

Den som i vissa fall tillhandahåller ett allmänt kommunikationsnät eller tjänster inom ett sådant nät har enligt 6 kap. 19 § lagen om elektronisk kommunikation en skyldighet att bedriva verksamheten så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Enligt motiven till lagstiftningen är bestämmelsen avsedd att så nära som möjligt täcka samma typer av verksamhet för vilket anpassningsskyldighet gällt enligt 17 § telelagen (prop. 2002/03:110 s. 269).

Därutöver innehåller lagen om elektronisk kommunikation bestämmelser som ger de brottsutredande myndigheterna vissa möjligheter att utan domstolsprövning hämta in uppgifter om elektroniska meddelanden (6 kap. 20–23 §§). Enligt motiven till lagstiftningen motsvarar dessa bestämmelser det som gällt enligt 45–47 samt 54 §§ telelagen (a. prop. s. 397).

Utgångspunkter

Lagen om elektronisk kommunikation bygger på de förslag som e-komutredningen lämnade i delbetänkandet Lag om elektronisk kommunikation (SOU 2002:60). När utredningens förslag remitterades angavs i remisskrivelsen (dnr N2002/7230/ITFoU) bl.a. föl-

jande. De föreslagna bestämmelserna har ett delvis annat innehåll än de bestämmelser som gäller i dag. Vissa av de frågor som utredningen tar upp och vissa av de förslag som läggs fram har betydelse för de brottsbekämpande myndigheternas brottsutredande verksamhet. Det finns också ytterligare frågor av stor betydelse på området som inte behandlas i betänkandet. En viktig fråga ur brottsbekämpningssynpunkt är vilka verksamheter som bör omfattas av anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. En annan fråga är vilka trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndigheterna. Ytterligare en fråga är i vilken utsträckning och under vilka förutsättningar som trafikuppgifter bör bevaras hos operatörerna. Dessa frågor och andra frågor som har ett samband med dessa finns det ett klart behov av att utreda ytterligare. Detta kommer att ske i särskild ordning.

Att det finns ett behov av att utreda dessa frågor bekräftas av regeringen i den proposition som ligger till grund för den nya lagstiftningen. Regeringen anger att anpassningsskyldighetens omfattning i förhållande till det nya regelverket på området för elektronisk kommunikation är komplicerad och kräver en fördjupad analys som inte kan göras inom ramen för det lagstiftningsärendet. Regeringen förklarar att frågan i stället kommer att behandlas i ett annat sammanhang där även närliggande frågor kommer att utredas. Regeringen framhåller att begreppet telemeddelande används i rättegångsbalken och att det även fanns definierat i telelagen men att det däremot inte används i EG:s regelverk för elektronisk kommunikation. I avvaktan på nämnda utredning ansåg regeringen det vara lämpligt att, för att inte skapa rättsosäkerhet i fråga om tillämpningen av de författningar som innehåller begreppet telemeddelande, såsom en övergångslösning använda begreppet telemeddelande såvitt avser anpassningsskyldighet (prop. 2002/03:110 s. 269).

Även i propositionen 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering gör regeringen bedömningen att vissa frågor kräver ytterligare utredning. I det lagstiftningsärendet föreslår regeringen vissa ändringar när det gäller bestämmelserna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. Regeringen anger att när det bl.a. gäller frågan om att avskaffa möjligheten för brottsutredande myndigheter att inhämta uppgifter om telemeddelande direkt från teleoperatören, så kommer den att övervägas ytterligare inom ramen

för den kommande översynen av vissa frågor som rör teleoperatörers anpassningsskyldighet m.m.

Beredningen har enligt sina ursprungliga direktiv till uppgift att komma med förslag som kan förbättra den brottsutredande verksamheten. I den uppgiften ingår att överväga frågor om de brottsbekämpande myndigheternas arbetsmetoder, inklusive frågor om tvångsmedel och möjligheten att utnyttja modern teknik i arbetet. Det framstår därigenom som ändamålsenligt att beredningen överväger även de frågor om elektronisk kommunikation som inte behandlades i de nämnda lagstiftningsärendena. Även i denna del finns det behov av att ge beredningen vissa riktlinjer för arbetet.

Uppdraget

Uppgifts- och ansvarsfördelning mellan polis och åklagare

Som ett led i sitt arbete enligt de ursprungliga direktiven skall beredningen särskilt överväga om förändringar i uppgifts- och ansvarsfördelningen mellan polis och åklagare kan bidra till att öka effektiviteten och kvaliteten i den verksamhet som syftar till att uppdaga, utreda och lagföra brott. Dessa överväganden skall utgå från att polisen och åklagarväsendet även i fortsättningen skall vara skilda myndigheter. Inget hindrar dock att beredningen överväger om en ökad administrativ eller annan samverkan mellan myndigheterna kan ge fördelar för bl.a. verksamheten med att uppdaga, utreda och lagföra brott.

Vid bedömningen av vilka uppgifter som bör tilldelas polisen respektive åklagarna bör beredningen utgå från att åklagarinsatserna skall intensifieras när det gäller den mer kvalificerade brottsligheten och att åklagarna där skall delta i brottsutredningarna mera aktivt och i större omfattning än i dag. En utgångspunkt skall vara att åklagarna i sin roll som förundersökningsledare skall ges bättre reella möjligheter att påverka brottsutredningarnas förlopp och därigenom få ett tydligare helhetsansvar för utredningarnas kvalitet och resultat. Det kräver att åklagarna avsätter mer egna resurser för det. För att det skall vara möjligt måste de avlastas från andra uppgifter som är av sådan art att de inte kräver åklagarinsats. Beredningen bör därför vid genomförandet av uppdraget utgå från att polisen alltid skall vara förundersökningsledare i utredningar som rör inte alltför kvalificerad brottslighet. Det bör också övervägas i vilken mån andra omständigheter än brottets svårhetsgrad bör

kunna vägas in vid bedömningen av hur ledarskapet för förundersökningen skall fördelas.

Beredningen skall vidare överväga i vad mån det behövs ytterligare åtgärder för att polisen skall kunna fullgöra förundersökningsledning på ett effektivt sätt och med hög kvalitet. En viktig fråga som beredningen skall överväga i det sammanhanget är om det kan finnas ett behov av att tillföra polisen ytterligare juridisk kompetens.

Beredningen skall också överväga om det kan finnas skäl att förändra det nuvarande sättet att leda och styra över tillgängliga utredningsresurser samt formerna för operativ samverkan i brottsutredningsverksamheten. I det ligger att beskriva och undersöka vad som behöver göras för att klarlägga polisens och åklagarnas ansvar vid genomförandet av en förundersökning. Dessa överväganden skall framför allt avse polisens och åklagarnas bekämpning av omfattande eller kvalificerad brottslighet, t.ex. sådan som är grov eller gränsöverskridande. I anslutning till dessa överväganden skall beredningen särskilt undersöka om brottsutredningsverksamheten som gäller sådan brottslighet kan förbättras genom att arbetet bedrivs i gemensamma utredningsgrupper med åklagare, poliser, befattningshavare från andra brottsbekämpande myndigheter samt andra experter. Beredningen skall i samband med det överväga hur en effektiv styrnings- och ledningsfunktion för en sådan grupp bör vara utformad. En annan central fråga som beredningen skall överväga i det sammanhanget är om det finns anledning att förändra åklagarnas uppgifter vid sådan brottsbekämpning, t.ex. om det kan finnas behov av åklagarkompetens vid polisens spanings- och kriminalunderrättelseverksamhet.

Beredningen bör mot bakgrund av vad den i övrigt kommer fram till även överväga i vad mån det finns anledning att åklagare och polis samlokaliseras helt eller delvis.

I uppdraget ingår alltså att beskriva och analysera den rättsliga regleringen och ordningen som styr polisens och åklagarnas roller och funktioner. Beredningen skall överväga om regleringen och ordningen är ändamålsenligt utformad. En central fråga i det avseendet är om det är nödvändigt med förändringar i nuvarande uppgifts- och ansvarsfördelning mellan polis och åklagare.

Därutöver skall beredningen överväga om förbättringar av brottsutredningsverksamheten kan åstadkommas genom att polisen och åklagarväsendet i större utsträckning utfärdar gemensamma föreskrifter och riktlinjer för hur det operativa brottsutredningsarbetet bör bedrivas.

Beredningen bör även undersöka i vad mån den ordning som finns för uppgifts- och ansvarsfördelning mellan polis och åklagare i andra europeiska stater kan ligga till grund för beredningens överväganden.

Beredningen skall vid genomförandet av uppdraget beakta de särskilda förutsättningar som gäller för Ekobrottsmyndigheten, bl.a. när det gäller organisation och arbetsformer.

Vid genomförandet av uppdraget skall beredningen också beakta det arbete som bedrivs i olika internationella forum – framför allt inom EU och Europarådet – för att vidareutveckla och förstärka brottsbekämpningen. I det sammanhanget bör beredningen – vid fördelningen av polisens och åklagarnas uppgifter och ansvar – särskilt beakta att det internationella straffrättsliga samarbetet (t.ex. utlämning, överlämnande och rättslig hjälp) är ett samarbete mellan rättsliga myndigheter i de olika staterna, dvs. i regel domstolar och åklagare.

Elektronisk kommunikation

Beredningen skall göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I detta ingår bl.a. en anpassning och modernisering av rättegångsbalkens terminologi, översyn av vilka verksamheter som bör omfattas av anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning, vilka typer av trafikuppgifter som bör få lämnas ut till de brottsbekämpande myndigheterna och om och i så fall under vilka förutsättningar som trafikuppgifter skall bevaras hos operatörerna. Beredningen bör särskilt analysera om utökade möjligheter för de brottsbekämpande myndigheterna medför ökade kostnader och hur dessa kostnader i så fall skall finansieras. Beredningen bör i det sammanhanget göra en avvägning mellan den nytta som de utökade möjligheterna ger i förhållande till de kostnadsökningar som kan uppstå.

En utgångspunkt för uppdraget skall vara att inte fler uppgifter bevaras för brottsbekämpande ändamål eller under längre tid än vad som är nödvändigt. En annan utgångspunkt är att personuppgifter som bevaras inte skall användas för något annat ändamål än brottsbekämpning.

Det står beredningen fritt att ta upp sådana frågor inom ramen för uppdraget som aktualiseras under utredningsarbetet.

Målsättningen för arbetet bör vara att skapa en enhetlig reglering som, särskilt med hänsyn till den snabba tekniska utvecklingen, kan stå sig över tiden.

Beredningen bör hålla sig underrättad om internationellt förhandlingsarbete som kan ha betydelse för beredningens uppdrag samt det arbete som pågår för att i svensk lagstiftning genomföra internationella åtaganden.

Övrigt

Beredningen skall lämna de förslag till författningsändringar och andra åtgärder som uppdraget kan ge anledning till.

I arbetet med att i brottsbekämpningen få tillgång till elektronisk kommunikation skall beredningen ha tillgång till en referensgrupp bestående av representanter för riksdagspartierna.

De nu berörda frågorna skall tas upp i beredningens plan för det fortsatta arbetet. Därvid skall frågan om att i brottsbekämpningen få tillgång till elektronisk kommunikation ges prioritet.

Beredningen skall redovisa uppdraget senast den 31 december 2005. Det står beredningen fritt att redovisa uppdraget i delbetänkanden.

(Justitiedepartementet)